

**Proiect:**

Proiect selectat în cadrul Programului Operațional Capacitate Administrativă cofinanțat de Uniunea Europeană, din Fondul Social European

Axa Prioritară 1: Administrație publică și sistem judiciar eficiente

Obiectivul specific 1.1: Dezvoltarea și introducerea de sisteme și standarde comune în administrația publică ce optimizează procesele decizionale orientate către cetățeni și mediul de afaceri, în concordanță cu SCAP.

Titlul proiectului: „Cadru strategic pentru adoptarea și utilizarea de tehnologii inovative în administrația publică 2021-2027 – soluții pentru eficientizarea activității”

COD: SIPOCA 704

Beneficiar: AUTORITATEA PENTRU DIGITALIZAREA ROMÂNIEI

Partener: UNIVERSITATEA TEHNICĂ DIN CLUJ - NAPOCA

Fundamentarea cazului de utilizare și studiu de
evaluare ex-ante pentru
Eliberare și urmărire certificate, diplome și alte
documente în domeniul educației

Cuprins

Referințe	3
Acronime și abrevieri	4
Scopul intervenției	6
Părțile interesate.....	8
Beneficiile estimate.....	9
Factori critici în asociere cu cazurile de utilizare	10
Provocări tehnice în implementarea intervenției.....	12
Procese curente care ar putea fi afectate de dezvoltarea proiectului	13
Obiectivele funcționale	17
Obiectivele de performanță.....	17
Elementele de noutate	18
Criteriile de selecție	19
Descrierea în detaliu a cazului de referință	21
Opțiuni de îmbunătățire	22
Analiza comparativă.....	24
Constrângeri privind implementarea.....	26
Resurse tehnice pentru implementare	27
Resurse umane pentru implementare.....	28
Resurse financiare pentru implementare	29
Resurse logistice pentru implementare.....	33
Riscuri și planuri de contingență.....	33
Interacțiunea cu alte sisteme tehnice	47
Diagrama pentru implementare	48
Metodologia de management a proiectului și modelul de dezvoltare	49
Precondiții și factori critici pentru succes	49
Indicatori pentru monitorizare și evaluare	50
Referințe bibliografice	51

Referințe

Numărul de proiecte pentru diplome educaționale stocate pe blockchain, în fază de pilot sau producție, este în creștere. Vom evidenția doar câteva din cele analizate, celelalte surse fiind amintite în restul capitolelor.

Universitatea din Nicosia (Cipru) emite certificate academice publice, care se pot verifica pe sistemul Bitcoin, fără să fie nevoie de contactarea instituției¹. Universitatea a început emiterea acestor diplome în 2015, studenților care au participat la cursul „Introducere în Monede Digitale. Din 2017, universitatea emite toate diplomele pe blockchain-ul Bitcoin, folosind o tehnologie deschisă, dezvoltare proprie. Diploma-document se emite sub formă digitală (PDF), universitatea o semnează digital, se calculează amprenta digitală a fișierului semnat, se înregistrează în blockchain. Oricine poate accesa blockchain și verifica cui s-a emis diploma, de către cine, când. Se poate valida originalitatea nemodificată a conținutului diplomei.

Soluția lor este deja în uz și la alte universități din lume; universitatea a lansat și un serviciu „spin-off” de înregistrare de documente pe blockchain².

Guvernul maltez a colaborat cu firma americană *Learning Machine Technologies* pentru a oferi certificate ancorate în blockchain oricărui cetățean înrolat în învățământul superior, pregătire de funcționar public sau vocațională³.

Utilizatorii folosesc aplicația gratuită Blockcerts, cu care gestionează perechea de cheie privată și cheie publică. Criptografia asimetrică, cu pereche de cheie privată și publică, nu este nouă, însă combinarea sa cu blockchain oferă și o urmă nemodificabilă a informațiilor.

Mai multe instituții malteze sunt implicate în acest sistem: Ministerul educației și angajării, Institutul de studii în turism, Colegiul maltez de arte, știință și tehnologie, Comitetul național pentru educație continuă și învățământ superior. Acesta din urmă înlocuiește și certificate vechi pierdute cu unele noi, bazate pe blockchain.

Pe lângă utilitatea evidentă pentru cetățenii din Malta, programul este și un experiment reușit la nivel global, posibil într-o țară cu doar 442 mii de locuitori în 2020⁴.

¹ UNIC. (2021). Publication of Academic Certificates. <https://www.unic.ac.cy/iff/blockchain-certificates/>.

² UNIC. (2021). The ONLY truly decentralized solution to secure PDF documents from fraud without intermediaries!, <https://blog.block.co/what-differentiates-block-co-from-its-centralized-competitors/>.

³ Patel, N. (2019). Malta Pilots Blockchain-Based Credentials Program. <https://spectrum.ieee.org/tech-talk/computing/networks/malta-pilots-blockchainbased-credentials-program>.

⁴ Worldometer. (2020). Malta Population. <https://www.worldometers.info/world-population/malta-population/>.

Ministerul Educației din Malaysia a decis înființarea unui consorțiu blockchain de universități malaysiene, atât pentru dezvoltarea unei soluții de diplome greu de falsificat, cât și pentru utilizarea sa⁵. Soluția dezvoltată se bazează pe NEM Blockchain și are avantajul simplității: cine dorește verificarea diplomei trebuie să scaneze codul bidimensional QR tipărit pe aceasta, iar autenticitatea se confirmă – sau se infirmă – în câteva secunde.

Firma BCdiploma s-a născut în 2017, în Franța. De atunci, oferă servicii de registru blockchain pentru diplome, certificate de educație continuă, certificate profesionale, certificări ISO, certificări notariale. Certificatele înregistrate sunt accesibile gratuit, pe toată durata vieții titularului⁶.

BCdiploma se laudă cu peste 90 clienți din 12 țări de pe 4 continente⁷. Printre instituții, majoritatea universități, se numără Université de Lille (70.000 studenți, 6.000 angajați), Blockchain at Berkeley, eCampusOntario, Honoris Online Academy (Mauritius), MANCOSA (Africa de sud), Can Tho University (Vietnam), MUST University (SUA), Facultad de Ciencias Políticas y Relaciones Internacionales (Mexic).

Canada, în cadrul proiectului „Talent Cloud”, emite diplome digitale, protejate cu blockchain.⁸

Faimosul **Massachusetts Institute of Technology** emite, similar, certificate educaționale pentru studenții care îi promovează cursurile.⁹

Acronime și abrevieri

Tabel 1: Acronime și abrevieri

⁵ Abas, A. (2018). University consortium set up to authenticate degrees using blockchain technology. <https://www.nst.com.my/news/nation/2018/11/429615/university-consortium-set-authenticate-degrees-using-blockchain>.

⁶ BCdiploma. (2021). Success stories. <https://www.bcdiploma.com/en/customersSuccess>.

⁷ BCdiploma. (2021). They certify with BCdiploma. <https://www.bcdiploma.com/en/issuersList/>.

⁸ Benay, A. (2019). Securing the future of talent mobility in the Government of Canada. <https://tbs-blog.canada.ca/en/securing-future-talent-mobility-government-canada> și (2017). Government of Canada: Talent cloud. <https://talent.canada.ca/en>.

⁹ Durant, E. (2017). Digital Diploma debuts at MIT. <https://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017>.

Abreviere sau acronim	Expresia completă	Explicație
API	Application Programming Interface	Interfață de programare aplicație: modalitatea documentată a unei aplicații software, prin care dezvoltatorul unei alte aplicații își poate programa propria aplicație ca să trimită sau să primească date spre/dinspre prima aplicație, fără să cunoască funcționarea internă a primei aplicații.
BSD	Berkeley Software Distribution	Sisteme de operare deschise, descendente al UNIX, similare cu Linux. Distribuțiile principale sunt FreeBSD, OpenBSD, NetBSD.
CBDE	Certified Blockchain Developer-Ethereum	Dezvoltator blockchain Ethereum certificat: unul din certificările posibile pe care le poate obține un dezvoltator de sisteme blockchain de tip Ethereum.
CHFD	Certified Hyperledger Fabric Developer	Dezvoltator structuri Hyperledger certificat: unul din certificările posibile pe care le poate obține un dezvoltator de sisteme blockchain de tip Hyperledger.
COR	Clasificarea Ocupațiilor din România	“Nomenclator apărut în anul 1995, ce reprezintă sistemul de identificare, ierarhizare și codificare a tuturor ocupațiilor desfășurate în economie, indiferent de tipul și locul desfășurării lor.”
DLT	Distributed Ledger Technology	Tehnologie de tip registru distribuit
EBSI	European Blockchain Services Infrastructure	Infrastructura europeană pentru servicii blockchain, promovată de Comisia Europeană.
IaaS	Infrastructure as a Service	Infrastructură ca serviciu: servicii cloud, în care nu doar software-ul și chiar sistemul de operare rulează pe serverele furnizorului, dar și rețeaua, interconexiunile dintre servere, infrastructura de calcul rulează pe echipamentele furnizorului, contra cost.
INS	Institutul Național de Statistică	“Principal producător de date statistice oficiale, responsabil de coordonarea tuturor activităților la nivel național privind dezvoltarea, elaborarea și difuzarea statisticilor europene.”
IoT	Internet of Things	Internetul obiectelor
LTO	Linear Tape-Open	Bandă liniară-deschis: tehnologie de stocare a datelor pe bandă magnetică (în cartușe). Este un standard deschis.

Abreviere sau acronim	Expresia completă	Explicație
MTBF	Mean Time Between (Before) Failures	Timpul mediu dintre (dinaintea) defectări: timp estimat și specificat de producător în cartea tehnică a unei componente hardware, pentru durata de viață normală a sa. Pentru echipamente unde funcționarea este critică, se recomandă schimbarea componentelor înainte de atingerea acestor termene.
PoS	Proof-of-Stake	Dovada mizei: unul din metodele principale de consens utilizate în sistemele blockchain.
PoW	Proof-of-Work	Dovada lucrului: unul din metodele principale de consens utilizate în sistemele blockchain.
QR	Quick Response code	Cod QR: grafică bidimensională ce codifică informații care pot fi citite de un echipament, de regulă cu cameră digitală.
RoEduNet	Romanian Education Network	Rețeaua națională pentru educație și cercetare: „asigură servicii de comunicații de date pentru instituțiile de cercetare și academice de toate gradele din România”. „Membru al consorțiului GEANT, rețeaua care interconectează toate rețelele pentru cercetare și educație din țările membre ale Uniunii Europene.”
SGX	Software Guard Extensions	Tehnologie de protecție software, inițiată de firma Intel.
TRL	Technology Readiness Level	Nivel de Pregătire Tehnologică (1-9): faza în care este o tehnologie anume, de la principii până la exploatare în mediul operațional.

Scopul intervenției

Definirea problemei

În zilele noastre, verificarea autenticității unei diplomei sau a unei certificări este un proces care se desfășoară manual, este costisitor și adesea necesită o lungă perioadă de timp. Un exemplu concret este cazul studenților care aplică pentru un master/doctorat în țară la o altă universitate decât cea absolvită, ori cazul unui absolvent care aplică pentru un job. În astfel de situații, instituțiile angajatoare solicită verificarea validității actelor care atestă competențele persoanelor respective. Problema se complică și mai mult în cazul instituțiilor din afara țării, caz în care sunt necesare atestări suplimentare cum ar fi traduceri lingvistice și autentificări/legalizări internaționale pentru a se putea dovedi autenticitatea documentelor originale.

O altă problemă cu care se confruntă societatea la ora actuală este cea de falsificare a diplomelor, respectiv a vânzării de certificate frauduloase. În România, exemple concrete sunt cazul diplomelor false emise de Universitatea Spiru Haret¹⁰ sau cazul emiterii unor diplome false pentru asistenți de medicină dentară de către o asociație care nu deținea acreditare din parte Ministerului Educației¹¹. Exemple similare întâlnim și în alte țări din Europa. Amintim aici cazul diplomelor false emise de către o firmă din Pakistan, unor cetățeni britanici¹².

Tehnologia blockchain, prin caracteristicile pe care le oferă (ex. imuabilitate, descentralizare, securitate, trasabilitate, și consens) poate fi folosită cu succes în implementarea unui sistem robust și de încredere pentru eliberarea diplomelor digitale¹³. Principalele avantaje oferite de implementarea unui astfel de sistem pe tehnologia blockchain sunt: (i) facilitează verificarea ușoară a validității și autenticității unei diplome sau certificări de orice parte interesată din întreaga lume, fără a fi nevoie de intermediari, (ii) elimină practicile frauduloase cu privire la modul de eliberare a diplomelor/certificatelor. Beneficiarii unei astfel de soluții sunt milioane de oameni (de ex. absolvenți, angajatori, instituții acreditate), iar beneficiile sunt imense. Din perspectiva absolvenților și angajatorilor, pe lângă beneficiile anterior menționate, se numără și cele de natură financiară: se salvează bani și timp.

Obiectivele generale

Obiectivele generale urmărite prin adoptarea unei soluții bazate pe tehnologia blockchain pentru eliberare și urmărire a certificatelor, diplomelor și altor documente în domeniul educației sunt următoarele:

- Îmbunătățirea încrederii interne și internaționale în diplomele emise de Ministerul Educației din România;
- Asigurarea interoperabilității cu sistemele din Uniunea Europeană și nu numai.
- Verificare facilă a calificărilor academice și transparență;

¹⁰ Digi24. Fraudă universitară de proporții la "Spiru Haret" privind diplomele emise.

<https://www.digi24.ro/stiri/actualitate/justitie/frauda-universitara-de-proportii-la-spiru-haret-diicot-investigheaza-cum-au-fost-date-diplomele-false-1233377>.

¹¹ Alexandra Andronie. Diplome false pentru asistenți de medicină dentară. <https://www.digi24.ro/stiri/actualitate/diplome-false-pentru-asistenti-de-medicina-dentara-programele-de-masterat-aveau-presupuse-colaborari-cu-universitati-din-europa-1624509>.

¹² The Times of India. Pakistani 'diploma mill' of fake degrees exposed. <https://timesofindia.indiatimes.com/world/uk/pakistani-diploma-mill-of-fake-degrees-exposed/articleshow/62528163.cms>.

¹³ J.C. Cheng, N.Y. Lee, C. Chi, Y.H. Chen, Blockchain and Smart Contract for Digital Certificate, the 4th IEEE International Conference on Applied System Innovation, ICASI, Chiba, Japan, 13–17 April 2018 și Kamišalić A., Turkanović M., Mrdović S., Heričko M. (2019) A Preliminary Review of Blockchain-Based Solutions in Higher Education. In: Uden L., Liberona D., Sanchez G., Rodríguez-González S. (eds) Learning Technology for Education Challenges. LTEC 2019. Communications in Computer and Information Science, vol 1011. Springer, Cham. https://doi.org/10.1007/978-3-030-20798-4_11.

- Posibilitatea arătării actelor de studii (i.e. diplomele, certificărilor) de către absolvent chiar și în situație în care nu dispune fizic de ele (de ex. diploma a fost pierdută și încă nu a fost eliberat duplicatul).

Obiectivele specifice

Ca obiective specifice amintim:

- Înregistrare în blockchain, la emitere a diplomelor de studii;
- Verificare facilă a validității diplomelor de studii;
- Partajarea actelor de studii cu părțile interesate;
- Acces pe tot parcursul vieții la diplomele de studii.

Obiectivele operaționale

Obiectivele operaționale urmărite prin adoptarea unei soluții bazate pe tehnologia blockchain pentru eliberare și urmărire a certificatelor, diplomelor și altor documente în domeniul educației sunt :

- Asigurarea unei infrastructuri tehnologice și organizaționale la nivel de universitate;
- Asigurarea unei infrastructuri tehnologice și organizaționale la nivel de minister;
- Asigurarea unei infrastructuri tehnologice și organizaționale pentru publicul larg;
- Asigurarea interoperabilității cu instituțiile de învățământ Uniunea Europeană și nu numai în vederea recunoașterii automate a calificărilor și a perioadelor de studii în străinătate.

Părțile interesate

Părțile interesate în implementarea unei soluții bazate pe tehnologia blockchain pentru eliberarea și urmărirea certificatelor, diplomelor și altor documente în domeniul educației pot fi clasificate în două mari categorii: *beneficiarii*, respectiv *utilizatorii* soluției dezvoltate.

Potențialii beneficiari ai unei soluții bazate pe tehnologia blockchain pentru eliberarea și urmărirea certificatelor, diplomelor și altor documente în domeniul educației sunt:

- Ministerul Educației
- Instituții de învățământ universitar
- Instituții de învățământ preuniversitar (e.g. liceu, colegiu, școală gimnazială)
- Instituții publice, firmele, persoane care organizează cursuri de formare profesională
- Absolvenți ai unei instituții de învățământ
- Absolvenți ai unor cursuri de formare profesională
- Angajatori din mediu privat
- Organizații guvernamentale, neguvernamentale.

Utilizatorii soluției dezvoltate sunt:

- Angajați ai departamentelor de resurse umane din cadrul companiilor/ organizațiilor responsabile cu recrutarea angajaților
- Angajați ai firmelor specializate în recrutare de personal
- Angajați ai birourilor Acte de Studii din cadrul instituțiilor de învățământ.

Beneficiarii și utilizatorii soluției tehnice/tehnologiei vor fi consultați permanent în procesul de luare a deciziilor cu privire la soluția propusă. Acest lucru se va realiza prin organizarea de sondaje pe bază de chestionare la care sunt invitați să participe toate părțile interesate. Promovarea chestionarelor se va face prin trimiterea de newsletters angajatorilor, instituțiilor acreditate, etc. cât și prin social media.

Beneficiile estimate

Principalele beneficii care ar putea fi obținute prin adoptarea unei soluții bazate pe tehnologia blockchain pentru eliberarea și urmărirea certificatelor, diplomelor și altor documente în domeniul educației sunt:

- Verificare rapidă a validității diplomelor de studii de către instituțiile de învățământ și de către angajatori (e.g. verificare diplome de bacalaureat în contextul admiterii în instituțiile de învățământ superior, verificare diplome de licență în cazul absolvenților care doresc să urmeze programe de masterat/doctorat în alte universități decât cea absolvită, verificare de către angajatori a diplomelor/certificărilor deținute de persoana care candidează pe o anumită poziție pentru angajare).
- Posibilitate de partajare rapidă a diplomelor/certificărilor cu părțile interesate.
- Sfârșitul cererilor intempestive de verificare a diplomelor sau emitere a duplicatelor.
- Recunoaștere mai ușoară a diplomelor emise în alt stat, a abilităților aprofundate de absolvent (interoperabilitate).
- Reduc sarcinile personalului administrativ responsabil cu eliberarea de diplome/certificate.
- Face posibilă urmărirea într-o manieră rapidă și sigură a înregistrărilor academice, ceea ce permite depistarea rapidă a diplomelor false.
- Caracteristica de imuabilitate a blockchain-ului poate spori credibilitatea și poate reduce riscul de pierdere a informațiilor¹⁴

¹⁴ J.C. Cheng, N.Y. Lee, C. Chi, Y.H. Chen, Blockchain and Smart Contract for Digital Certificate, the 4th IEEE International Conference on Applied System Innovation, ICASI, Chiba, Japan, 13–17 April 2018.

- Blockchain poate fi folosit și pentru a construi un ecosistem global (transnațional) de validare a certificatelor¹⁵.
- Din punctul de vedere al absolvenților, soluțiile bazate pe blockchain pot simplifica procesul de validare a acreditărilor primite și elimină necesitatea intermediarilor.
- Beneficii legate de costuri și timp pentru absolvenți (nu mai sunt necesare traduceri lingvistice și autentificări internaționale/legalizări ca modalitate de a dovedi autenticitatea documentelor originale în cazul în care vor să aplice pentru un job în străinătate sau doresc să își continue studiile în afara țării)
- Utilizarea de diferite mecanisme criptografice, combinate cu adoptarea unui registru distribuit, oferă certificărilor academice un nivel mai ridicat de securitate¹⁶.
- Prin posibilitatea implementării unor contracte inteligente imbricate în blockchain, care să declanșeze anumite acțiuni la emiterea sau/și verificarea diplomelor:
 - Sistemul poate contribui automat la statistici, de exemplu a celor mai căutate specializări (corelate cu COR) sau alți indicatori de interes (posibil corelate cu INS);
 - Titularii pot fi anunțați automat despre emiterea diplomei, respectiv de fiecare dată când cineva – un potențial angajator sau altă instituție - le verifică diploma, sau prin posibilitatea vizualizării istoricului de accesări, contribuind la democratizare și transparență.
 - Apare posibilitatea de soluționare a unor probleme etice, de exemplu la admiterea pentru studii superioare. Au existat cazuri de admitere în care unele universități au reținut diploma studiilor anterioare, în original, pentru o perioadă mai lungă, candidatul neavând posibilitatea să-și depună actele la altă universitate, concurentă. Se poate crea un contract inteligent care să marcheze faptul că diploma este „ocupată” la o admitere, la o anumită universitate, acest fapt putând fi verificat de către alte universități.

Factori critici în asociere cu cazurile de utilizare

Factorii care afectează adoptarea tehnologiei blockchain în dezvoltarea unei soluții pentru eliberarea și urmărirea certificatelor, diplomelor și altor documente în domeniul educației pot fi împărțiți în următoarele categorii: (a) *Factori critici privind cerințele tehnice*, (b) *Factori critici de cost*, (c) *Factori critici privind calitatea*, (d) *Factori critici privind ușurința execuției*, (e)

¹⁵ Serranito D., Vasconcelos A., Guerreiro S., Correia M. Blockchain Ecosystem for Verifiable Qualifications; Presented at the 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS; Paris, France, 28–30 September 2020.

¹⁶ Fernando Richter Vidal, Feliz Gouveia, Christophe Soares, Blockchain Application in Higher Education Diploma Management and Results Analysis, Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 6, 871-882 (2020) Distributed Ledger Technology (DLT) and Blockchain, FinTech Note | No. 1.

Factori critici sub aspect economic, (f) Factori critici sub aspect legal. Vom prezenta în continuare factorii critici identificați pentru fiecare din cele șase categorii.

Factori critici privind cerințele tehnice:

- Necesitatea existenței unei rețele de servere, distribuite geografic;
- Probleme de scalabilitate;
- Capacitatea hardware mare necesară pentru a susține aplicații pe blockchain cu volum mare de tranzacții¹⁷;
- Capacitatea de stocare mare, necesară pentru participarea la blockchain pe termen lung¹⁸;
- Capacitate de rețea și procesare suplimentară pentru interfațarea aplicațiilor blockchain cu aplicațiile existente¹⁹;
- Absența standardizării limbajelor de programare²⁰;
- Imaturitatea tehnologiei.

Factori critici de cost

- Costuri legate de mentenanță pe termen lung, pentru asigurarea disponibilității blocurilor mai vechi;
- Consum de energie mare necesar pentru efectuarea calculelor criptografice;
- Cost ridicat de implementare (costuri legate de echipamentele hardware și software);
- Costul schimbării infrastructurii actuale, costul de timp din cauza tranzacțiilor lente și costul de gestionare a datelor de dimensiuni mari;
- Costuri legate de formarea și recrutarea personalului specializat.

Factori critici privind calitatea

- Acces la blocuri, conform arhitecturii și protocolului;
- Probleme de latență;
- Risc de atac cibernetic.²¹

¹⁷ Raritan. Blockchain Infrastructure BlockOps. <https://www.raritan.com/landing/blockchain-infrastructure-blockops-wp/thanks>.

¹⁸ Raritan. Blockchain Infrastructure BlockOps. <https://www.raritan.com/landing/blockchain-infrastructure-blockops-wp/thanks>.

¹⁹ Raritan. Blockchain Infrastructure BlockOps. <https://www.raritan.com/landing/blockchain-infrastructure-blockops-wp/thanks>.

²⁰ Choi, D.; Chung, C.Y.; Seyha, T.; Young, J. Factors Affecting Organizations' Resistance to the Adoption of Blockchain Technology in Supply Networks. *Sustainability* 2020, 12, 8882. <https://doi.org/10.3390/su12218882>.

²¹ Bojana Koteska, Anastas Mishev, Blockchain Implementation Quality Challenges: A Literature Review, In: Z. Budimac (ed.): Proceedings of the SQAMIA 2017: 6th Workshop of Software Quality, Analysis, Monitoring, Improvement, and Applications, Belgrade, Serbia, 11-13.9.2017.

Factori critici privind ușurința execuției

- Lipsa de expertiză și cunoștințe tehnice. Este necesară pregătirea personalului pentru dezvoltare de aplicații back-end, front-end, respectiv a utilizatorilor.
- Menținerea fluxului de personal calificat.

Factori critici sub aspect economic (efecte colaterale negative, costuri de oportunitate)

- Asigurarea de fonduri pentru mentenanță hardware/software;
- Asigurarea de fonduri pentru instruirea personalului/utilizatorilor.

Factori critici sub aspect legal

- Lipsa unor reglementări și cadre legale adecvate în blockchain;
- Nu există o autoritate responsabilă pentru rezolvarea disputelor;
- Structurile juridice nu protejează în mod satisfăcător utilizatorii de cauza problemelor care pot să apară pe platforma blockchain;
- Probleme legate de regulile privind confidențialitatea și protecția datelor (de exemplu, Regulamentul general privind protecția datelor);
- Imuabilitatea datelor în blockchain poate impune bariere pentru a respecta „dreptul de a fi uitat”²²;
- Lipsa posibilității de a corecta informații, capacității de a retrage diplome și acreditări²³.

Provocări tehnice în implementarea intervenției

Principalele provocări tehnice în implementarea unei soluții bazate pe blockchain pentru eliberarea și urmărirea certificatelor, diplomelor și altor documente în domeniul educației sunt:

- Construirea infrastructurii hardware;
- Construirea infrastructurii software;
- Menținerea disponibilității serviciului, atât pentru înregistrarea diplomelor noi (operațiune rară), cât și verificarea valabilității diplomelor (operațiune frecventă);
- Asigurarea compatibilității hardware/software cu cerințele sistemului blockchain și ale clienților, atât pentru sistemul nou implementat, cât și a dezvoltărilor ulterioare, inclusiv interoperabilitatea cu sisteme similare naționale, europene și internaționale, dar și alte servicii care vor interacționa cu sistemul propus;
- Stabilirea unor standarde minime pentru hardware, software, calitatea furnizării serviciului.

²² Castro RQ, Au-Yong-Oliveira M. Blockchain and Higher Education Diplomas. *Eur J Investig Health Psychol Educ.* 2021;11(1):154-167. Published 2021 Feb 19. doi:10.3390/ejihpe11010013.

²³ Castro RQ, Au-Yong-Oliveira M. Blockchain and Higher Education Diplomas. *Eur J Investig Health Psychol Educ.* 2021;11(1):154-167. Published 2021 Feb 19. doi:10.3390/ejihpe11010013.

Un aspect ce introduce provocări adiționale este utilitatea stocării istoricului pașilor care au dus la emiterea diplomei, înainte de diploma propriu-zisă:

- Documentul lucrării de diplomă și materialele software dezvoltate, posibil prezentarea și/sau înregistrarea video ale susținerilor, ca bază pentru nota finală;
- Foaia matricolă a anilor de studii;
- Urma verificării anti-plagiat a lucrării, de exemplu cu Turnitin;
- Alte informații premergătoare elaborării, susținerii, evaluării și emiterii diplomei.

Colectarea și stocarea acestor date auxiliare presupune digitalizarea lor, stocarea și înregistrarea lor - imutabilă - în blockchain. Se poate folosi același blockchain, blocul cu diploma putând conține și informațiile auxiliare, sau se pot înregistra într-un blockchain secundar, conectat de cel primar prin identificatori unici sau hash-uri. Se recomandă această soluție din urmă, pentru cazurile în care sunt dubii în privința validității provenienței diplomei validate și apare nevoia coroborării cu documentele auxiliare ce preced emiterea diplomei.

Documentele auxiliare nu trebuie stocate în blockchain, doar amprentele lor digitale, asta ajută și în conformitatea cu GDPR. Însă datele propriu-zise trebuie stocate digital undeva, preferabil online pentru verificare facilă. Această cerință de stocare online prezintă provocări similare cu cea a disponibilității serviciului blockchain pentru diplome, însă cu necesar mult mai ridicat de spațiu de stocare.

Procese curente care ar putea fi afectate de dezvoltarea proiectului

Procesele curente care ar pot fi afectate de dezvoltarea proiectului sunt: procesul de completare a actelor de studii, procesul de eliberare a actelor de studii, procesul de eliberare adeverință de absolvire, procesul de eliberare duplicat act de studiu în caz de pierdere/ furt, procesul de verificare a actelor de studii.

Procedura standard care se urmează în cazul eliberării actelor de studii la nivelul fiecărei universități constă din următorii pași²⁴:

- Într-un anumit termen stabilit la nivel de universitate de la încheierea examenelor de finalizare a studiilor, secretarii comisiilor de examen vor depune documentația privind rezultatele examenelor la secretariatele facultăților.
- Universitatea va elibera diplomele pentru absolvenții care au promovat examenul de finalizare a studiilor în termen de cel mult 12 luni de la data promovării.
- Până la eliberarea diplomei, absolvenții care au promovat examenul de finalizare a

²⁴ Senatul Universității Tehnice din Cluj-Napoca. Regulament privind organizarea și desfășurarea examenelor de finalizare a studiilor pentru ciclul I și II în Universitatea Tehnică din Cluj-Napoca (examene de licență/diplomă și disertație) pentru anul universitar 2020-2021, 2021, https://www.utcluj.ro/media/decisions/2021/03/30/Regulament_finalizare_studii.pdf.

studiilor primesc, la cerere, adeverințe de absolvire care îi conferă titularului aceleași drepturi legale ca și diploma. În caz de pierdere sau distrugere, eliberarea unei noi adeverințe urmează procedurile privind eliberarea duplicatelor diplomelor.

- Absolvenții care nu promovează examenul de finalizare a studiilor primesc, la cerere, un certificat de studii universitare care cuprinde următoarele informații: domeniu de studii universitare, programul de studii/specializarea, perioada de studii, mediile de promovare a anilor de studii, statutul de acreditare/autorizare provizorie, forma de învățământ, limba de predare, locația geografică, numărul de credite și actul normativ care le stabilește (Hotărâre a Guvernului, ordin al ministrului, după caz).
- Rectorul poate anula, cu aprobarea Senatului universității, un examen de finalizare a studiilor, un certificat sau o diplomă de studii atunci când se dovedește că s-a obținut prin mijloace frauduloase sau prin încălcarea prevederilor Codului de etică și deontologie universitară.
- În cazul instituțiilor de învățământ superior desființate, suplimentul de diplomă se completează și se eliberează de către instituția de învățământ universitar acreditată care a organizat examenul de finalizare de studii universitare, în baza situației școlare/foii matricole cu care absolventul a fost admis să susțină examenul de finalizare a studiilor, respectiv a documentelor eliberate de către Arhivele Naționale, serviciile județene/Serviciul Municipiului București ale/al Arhivelor Naționale sau de către instituțiile unde a fost depusă arhiva instituției desființate, după caz.

Din pașii descriși anterior se poate observa că acest proces este unul extrem de complex, care implică un număr mare de angajați/departamente (e.g. angajații ai biroului acte de studii, angajați ai secretariatelor facultăților, secretar șef la nivel de universitate, decani, rector, etc.). Întregul proces de eliberare a diplomelor de studii sau duplicate acte de studii durează un timp relativ lung (aproximativ un an în cazul eliberării actelor de studii, respectiv o lună în cazul eliberării duplicatelor).

Prezentăm în continuare o versiune simplificată a procesului de eliberare acte de studii care se desfășoară la ora actuală în cadrul Universității Tehnice din Cluj-Napoca și care are la baza *Procedura operațională de comandă, gestionare și eliberare a actelor de studii tipizate la nivelul Universității Tehnice din Cluj-Napoca*²⁵ precum și *Regulamentul privind organizarea și desfășurarea examenelor de finalizare a studiilor pentru ciclul I și II în Universitatea Tehnică din Cluj-Napoca* [49]. Procesul se bazează pe un set de sub proceduri stabilite la nivel de Universitate, sub proceduri care vor fi descrise în cele ce urmează:

1. Sub procedura de completare acte de studii:

- Se primesc tabele cu datele personale ale absolvenților, precum și cu notele acestora semnate de către secretar șef facultate și decan de la secretariatele facultăților care se

²⁵ Simona Cimponeriu, Lidia-Ioana Fodorean. Procedură operațională: comanda, gestionarea, completarea și eliberarea actelor de studii tipizate, Biroul Acte de Studii UTCN, 2014, https://www.utcluj.ro/media/page_document/148/Procedura%20Acte%20de%20studii.pdf.

verifică la Biroul Acte de studii cu certificatul de naștere și CI, pentru corectitudinea datelor personale;

- Se primesc de la Departamentul de informatică în format tabelar datele existente ale absolvenților care se confruntă cu datele din tabelele primite de la secretariate.
- Se completează diplomele de studii ale absolvenților în format electronic.
- Se listează diplomele absolvenților.
- Se înregistrează diplomele listate în registrele de evidență ale actelor de studii, unde primesc un număr de înregistrare unic.
- După listare și înregistrare, se aplică pozele absolvenților, se semnează de către persoanele responsabile (secretar șef facultate, decan, secretar șef universitate și rector), iar apoi se aplică timbru sec și stampila cu stemă.
- Se întocmește un proces verbal la sfârșit de an universitar care conține informații cu privire la numărul de formulare ridicate/ utilizate.
- Se întocmește un raportul anual privind gestionare, completare și eliberarea actelor de studii pe baza proceselor verbale întocmite în prealabil.

2. Sub procedura eliberare acte de studii

- Absolventul se prezintă la biroul acte de studii cu documentele necesare eliberării diplomei.
- Angajatul de la biroul acte de studii verifică fișa de lichidare a absolventului.
- Angajatul de la biroul acte de studii completează datele în Registru de evidență, eliberează și semnează de eliberarea.
- Absolventul semnează de primire în Registru de evidență, pe cotor și pe diploma după caz.
- În cazul eliberării actului unui împluternicit, aceste completează cererea tip, la care atașează procura notarială în original. Împluternicitul semnează de primire în toate locurile prevăzute pentru semnarea titularului, mai puțin pe actul de studiu.

3. Sub procedură eliberare adeverințe de absolvire

- Se primesc de la secretariatele facultăților următoarele informații
 - i. tabele cu datele personale ale absolvenților
 - ii. tabelele cu notele absolvenților de la examenul de finalizare studii
 - iii. adeverințele listate din baza de date semnate de secretar șef facultate și decan
 - iv. borderoul de eliberare a adeverințelor.
- Se verifică corectitudinea datelor personale și sesiunea în cazul adeverințelor pentru examen de diplomă sau data exactă a finalizării studiilor în cazul adeverințelor fără examen de diplomă.
- Tabelele și borderourile primesc același număr de înregistrare din registrul de eliberare adeverințe.
- Se semnează adeverințele de către persoanele responsabile, se aplică pe adeverință sigiliu și se predau adeverințele însoțite de borderouri secretariatelor

facultăților unde vor primi un număr de înregistrare.

4. Sub procedură eliberare acte duplicate

- Titularul sau împuternicitul adresează o cerere rectorului universității prin care solicita eliberarea duplicatului, cerere însoțită de actele necesare eliberării duplicatului (ex. Monitorul oficial al României unde apar publicat anunțul pierderii actului de studii, declarația titularului autenticată la notar în care sunt specificate elementele necesare identificării împrejurărilor în care a fost pierdut actul, copie legalizată certificate de naștere și CI, dovadă plată taxă pentru eliberare duplicat)
- Angajații biroului acte de studii verifică documentele necesare întocmirii duplicatului și menționează existența/ inexistența actului necesar întocmirii duplicatului.
- După aprobarea cererii, angajatul biroului acte de studii întocmește decizia rectorului privind aprobarea completării și eliberării duplicatului
- Angajatul biroului acte de studii completează duplicatul cu datele existente în documentele specificate din arhiva biroului acte de studii
- Titularul sau împuternicitul poate ridica duplicatul în termen de o luna de la biroul acte de studii

În cazul procesului de verificare a diplomelor, angajatorul fie solicită viitorului angajat o copia scanată a actului de studii care va fi comparată cu actul original, fie solicită o copie legalizată după actul de studiu. Dacă dorește angajatorul se poate adresa instituțiilor abilitate pentru a verifica veridicitatea actului original sau îi poate solicita viitorului angajat să aducă o dovadă de la universitatea emitentă care să ateste autenticitatea diplomei. Procesul de verificare al autenticității unei diplome este o sarcină extrem de costisitoare din puncte de vedere al timpului/ resurselor implicate.

Prin implementarea unei soluții bazate pe tehnologia blockchain aceste procese vor suferi modificări. De exemplu în cazul completării actelor de studii, s-ar putea să apară pași suplimentari cum ar fi: (a) crearea de către instituția emitentă a diplomei digitale (la ora actuală diploma digitală generată este folosită doar pentru tipărirea diplomei pe hârtie și nu este pusă la dispoziția destinatarului), (b) generarea pe baza diplomei digitale a unei funcție hash unidirecțională corespunzătoare diplomei pe hârtie, (c) stocarea hash-ului într-un contract inteligent. Prin adoptarea unei soluții bazate pe blockchain diploma electronică va fi disponibilă imediat, fără a mai fi necesară eliberarea adeverințelor de absolvire. În cazul verificării actelor de studii, compania verificatoare care primește diploma de la potențialul angajat va putea verifica autenticitatea documentului fără a contacta universitatea. Verificatorul ar putea folosi diploma digitală ca intrare pentru verificare autenticitatea hash-ului, care ar putea fi comparat cu toate hash-urile din contractul inteligent, iar dacă acesta se potrivește compania va fi informată că diploma este autentică. Diploma va putea fi verificată imediat după absolvire, chiar înainte de emiterea versiunii fizice, fără a mai fi nevoie de o copie a ei la momentul angajării. Un alt aspect care merită să fie menționat ar fi că s-ar putea renunța la pasul de eliberare a adeverințelor de absolvire deoarece absolventul va avea acces imediat la diplomă după absolvire. În cazul în care

absolventul aplică pentru un loc de muncă în străinătate, nu vor mai fi necesare traduceri lingvistice și autentificări internaționale/legalizări ca modalitate de a dovedi autenticitatea documentelor originale.

Prin procesul nou de emitere a actelor de studii, se reduce timpul necesar pentru emiterea actelor de studii.

Tehnologia blockchain permite crearea unei structuri capabile să facă procesul de verificare independent de universitatea emitentă a actelor de studii.

Pe lângă aceste aspecte, se reduce numărul de angajați din cadrul birourilor Acte de Studii, respectiv Resurse Umane. De asemenea, angajații trebuie instruiți în vederea utilizării soluției bazate pe blockchain, ceea ce adaugă la eforturile lor și la procesele pe care trebuie să le cunoască.

Obiectivele funcționale

Funcționalități dorite a fi regăsite în cadrul soluției tehnice/tehnologiei sunt:

- Emiterea rapidă a diplomelor/certificărilor academice.
- Verificarea ușoară a diplomelor/certificărilor academice.
- Posibilitate de partajare rapidă a diplomelor/certificărilor academice.
- Posibilitate de implementare a unor contracte inteligente imbricate în blockchain, pentru declanșarea automată a unor acțiuni sau contribuirea la statistici.

Obiectivele de performanță

Caracteristicile de performanță tehnică ale soluției propuse derivă din beneficiile rezultate din adoptarea unei soluții bazate pe blockchain și sunt următoarele²⁶:

- **Securitatea.** Implementarea unei rețele distribuite prin Internet are beneficii net superioare în ceea ce privește securitatea în contrast cu un sistem centralizat. Rețelele centralizate creează un singur punct de eșec pentru toate serviciile conectate, în timp ce dispozitivele dintr-o rețea distribuită sunt autonome și nu se bazează pe un sistem central. Orice încercări rău intenționate de a modifica sau ataca o bază de date distribuită ar necesita penetrarea majorității nodurilor conectate, care sunt de ordinul miilor, ceea ce face practic

²⁶ Harish Natarajan et al. Distributed Ledger Technology (DLT) and Blockchain.

<http://documents1.worldbank.org/curated/pt/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>; Josh Taubenheim. Distributed Ledger Technology (DLT): 7 Benefits for IoT Applications. <https://www.machnation.com/2019/03/13/distributed-ledger-technology-dlt-7-benefits-for-iot-applications/> și Ilker Koksall. The Benefits Of Applying Blockchain Technology In Any Industry. <https://www.forbes.com/sites/ilkerkoksall/2019/10/23/the-benefits-of-applying-blockchain-technology-in-any-industry/?sh=716e820c49a5>.

imposibilă spargerea.

- **Încredere.** Blockchain creează încredere între diferite entități în care încrederea este fie inexistentă, fie nedovedită.
- **Imuabilitate.** Imutabilitatea se referă la faptul că tranzacțiile, odată înregistrate pe blockchain, nu pot fi modificate sau șterse. Ca atare, blockchain poate fi folosit pentru a urmări informațiile în timp, permițând un audit sigur și de încredere al informațiilor.
- **Fiabilitatea datelor.** Deoarece modificările aduse unei baze de date distribuite sunt supuse mai multor niveluri de validare, în cazul tehnologiei de tip registru distribuit, riscul de a accesa/analiza datele inexacte/ nedorite este foarte redus.
- **Descentralizare și lipsa intermediarilor.** Tehnologia de tip registru distribuit permite transferuri directe de valoare sau token-uri între două părți implicate într-o manieră descentralizată, eliminând necesitatea unui intermediar sau a unei autorități centrale care controlează registrul.
- **Controlul individual al datelor.** Blockchain permite controlul individual asupra propriilor date digitale. Persoanele fizice și organizațiile individuale pot decide ce părți din datele lor digitale doresc să partajeze, cu cine și pentru cât timp. Se recomandă păstrarea doar a hash-urilor datelor în blockchain, cu păstrarea secretă a datelor originale.
- **Creșterea vitezei și a eficienței.** Tehnologia de tip registru distribuit oferă potențialul de creștere a vitezei și a eficienței prin eliminarea intermediarilor și automatizarea proceselor.
- **Automatizare și programabilitate.** Tehnologia de tip registru distribuit permite programarea unor condiții prestabilite care sunt executate automat odată ce anumite condiții sunt satisfăcute. Acest concept poartă numele de „contract inteligent”. Contractele inteligente pot fi definite și în cazul sistemelor de registre centralizate necesită ca acțiunile să fie implementate doar după ce părțile interesate au ajuns la un acord cu privire la faptul că tranzacția care a fost înregistrată în sistemul central, poate dura, în anumite contexte, mai mult de o zi. În contrast, în cazul tehnologiei de tip registru distribuit, părțile implicate se pun de acord în momentul în care tranzacția este finalizată, deoarece ambele au aceeași înregistrare a tranzacției. De asemenea, propagarea și reconcilierea, rezultatul execuției unui contract inteligent durează mai puțin decât în cazul unui sistem de registru tradițional.
- **Transparența și confidențialitatea.** În blockchain, toate tranzacțiile înregistrate într-un bloc pot fi verificate, fără a dezvălui identitatea persoanelor care le-au efectuat care este ascunsă prin intermediul unor protocoale avansate de securitate.

Elementele de noutate

Elementele de noutate aduse de tehnologia blockchain în dezvoltarea unei soluții pentru eliberarea și urmărirea certificatelor, diplomelor și altor documente în domeniul educației sunt:

- Eliminarea diplomelor contrafăcute și vânzarea frauduloasă de diplome/certificări

academice (datorită managementului descentralizat);

- Reducerea timpului necesar pentru eliberarea diplomelor/certificărilor academice;
- Asigurarea posibilității de partajare instantanee a diplomelor/certificărilor academice;
- Reducerea timpului de verificare și validare a autenticității diplomelor sau certificărilor academice care la ora actuală implică un proces de lungă durată, ce se face manual și este costisitor din perspectiva resurselor umane implicate;
- Asigurarea interoperabilității digitale între instituții de învățământ și angajatori, respectiv instituții de învățământ din cadrul Uniunii Europene și nu numai.
- Controlul asupra partajării actelor de studii/certificărilor academice va fi transferat de la instituțiile de învățământ/angajator la cursant, lucrător, absolvent.

Criteriile de selecție

Criteriile de selecție care stau la baza deciziei alegerii platformei blockchain cea mai potrivită pentru a fi folosită în implementarea unei soluții pentru eliberarea și urmărirea certificatelor, diplomelor și altor documente în domeniul educației sunt²⁷:

1. Scopul Platformei
2. Mod de operare
3. Nivelul de confidențialitate
4. Mecanismul de consens
5. Limbaje de programare
6. Rol nod în rețea.

Prezentăm în continuare o analiză comparativă între Hyperledger și Ethereum pe baza criteriilor anterior menționate.

1. Scopul Platformei.

a. Ethereum

- i. A fost introdus cu scop de a rula contracte inteligente pe EVM
- ii. Permite implementarea aplicațiilor descentralizate, cunoscute și sub numele de dApps
- iii. Platformă pentru afaceri de tip B2C și aplicații generalizate

b. Hyperledger

- i. A fost introdus pentru a accelera colaborarea în sectorul industrial
- ii. Este conceput pentru a oferi un grad ridicat de confidențialitate, rezistență și scalabilitate.

²⁷ Prerna Singh. Hyperledger vs Ethereum – Which Blockchain Platform Will Benefit Your Business? <https://www.edureka.co/blog/hyperledger-vs-ethereum/> și Nitish Srivastava. Ethereum Vs. Hyperledger: A Comprehensive Guide. <https://www.blockchain-council.org/ethereum/ethereum-vs-hyperledger-a-comprehensive-guide/>.

- iii. Are o arhitectură modulară și oferă multă flexibilitate
- iv. Platformă pentru afaceri de tip B2B.

2. Modul de operare

- a. În **Ethereum**, modul de operare este public/privat și nu este necesară nicio permisiune pentru a accesa rețeaua.
- b. În **Hyperledger**, fiind un blockchain privat, numai participanții autorizați pot accesa rețeaua (rețeaua este limitată la o comunitate predefinită de participanți cu permisiune).

3. Nivelul de confidențialitate

- a. **Ethereum** este absolut transparent și fiecare tranzacție este vizibilă pentru toată lumea din rețea.
- b. **Hyperledger** este privat și autorizat, ceea ce înseamnă că tranzacțiile care au loc în rețea sunt vizibile doar pentru membrii autorizați.

4. Mecanismul de consens

- a. **Ethereum** folosește un mecanism de consens în care toate nodurile trebuie să ajungă la un consens. În prezent, Ethereum folosește ca și algoritm de consens Proof-of-Work (PoW) și Proof-of-Stake (PoS).
- b. **Hyperledger** permite nodurilor să aleagă între No-op (nu este nevoie de consens) și un protocol de acord (PBFT) prin care două sau mai multe părți pot conveni asupra unei chei în așa fel încât ambele să influențeze rezultatul. Hyperledger are un control fin asupra consensului și acces restricționat la tranzacții, ceea ce se reflectă în scalabilitate și confidențialitate îmbunătățite.

5. Limbaj de programare

- a. Ethereum folosește limbajul de programare Solidity pentru a scrie contractele inteligente.
- b. Hyperledger folosește Golang pentru a scrie contracte inteligente.

6. Rol nod în rețea

- a. În Ethereum, fiecare nod are un rol, ceea ce înseamnă că, dacă are loc o tranzacție, mai multe noduri trebuie să participe la ea pentru finalizarea acesteia; datorită acestui fapt pot apărea probleme de scalabilitate, confidențialitate și eficiență.
- b. În Hyperledger nu este informat fiecare nod din rețea despre tranzacția efectuată.

Tabel 2: Comparatie între Hyperledger și Ethereum²⁸

²⁸ Prerna Singh. Hyperledger vs Ethereum – Which Blockchain Platform Will Benefit Your Business? <https://www.edureka.co/blog/hyperledger-vs-ethereum/>.

Caracteristici	Hyperledger	Ethereum
Scop	Platformă preferată pentru afacerile B2B	Platformă pentru afaceri B2C și aplicații generalizate
Confidențialitate	Tranzacții confidențiale	Transparent
Mecanism de consens	Algoritm de consens conectabil: nu este necesar mining	Algoritmul PoW: se ajunge la consens prin minerit
Limbaj de programare	Chaincode scris în Golang, Java, NodeJS	Contracte inteligente scrise în Solidity
Rol nod	Nu informează fiecare nod din rețea despre o tranzacție efectuată.	Fiecare nod în rețea are un rol; dacă are loc o tranzacție, mai multe noduri trebuie să participe la ea pentru a o finaliza
Modul de operare	Rețea privată și autorizată	Rețea publică/privată și fără permisiuni

Descrierea în detaliu a cazului de referință

Majoritatea instituțiilor de învățământ superior își păstrează informațiile despre studenții absolvenți într-un format proprietar (ex. baze de date structurate care pot fi accesate exclusiv de personalul acelei instituții pentru care au fost implementate prin intermediul unor sisteme online dedicate), fără a asigura interoperabilitate cu alte sisteme informatice administrative și de management din sistemul educațional. În general, aceste baze de date sunt găzduite într-un centru de date în cadrul instituțiilor de învățământ superior, cu acces restricționat la specialiștii IT din cadrul acelei instituții. Studenții au acces la datele lor într-o manieră restricționată, protejată prin parolă (ex. <https://websinu.utcluj.ro/>) din cadrul Universității Tehnice din Cluj-Napoca) și pot doar să vizualizeze/ listeze informații cu privire la examenele pe care le-au absolvit, respectiv creditele acumulate, fără a le oferi posibilitatea ca în momentul finalizării studiilor să aibă acces la următoarele documente digitale: suplimentul la diplomă, foaia matricolă, adeverința privind școlarizarea/absolvirea fără examen de finalizare a studiilor, adeverința privind finalizarea studiilor, etc. Chiar dacă s-ar implementa un sistem informatic integrat care să permită conectarea între sistemele existente din învățământul preuniversitar/universitar și Ministerul Educației, există câteva aspecte cheie care ridică probleme în ceea ce privește adoptarea unei soluții centralizate: standardizarea datelor, locația de stocare, securitatea datelor și modul de partajare în siguranță a datelor. Problemele legate de stocarea centralizată a datelor, lipsa standardizării, imposibilitatea accesării/partajării datelor, apar și în situația în care absolventul aplică pentru un loc de muncă în străinătate și trebuie să facă dovada diplomei universitare. În astfel de situații, absolvenții trebuie să-și traducă/legalizeze certificatul academic. Procesul de legalizare care include traducerea tuturor documentelor oficiale în limba instituției

gază, este un proces complex, care necesită un consum de timp/bani din partea absolventului și de timp din partea instituției angajatoare care trebuie să analizeze și să valideze fiecare aspect al documentelor legalizate. Deși există o inițiativă la nivel național pentru implementarea unui Sistem Informatic Integrat (<https://www.siiir.edu.ro/despre-proiect>), implementarea unei soluții bazată pe tehnologii de tip registru distribuit, oferă următoarele avantaje în contrast cu o soluție centralizată: securitate ridicată, cost redus, control mai bun al accesului la date, transparență, management eficient a datelor, partajare rapidă a datelor, autentificarea identității etc.

Opțiuni de îmbunătățire

Există 4 tipuri de implementări de tip blockchain: publice, private, de tip consorțiu sau hibride. Acestea pot fi de tip permissionless (adică fără permisiune) sau permissioned (cu permisiune). Într-un blockchain fără permisiuni, toate nodurile au drepturi egale, în ceea ce privește accesul la date, crearea de tranzacții, validarea tranzacțiilor și producerea de blocuri noi în contrast cu un blockchain cu permisiuni unde nodurile nu au drepturi egale.

Un blockchain public este un blockchain care permite oricui să se alăture. De obicei astfel de blockchain-uri sunt fără permisiune, dar pot fi și cu permisiune. Într-un blockchain public se presupune că majoritatea participanților sunt bine intenționați, realizând astfel o descentralizare ridicată. Cu toate acestea, întrucât este un sistem lipsit de încredere, trebuie să existe un mecanism de apărare (toleranță la defecțiuni bizantine) împotriva actorilor răuvoitori. În funcție de consens, cerința ar putea fi ca un anumit procent, de exemplu mai mult de 50% din noduri, să fie oneste pentru ca blockchain-ul să fie funcțional. Există multe blockchain-uri publice de succes care au fost implementate precum Bitcoin, Ethereum, Litecoin, Bitcoin Cash, Monero, etc.²⁹

Un blockchain privat este un blockchain închis în care confidențialitatea este importantă. Fiecare nod participant este preselecat și verificat. Deoarece este o rețea de încredere, motivația din spatele nodurilor participante nu trebuie să fie neapărat monetară. De obicei, întreprinderile folosesc astfel de blockchain-urile private în scopuri intra business, cu acces limitat la membrii companiei și angajați. Într-un blockchain privat, nu există coliziune, deoarece fiecare validator este cunoscut și are acreditările adecvate pentru a face parte din rețea. În contrast, într-un blockchain public, nu se cunoaște fiecare validator, iar acest lucru crește riscul unei potențiale coliziunii sau a unui atac în proporție de 51%. Cele mai multe dintre lanțuri private sunt cu permisiune, făcându-se o separare foarte clară a atribuțiilor. Exemple de blockchain-urile private includ Hyperledger Fabric, Hyperledger Sawtooth, Quorum, etc.³⁰

Blockchain-urile de tip consorțiu pot fi văzute ca și sub-categorie de blockchain-uri private. Ceea ce le distinge de blockchain-urile private este că ele sunt controlate și guvernate de grupuri și nu de o singură entitate. Blockchain-urile de tip consorțiu (a) oferă un model de utilizare colaborativ în cadrul

²⁹ Dr. M. R. Arun , Prof. M. R. Sheeba, Prof. F. Shabina Fred Rishma, Comparing BlockChain with other Cryptographic Technologies (DAG, Hashgraph, Holochain), International Journal of Computer Engineering in Research Trends Multidisciplinary, Open Access, Peer-Reviewed and fully refereed Research Paper Volume-7, Issue-4,2020.

³⁰ Dr. M. R. Arun , Prof. M. R. Sheeba, Prof. F. Shabina Fred Rishma, Comparing BlockChain with other Cryptographic Technologies (DAG, Hashgraph, Holochain), International Journal of Computer Engineering in Research Trends Multidisciplinary, Open Access, Peer-Reviewed and fully refereed Research Paper Volume-7, Issue-4,2020.

căruia concurenții în afaceri se pot întruni pentru a lucra împreună, precum și pentru a concura unul împotriva celuilalt și (b) promovează eficiența individuală și colectivă, prin colaborările pe care le face posibile³¹.

Blockchain-urile hibride combină de obicei caracteristicile de confidențialitate ale blockchain-urilor private cu caracteristicile de securitate/transparență ale blockchain-urilor publice. Se folosește de flexibilitatea substanțială a companiilor pentru a decide ce date să le facă publice, respectiv pe care să le mențină private. Cu ajutorul unui blockchain hibrid, o companie poate face platforma accesibilă tuturor din lume (printr-un blockchain public), în timp ce un blockchain privat rulează în fundal cu scopul de a controla accesul la modificările și editarea registrelor. Cel mai popular tip de blockchain hibrid este Dragonchain³².

Tabelul de mai jos prezintă o comparație din punct de vedere al avantajelor/dezavantajelor făcută între blockchain-ul public, privat și hibrid.

Tabel 3: Comparație între blockchain-ul public, privat și hibrid³³

	BLOCKCHAIN PUBLIC	BLOCKCHAIN PRIVAT	BLOCKCHAIN HIBRID
AVANTAJE	- Securitate maximă - Deschis pentru toată lumea - Natură anonimă - Nu sunt necesare reglementări - Cu adevărat descentralizat - Asigură transparență completă - Imutabilitate - Putere completă pentru utilizator	- Confidențialitate completă - Tranzacții mai rapide - Scalabil - Acces controlat - Guvernare și control eficiente	- Cost de tranzacție redus - Asigura comunicarea și protecția datelor - Lucrează eficient în ecosisteme închise
DEZAVANTAJE	- Probleme de scalabilitate - Cerințe de stocare greu de realizat - Necesită putere mare de calcul și energie - Lipsa confidențialității în cazul tranzacțiilor	- Lipsă de încredere - Probleme de securitate	

³¹ Dr. M. R. Arun , Prof. M. R. Sheeba, Prof. F. Shabina Fred Rishma, Comparing BlockChain with other Cryptographic Technologies (DAG, Hashgraph, Holochain), International Journal of Computer Engineering in Research Trends Multidisciplinary, Open Access, Peer-Reviewed and fully refereed Research Paper Volume-7, Issue-4,2020.

³² Dr. M. R. Arun , Prof. M. R. Sheeba, Prof. F. Shabina Fred Rishma, Comparing BlockChain with other Cryptographic Technologies (DAG, Hashgraph, Holochain), International Journal of Computer Engineering in Research Trends Multidisciplinary, Open Access, Peer-Reviewed and fully refereed Research Paper Volume-7, Issue-4,2020.

³³ Alammary, A.; Alhazmi, S.; Almasri, M.; Gillani, S. Blockchain-Based Applications in Education: A Systematic Review. *Appl. Sci.* **2019**, *9*, 2400 și Blockchain Training Alliance. Ethereum Developer On Demand with CBDE Exam and retake. <https://blockchaintrainingalliance.com/collections/instructor-led-classes/products/ethereum-developer-training-on-demand>.

	- Riscul de a implementa contracte inteligente cu erori și consecințele ireversibile ale aplicării automate a acestora		
--	--	--	--

O soluție care ar îmbunătăți emiterea/stocarea/verificarea actuală a diplomelor, folosind blockchain, ar fi crearea diplomei sub formă de document digital (PDF), calcularea semnăturii digitale și stocarea acesteia în blockchain. O altă variantă, recomandată, este stocarea doar a semnăturii digitale, care devine astfel imuabilă. Această soluție este mai bună decât cea existentă la momentul actual, deoarece respectă anonimitatea și dreptul la intimitate – datele personal identificatoare nu ajung pe blockchain, de unde nu se mai pot retrage, iar din semnătura digitală nu se pot reconstrui datele personale.

Analiza comparativă

Înainte de compararea soluțiilor blockchain de aplicat, în orice domeniu trebuie analizată potrivirea și simpla necesitate a acestor tehnologii în rezolvarea problemelor identificate. Chiar și digitalizarea – fără blockchain – a sistemului de emitere/verificare diplome este benefică, fără includerea tehnologiilor DLT. Cel puțin timpii de răspuns și costurile pot fi reduse, doar prin digitalizarea, centralizată sau nu, a emiterilor și validărilor de diplome de studii. Desigur, unele instituții educaționale au deja astfel de programe bine testate. Însă, din analiza soluțiilor blockchain existente în alte domenii, respectiv analiza soluțiilor blockchain pentru diplome, existente în țări ale UE și alte regiuni, se poate observa un folos ce depășește investițiile necesare.

Similar cu trecerea accelerată a României peste soluțiile intermediare de acces la Internet și trecerea la fibră optică și viteze gigabit (în curând 10Gbps³⁴ pentru consumatorii casnici), printre primele dintre țările europene, apare oportunitatea de salt peste digitalizarea cu bază de date centralizată, sensibilă la atacuri direcționate, imediat la soluția modernă, bine testată și în special imuabilă, a stocării pe blockchain. Acest aspect este susținut și de inițiativa similară EBSI, promovând interoperabilitatea diplomelor de studii la nivel european.

Tabelul de mai jos prezintă o analiză comparativă între diferite platforme care permit dezvoltarea de aplicații bazate pe blockchain și care pot fi folosite pentru implementarea unei soluții bazate pe blockchain pentru eliberarea și urmărirea certificatelor, diplomelor și altor documente în domeniul educației³⁵.

Tabel 4: Comparație între platforme blockchain disponibile

³⁴ Digi România. DIGI lansează internetul de 10 Gbps, 2021, <https://www.digi.ro/anunturi/digi-lanseaza-internetul-de-10-gbps-fiberlink-10-g-cel-mai-rapid-internet-din-romania-29465>.

³⁵ Blockchain Training Alliance. Ethereum Developer On Demand with CBDE Exam and retake. <https://blockchaintrainingalliance.com/collections/instructor-led-classes/products/ethereum-developer-training-on-demand>.

	Orientat pe industrie	Tip	Algoritm de consens	Contracte inteligente	Guvernare	Limbaj de programare
Ethereum	Cross - Industry	ambele (public& privat)	Proof-of work	da	Ethereum	Solidity, Vyper
Hyperledger Fabric	Cross – Industry	privat	framework conectabil	da	Linux	Golang, JAVA
R3 Corda	Servicii financiare	privat	framework conectabil	da	R3 Consortium	Kotlin
Ripple	Servicii financiare	privat	vot probabilistic	nu	Ripple Labs	C++ JavaScript
Quorum	Cross – Industry	privat	vot majoritar	nu	Ethereum & JP Morgan Chase	Java, Kotlin
Hyperledger Saw tooth	Cross – Industry	privat	framework conectabil	da	Linux	Python, C++, Go, Java, JS
EOS	Cross – Industry	privat	Delegated Proof-of-Stake	da	EOSIO Core Arbitration Forum	C++, Web Assembly
Hyper ledger Iroha	Cross - Industry	privat	Tolerant la erori bizantine pe bază de lanț	da	Linux	C++
Stellar	Servicii financiare	ambele (public& privat)	Protocolul de consens stelar	da	Stellar Foundation	C++, Go, Java, JS, Python, Ruby

Selectarea unei platforme blockchain pentru dezvoltarea de aplicații în domeniul educațional depinde de o serie de aspecte tehnice care trebuie luate în considerare și anume: tipul platformei (ex. publică/privată), cerințele hardware specifice (de exemplu, procesoare SGX activate), tipul de algoritm de consens (de exemplu Ethereum folosește un algoritm de consens care consumă cantitate mare de energie pentru efectuarea calculelor criptografice), costurile privind adoptarea și implementarea tehnologiei blockchain în dezvoltarea soluției propuse.

Concluzia la care s-a ajuns pe baza analizei platformelor blockchain disponibile, a fost că Hyperledger Fabric poate fi văzut ca și o alegere viabilă în ceea ce privește implementarea unei soluții bazate pe blockchain pentru eliberarea și urmărirea certificatelor, diplomelor și altor

documente în domeniul educației. Motivele sunt următoarele³⁶:

- Oferă soluții de registru distribuit pe rețele private.
- Are o arhitectura modulară ceea ce maximizează flexibilitatea; în Hyperledger Fabric, putem schimba consensul, tipurile de registru, putem adăuga noi funcționalități, etc.
- Oferă suport pentru protejarea și gestionarea cheilor digitale.
- Este conceput pentru rețelele de tip permissionless, ceea ce înseamnă că doar participanții autorizați pot accesa rețeaua.
- Tranzacțiile care au loc în rețea sunt vizibile doar pentru membrii autorizați.
- Este open-source (oricine poate folosi platforma în beneficiul companiei sale).
- Eficientă mai ridicată în comparație cu alte blockchain-uri.
- Potrivit pentru o serie largă de aplicații (ex. aplicații în domeniul medical, lanțul de aprovizionare, asigurările, mass-media, securitatea cibernetică, IoT, bancar, guvern, imobiliare etc.).
- Cod de calitate.

Constrângeri privind implementarea

Constrângerile privind implementarea unei soluții bazate pe blockchain pentru eliberarea și urmărirea certificatelor, diplomelor și altor documente în domeniul educației sunt³⁷:

- Lipsă voință administrativă;
- Lipsa unui cadru legal clar;
- Problema diplomelor pre-existente implementării sistemului:
 - Digitizarea și înregistrarea pe blockchain presupune un efort birocratic semnificativ, în primul rând pentru găsirea și identificarea documentelor;
 - Ne-digitizarea diplomelor vechi necesită păstrarea, în paralel, a sistemului vechi, a infrastructurii și a personalului format pentru procedura de verificare a diplomelor, pentru toată perioada în care titularii ar avea nevoie de ele.
- Lipsa finanțării pentru dezvoltarea unei soluții bazate pe tehnologia blockchain;
- Costurile suplimentare pe care le implică folosirea tehnologiei blockchain: costul energiei de calcul, costul schimbării infrastructurii actuale, costul de timp din cauza tranzacțiilor lente și costul de gestionare a volumelor mari de date;

³⁶ Kumutha K, S. Jayalakshmi, The Impact of the Blockchain on Academic Certificate Verification System-Review, EAI Endorsed Transactions on Energy Web, April 2021, <http://dx.doi.org/10.4108/eai.29-4-2021.169426> și Gwyneth Iredale. Hyperledger Fabric Vs Ethereum: Head-To-Head Battle. <https://101blockchains.com/ethereum-vs-hyperledger-fabric/>.

³⁷ Alammary, A.; Alhazmi, S.; Almasri, M.; Gillani, S. Blockchain-Based Applications in Education: A Systematic Review. *Appl. Sci.* **2019**, *9*, 2400 și Mara-Florina Steiu. Blockchain in education: Opportunities, applications, and challenges. <https://firstmonday.org/ojs/index.php/fm/article/view/10654/9726>.

- Nevoia de personal calificat pentru dezvoltare unei soluții bazate pe blockchain, mentenanță, integrarea cu aplicațiile/soluțiile existente nevoia de dezvoltare profesională continuă și recalificare a forței de muncă;
- Reticența instituțiilor de învățământ în ceea ce privește partajarea datelor într-o rețea blockchain;
- Dificultatea instituțiilor de învățământ în a decide ce date / servicii să fie oferite prin intermediul rețelei blockchain;
- Imuabilitate datelor asigurată de tehnologia blockchain care face dificil pentru instituțiile de învățământ să corecteze date inexacte;
- Reticența instituțiilor de învățământ în ceea ce privește plasarea gestionării datelor în mâinile utilizatorilor ceea ce ar putea conduce la situații în care datele sunt indisponibile, afectând astfel aplicațiile care depind de ele;
- Lipsa cunoștințelor și abilităților necesare din partea personalului emitent în ceea ce privește gestionarea datelor studenților pe o platformă blockchain;
- Lipsa unei cereri reale din partea angajatorilor pentru adoptarea unei soluții bazate pe tehnologia blockchain în educație. Chiar dacă angajatorii recunosc importanța validării competențelor și a acreditărilor prin blockchain, adesea le lipsește expertiza, infrastructura și finanțarea necesare pentru a modifica practicile de recrutare și a integra noi aplicații;
- Nevoia de formare profesională a personalului emitent diplome.

Resurse tehnice pentru implementare

Resursele tehnice constă în hardware și software necesar pentru sistemul blockchain propriu-zis, cât și resursele de a-l menține în funcțiune și de a-l utiliza la capacitate optimă după implementare. De asemenea, utilizatorii (emitenți și verificatori de diplome) au nevoie de uneltele necesare pentru exploatarea eficientă a sistemului.

Resursele tehnice necesare:

- Resurse pentru proiectarea, dezvoltarea și testarea experimentală a soluției
 - Partea server (hardware/software server și platforme de dezvoltare)
 - Consumatori
 - Aplicații pentru înregistrare date în blockchain (desktop/web/mobil)
 - Aplicații pentru verificare a datelor/validare diplome: (desktop/web/mobil)
- Resurse pentru funcționarea propriu-zisă:
 - Noduri blockchain (serve)re
 - Infrastructura de alimentare și interconectare a nodurilor
 - Mentenanță noduri
 - Mentenanță aplicații consumator
 - Înregistrare

- Verificare
- Necesități tehnice pentru formarea resursei umane implicate
 - Pre-implementare: hardware/software pentru specialiști implementare
 - Pentru sistem server blockchain
 - Pentru aplicațiile client
 - Post-implementare
 - Hardware/software/material formator pentru specialiști mentenanță
 - Hardware/software/material formator pentru utilizatori
 - Emitere și înregistrare diplome
 - Verificare diplome.

Resurse umane pentru implementare

Resursa umană necesară implementării se poate împărți în trei categorii:

- Dezvoltatori ai sistemului
- Specialiști de mentenanță
- Personal utilizator

Dezvoltatorii sistemului trebuie să creeze atât partea de server „back-end” (nodurile și interconectarea lor în blockchain), cât și aplicație(-ii) „front-end” capabile să înregistreze pe blockchain noile diplome emise. Pe lângă acestea, este nevoie și de aplicație(-ii) verificatoare de diplome – dacă nu aplicație publică, ca oricine să poată verifica oricare diplomă, atunci cel puțin pusă la dispoziția firmelor-angajator și altor organizații cu nevoia de validare a diplomelor pe care le primesc ca dovadă de la persoane care se declară absolvenți.

Deși România are o bază bogată de dezvoltatori IT, tehnologia blockchain și sistemele conexe sunt relativ noi chiar și pentru această resursă umană. Totuși, există material didactic și programe internaționale de formare pentru acest domeniu, limba engleză sau accesul la material nepunând o problemă, chiar dacă costurile certificărilor sunt relativ ridicate. Mai mult, se preconizează includerea materialului teoretic și practic despre DLT și blockchain în cursurile din planurile de învățământ românești, ceea ce înseamnă și creșterea numărului local de formatori în domeniu.

Dezvoltatorii blockchain au nevoie de aptitudini³⁸ în:

- Programare
- Criptografie
- Structuri de date și stocare distribuită

³⁸ Toshendra Kumar Sharma. 5 Skill Sets a Blockchain Developer Must Have. <https://www.blockchain-council.org/blockchain/5-skill-sets-a-blockchain-developer-must-have/> și Robert Sheldon. 6 must-have blockchain developer skills. <https://whatistechtarget.com/feature/6-must-have-blockchain-developer-skills>.

- Arhitecturi software
- Aplicații web
- Contracte inteligente
- Interoperabilitate.

Dacă API-ul (interfața de programare aplicație) sistemului server este dezvoltat corect, atunci dezvoltatorii aplicațiilor client (emitere/verificare diplome) nu au nevoie de multe cunoștințe blockchain, sau chiar deloc. Eliminarea acestei cerințe lărgeste bazinul de experți din care se pot alege dezvoltatorii aplicațiilor client, fie ele de tip desktop, web sau mobil, atât din domeniul public, cât și cel privat.

Specialiștii de mentenanță trebuie să se ocupe de trei aspecte principale: păstrarea în funcțiune a hardware-ului și software-ului peste care rulează sistemul blockchain, păstrarea în funcțiune și eventual extinderea/scalarea părții software caracteristic sistemului blockchain, și menținerea în funcțiune a aplicațiilor client (emitere/verificare diplome).

Pentru mentenanța părții de server și rețea, care constituie suportul de sub sistemul blockchain, există specialiști bine pregătiți, cu experiență, care gestionează astfel de sisteme chiar și acum, pentru diverse soluții software. Un sistem blockchain nu are cerințe hardware/software subiacente mult diferite de alte sisteme software distribuite similare. La fel, mentenanța aplicațiilor client, fie ele pentru emiterea sau pentru verificarea diplomelor, nu pune probleme dezvoltatorilor români.

Mentenanța sistemului blockchain propriu-zis cere specialiști în domeniu. Chiar dacă puțin diferite de cele pentru dezvoltarea sistemului, acești experți trebuie să posede abilități specifice DLT și blockchain (criptografie, stocare distribuită, desigur DLT, dar și alte domenii relevante). Numărul experților în acest domeniu, cum s-a menționat și mai sus, este mai mic decât pentru tehnologii mai vechi, însă este în creștere.

Personalul utilizator, care se ocupă de emiterea și înregistrarea diplomelor pe blockchain, respectiv care verifică validitatea unor diplome prezentate de un candidat (pentru angajare, echivalare sau continuare studii, sau alt scop), sunt utilizatorii finali ai sistemului propus.

Unul din obiectivele dezvoltării aplicațiilor client este transparentizarea accesului la blockchain care stă la baza lor, astfel încât să se asigure ușurința în utilizare. În acest fel, cei care gestionează emiterea diplomelor și înregistrarea lor în sistem (pe blockchain) pot fi persoanele deja angajate în cadrul departamentelor „Acte de studii” ale instituțiilor educaționale și de formare profesională, iar cei care verifică diplomele pot fi persoanele de la „Personal” sau „Resurse umane”, care oricum verifică deja eligibilitatea candidaților și actele lor.

Resurse financiare pentru implementare

Resursele financiare sunt dependente de necesarul de resurse tehnice și umane. Tabelul de mai jos prezintă componentele de cost principale asociate implementării soluției propuse.

Tabel 5: Detaliere resurse financiare pentru implementare

Tip cost	Necesar estimat	Suma estimată	Observații
Costuri dezvoltare software	Salariu mediu lunar brut dezvoltator software ³⁹ . Calculator, periferice, software, electricitate, Internet, spațiu birou/home office.	13586 RON (85 RON/h) per dezvoltator, posibil mai ridicat, datorită tehnologiei noi și a deficitului de specialiști în domeniul blockchain.	În funcție de organizație, locație, beneficii, necesar număr de dezvoltatori. Pentru dezvoltatori deja angajați, costurile operaționale se rezumă la salariu.
Costuri inițiale hardware	Server: 10 bucăți, câte două per locație (cu echilibrare de sarcină). Stocare online: 1TB/server, în configurație RAID cu disponibilitate ridicată. Stocare offline (copii de rezervă): discuri hot-swap sau	Server cu discuri în RAID incluse: 70000 RON/server ⁴⁰ , 700000 RON/10 servere. Stocare offline pe cartușe LTO-9 ⁴¹ : 722 RON/cartuș (16 RON/TB), 17000 RON/unitate de scriere/citire (estimare 2022).	Câte 2 servere per universitate de vârf, în locații diferite. Se stochează doar identicatorii datelor, nu diplomele în sine, deoarece conțin date personal identificatoare. Se recomandă câteva servere la locații non-Minister. În cazul stocării hash+detalii valabilitate diplomă, se recomandă 2TB stocare/server.

³⁹ Institutul Național de Statistică. Câștigul salarial mediu lunar. <https://insse.ro/cms/ro/content/c%C3%A2%C8%99tigul-salarial-mediulunar-78>.

⁴⁰ DELL. PowerEdge R750 Rack Server. https://www.dell.com/en-us/work/shop/servers-storage-and-networking/poweredge-r750-rack-server/spd/poweredge-r750/pe_r750_tm_vi_vpsb?view=configurations&configurationid=55c6be4e-c931-49b0-ad82-d7c472eba2e5.

⁴¹ Tom Coughlin. LTO-9 Tape Products Now Available. <https://www.forbes.com/sites/tomcoughlin/2021/09/15/lto-9-tape-products-now-available/> și TapeAndMedia. IBM LTO Ultrium 9 Tape with Barium Ferrite. <https://tapeandmedia.com/ibm-lto-9-tape-with-barium-ferrite-bafe-02XW568/>.

Tip cost	Necesar estimat	Suma estimată	Observații
	unități de bandă LTO. Conectivitate rețea: abonament RoEduNet existent pentru instituții educaționale, sau abonament de bandă largă și disponibilitate ridicată.	Conectivitate Internet, fibră optică 10Gbps: 50-100 RON/lună (preconizat 2022).	Viteza de generare blocuri/verificare nu este critică, deoarece diplomele nu sunt generate/verificate frecvent.
Costuri inițiale software	Sistem de operare: open-source/gratuit (Linux/BSD). Software blockchain: open-source/gratuit. Software gestiune server/sistem de operare/blockchain: open-source/gratuit.	Sistem de operare: 0 RON Software: 0 RON.	Posibil variante de sisteme de operare „enterprise” cu suport contra cost. Exemplu costuri serviciu implementare HyperLedger, oferit de IBM, pentru proces publicare diplome: 250k EUR (doar serviciul, fără costuri hardware sau software).
Costuri operaționale/mentenanță	Soft, hard, sysadmin, specialist blockchain. Electricitate server x 10. Costuri adiționale (clădire, administrație, altele).	Salariu brut lunar administrator de sistem: 13586 RON (85 RON/h). Salariu brut lunar specialist blockchain: 13586 RON (85 RON/h). Electricitate server: 500 RON/server/lună,	Recomandat instanțe Docker, preferabil pe aceeași mașină fizică, pentru scalabilitate. S-a analizat costurile și dependabilitatea propriei rețele de servere fizice, versus dependabilitatea unei soluții IaaS („Infrastructure as a Service”, servere virtuale găzduite în cloud

Tip cost	Necesar estimat	Suma estimată	Observații
		5000 RON/lună/zece servere. Depanarea/înlocui rea componentelor care se defectează: în medie aproximativ 5% din costul lunar de funcționare.	Amazon/Google/Microsoft /alți furnizori). Deși dependabilitatea hardware și disponibilitatea garantată de marii furnizori cloud este mai ridicată decât cea a serverelor proprii ale instituțiilor ne-specializate pe găzduire servicii software din România, importanța datelor stocate și necesitatea de disponibilitate pe termen lung a lor contrabalansează comoditatea mutării soluției în cloud.
Costuri pregătire specialiști de dezvoltare/mentenanță	Cel puțin un specialist de mentenanță per locație.	La universități publice din România: 0 RON Curs și examen „Certified Hyperledger Fabric Developer (CHFD)” ⁴² : 2516 RON/dezvoltator. Curs și examen „Ethereum Developer On Demand with Certified Blockchain Developer- Ethereum Exam	Gratuit, în cadrul unor programe lansate de universități de vârf din țară. Se recomandă integrarea în planurile de învățământ ale unor cursuri existente sau dezvoltarea unor cursuri noi. Contra cost, în cadrul unor instituții de formare profesională românești sau străine.

⁴² The Linux Foundation. Certified Hyperledger Fabric Developer.
<https://training.linuxfoundation.org/certification/certified-hyperledger-fabric-developer/>.

Tip cost	Necesar estimat	Suma estimată	Observații
		(CBDE) ⁴³ : 2400 RON/dezvoltator.	
Costuri pregătire utilizatori: - membri birouri "Acte de Studii" ale instituțiilor emitente de diplome; - membri birouri „Resurse umane” ale firmelor angajatoare.	Cel puțin un utilizator cu pregătire în domeniu, per birou.	Creare și diseminare materiale instructionale online: 1000 RON.	Se recomandă lansarea unor programe de conștientizare și formare, din partea Ministerului Educației/ Autoritatea pentru Digitalizarea României /Ministerul Muncii.

Resurse logistice pentru implementare

Cerințele logistice ale sistemului propus rezultă atât din caracteristica distribuită a sistemelor blockchain, cât și a scopului acestui sistem, care implică actori diferiți – instituții educaționale, angajatori publici și privați, entități europene.

Necesarul de coordonare administrativă și interoperare tehnică între organizațiile participante este o noutate relativă, conexiuni de rețea și dialog existând deja între majoritatea actorilor.

Adițional, formarea personalului pentru utilizarea aplicațiilor client – emitenți de diplome și verficatori de diplome – necesită organizarea de cursuri dedicate, și/sau dezvoltarea și diseminarea de materiale de training/manuale de utilizare corespunzătoare.

Riscuri și planuri de contingență

Riscurile datorate adoptării unei soluții bazate pe blockchain pentru eliberarea și urmărirea certificatelor, diplomelor și altor documente în domeniul educației pot fi clasificate conform categoriilor de mai jos.

⁴³ Blockchain Training Alliance. Ethereum Developer On Demand with CBDE Exam and retake.
<https://blockchaintrainingalliance.com/collections/instructor-led-classes/products/ethereum-developer-training-on-demand>.

Legendă:

Probabilitate de apariție: **1** - aproape sigur (frecvent), **2** – posibil (periodic), **3** – distant (rar).

Magnitudinea consecințelor: **A** - sever (difícil de gestionat), **B** - moderat (gestionabil), **C** - neglijabil (fără probleme).

Detectabilitate: **<** - ușor (repede), **^** - cunoscut (din timp), **>** - greu (târziu).

Prioritățile sunt ordonate de la maxim în jos spre minim, în cadrul fiecărei categorii.

Tabel 6: Riscuri și planuri de contingență

Prioritate	Risc	Probabilitate	Severitate	Detectabilitate	Plan de contingență / reziliență
1. Riscuri de finanțare					
1.1	Riscuri de interoperabilitate defectuoasă și deficiențe în accesarea diplomelor înregistrate înaintea interconectării	2	B	<	Instituțiile educaționale rezervă resursele necesare pentru implementarea sistemului pentru uz propriu, de jos în sus, pe câteva noduri proprii, urmând apoi interconectarea în clustere de universități, mai apoi la nivel național, european și internațional. Dezvoltarea timpurie a unor soluții de interoperabilitate obișnuită (automată) și a unora de rezervă (în cel mai rău caz cu transpunere supervizată a datelor).
1.2	Riscul de oprire/diminuare a fondurilor pentru implementarea de sus în jos a sistemului propus la nivel național, în oricare fază a sa	2	A	>	Asumarea, de către conducerea la nivel național, a finanțării pe termen mediu (implementare), și pe termen lung (mentenanță). Bugetare instituțională pentru asigurarea fondurilor anuale de susținere a serviciului.
2. Riscuri legislative					
2.1	Riscuri legate de regulile privind confidențialitatea și protecția datelor (GDPR)	3	A	<	Implicarea inițială și continuă a experților tehnici și legali pentru GDPR și dreptul la intimitate.

Prioritate	Risc	Probabilitate	Severitate	Detectabilitate	Plan de contingență / reziliență
					Analiza pre-implementare a pericolului parametric și cuantic (riscul identificării neautorizate a persoanei prin reconstrucție criptografică din amprente digitale ale datelor înregistrate și ale datelor secundare). Soluții de avertizare a persoanei a cărei anonimitate a fost compromisă (controlul daunelor).
2.2	Riscul să nu se accepte încrederea legală, simplificată de utilizarea blockchain	1	B	^	Cadrul legal românesc este deja de partea utilizării documentelor și semnăturii electronice (Legea nr. 455/2001, Legea nr. 187/2012, Regulamentul UE nr. 910/2014, OUG nr. 38/2020, OUG nr. 39/2020, Decretul nr. 195/2020)⁴⁴, astfel că este minim riscul de a nu se legisla soluția întărită cu blockchain. Un alt precedent deja în uz este suportul legal pentru emiterea facturilor în formă electronică (Lege 260/2007), și noul proiect de reglementare a acestei activități la nivel național (proiectul e-Factura din 2021)⁴⁵.

⁴⁴ Valeriu Mina, Andreea Amorăritei, Utilizarea semnăturii electronice în relațiile cu autoritățile și instituțiile publice, <https://www.lexology.com/library/detail.aspx?g=9f3bbff5-6288-4424-ad99-76bedb1d3288>; Andreea-Maria Maxim. Scurte considerații privind semnătura electronică, <https://www.juridice.ro/680239/scurte-consideratii-privind-semnatura-electronica.html> și *, Normele tehnice și metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică, <https://www.certsig.ro/ro/depozitar/legislatie/norme-aplicare-lege-semnatura-electronica/>.

⁴⁵ Parlamentul României. Înregistrarea operațiunilor comerciale prin mijloace electronice, https://static.anaf.ro/static/10/Anaf/legislatie/L_260_2007.pdf și Guvernul României. Administrarea, funcționarea și implementarea sistemului național privind factura electronică RO e-Factura și factura electronică în România,

Prioritate	Risc	Probabilitate	Severitate	Detectabilitate	Plan de contingență / reziliență
					Totuși, în cazul dezvoltării întârziate a cadrului legal, se poate menține emiterea/verificarea tradițională a diplomelor, ca soluția cu fundament legal, dar mergând, în paralel, și cu soluția nouă, pe blockchain, ca în momentul aprobării validității legale a soluției, trecerea să se facă ușor.
2.3	Lipsa unei autorități legale de regularizare/legiferare utilizare blockchain	1	B	^	Stabilirea unui for competent cu drepturi legale, care să clarifice, reglementeze și să susțină utilizarea blockchain pentru emiterea/verificarea diplomelor de studii. Inițial, se poate trece din experimental în producție – internă, în cadrul instituției –, dar și aici, este necesar un departament sau consiliu care să reglementeze utilizarea soluției.
2.4	Imposibilitatea de a corecta/actualiza date (imuabilitatea datelor)	1	B	<	Cazurile de retragere/anulare a unei diplome sunt rare și, cum procesul de digitalizare în general și tocmai sistemul propus, în particular, crește transparența și trasabilitatea diplomelor, aceste cazuri se vor rări și mai mult, deși nu vor dispărea complet. De aceea, resursele alocate pentru această operațiune pot fi menținute la minim. Însă, trebuie să existe o procedură clară pentru implementarea operațiunii.

Prioritate	Risc	Probabilitate	Severitate	Detectabilitate	Plan de contingență / reziliență
					Deja din timpul proiectării structurii blocurilor și a datelor înregistrate, trebuie găsită o soluție care permite invalidarea unor blocuri sau a unor date din ele. Nu schimbarea datelor – asta ar contraveni avantajului major de imuabilitate a blockchain – ci păstrarea originalului și marcarea sa ca invalid. Există soluții cu blockchain-uri „redactabile”⁴⁶, în care este posibilă modificarea unor date, dare de regulă, ele sunt complexe, cu soluții criptologice particularizate, în plus scade performanța și securitatea. Pornind de la faptul că anularea unei diplome este un eveniment rar, se poate crea o bază de date secundară, care să conțină toate diplomele retrase. Pentru siguranță sporită, aceste înregistrări de anulare se pot stoca, și ele, într-un blockchain secundar. La fiecare verificare de diplomă, prima dată se verifică posibila invaliditate în lista diplomelor invalide, doar la lipsa acestei înregistrări se trece la validarea în blockchain-ul mare, care merge mai încet.

⁴⁶ Yakob Mesengiser, Natalia Miloslavskaya. Problems of Using Redactable Blockchain Technology, 2021, DOI 10.1016/j.procs.2021.06.068; Giuseppe Ateniese et al. Redactable Blockchain – or – Rewriting History in Bitcoin and Friends, 2017, DOI 10.1109/EuroSP.2017.37 și Damiano Sartori. Redactable Blockchain : How to Change the Immutable and the Consequences of Doing So, 2020, <http://purl.utwente.nl/essays/82755>.

Prioritate	Risc	Probabilitate	Severitate	Detectabilitate	Plan de contingență / reziliență
					O soluție similară practică organizatorii de conferințe sau editorii unor reviste, pentru autorii de lucrări științifice, pentru refuzarea autorilor cunoscuți plagiatori sau din alte motive ⁴⁷ .
3. Riscuri ale costurilor de întreținere					
3.1	Încetarea finanțării susținute pe termen lung	2	B	^	Asumarea, de către conducerea la nivel național, a finanțării pe termen mediu (implementare), și pe termen lung (mentenanță). Bugetare instituțională pentru asigurarea fondurilor anuale de susținere a serviciului.
4. Riscuri de ocupare					
4.1	Posibilitatea lipsei de specialiști	3	A	>	Materialul de formare asigură un flux adecvat de experți, iar noutatea tehnologiei blockchain și posibilitatea dobândirii de experiență în acest domeniu în dezvoltare, într-un proiect național, regional sau european, este atractiv pentru experții din domeniu. În cazul lipsei de specialiști pentru dezvoltări ale sistemului sau îmbunătățirii sale cu tehnologii curente, se poate menține sistemul funcțional, cu tehnologia testat funcțională. În cazul lipsei de personal pentru mentenanță, se pot contacta specialiștii existenți, desigur cu remunerație corespunzătoare.

⁴⁷ Bill Hagen, Tony VenGraitis. Appropriate Use of the IEEE Prohibited Authors List, 2015, https://www.ieee.org/content/dam/ieee-org/ieee/web/org/pubs/appropriate_use_of_pal.pdf.

Prioritate	Risc	Probabilitate	Severitate	Detectabilitate	Plan de contingență / reziliență
					În caz de probleme, se poate apela la specialiști străini, cu cunoștințe în domeniu, desigur după completarea documentației necesare. Pe termen lung, se recomandă crearea unui cadru legal, legislativ, care să încurajeze utilizarea tehnologiilor blockchain în general, atât în domeniul public, cât și cel privat. De asemenea, este imperativă includerea acestor tehnologii în programa educațională, pe cât mai multe nivele, atât pentru viitorii dezvoltatori, dar și pentru personalul de întreținere și de utilizare.
4.2	Utilizare sub așteptări a sistemului	2	C	^	Poate fi contracarat pe de o parte prin diseminarea informațiilor despre avantajele sistemului, în cadrul factorilor decizionali și al personalului utilizator, iar pe de altă parte, cu impunerea, la nivel național, a testării și adoptării sistemului până la un termen limită. Se preconizează ca, poate nu în termenul estimat, dar mai devreme sau mai târziu instituțiile emitente și angajatorii vor realiza utilitatea sistemului propus.
5. Riscuri operaționale					
5.1	Probleme de securitate	3	A	^	Stabilirea, din timp și detaliat, a politicilor de acces și de securitate a datelor.

Prioritate	Risc	Probabilitate	Severitate	Detectabilitate	Plan de contingență / reziliență
					Punerea la punct a unor proceduri de creare copii de rezervă offline, pentru date. Proiectarea soluțiilor de consens astfel ca introducerea de date alterate să fie îngreunată. Audit periodic a nivelului de sănătate sistem și procese.
5.2	Probleme de scalabilitate	2	B	^	Alegerea/proiectarea, de la început, a unei platforme blockchain care permite expansiune ulterioară, în special ca număr de noduri, stocare, putere de procesare. Proiectarea optimizată a proceselor software, în special tokenizare, consens, sincronizare, pentru utilizare cât mai eficientă a resurselor hardware. Alocarea de fonduri pentru achiziția, pregătirea și adăugarea unor noduri noi, în funcție de necesități. Pregătirea și asigurarea disponibilității de fonduri și specialiști pentru extinderea dinamică a sistemului, în instanțe în cloud-uri comerciale.
5.3	Întreruperea serviciilor (energie, conectivitate)	1	A	<	Asigurarea alimentării redundante cu energie și a conectivității multicanal, verificarea periodică a stării soluțiilor redundante.
5.4	În cazul folosirii unei metode de consens „Proof-of-Work”,	1	A	<	Proiectarea sistemului cu posibilitatea utilizării algoritmilor de consens

Prioritate	Risc	Probabilitate	Severitate	Detectabilitate	Plan de contingență / reziliență
	consum ridicat de energie și afectarea mediului				multipli sau cel puțin unul mai prietenos cu mediul, decât PoW. Delegarea procesării PoW spre echipament optimizat și dedicat acestui scop, previzionat în bugetare.
5.5	Probleme de disponibilitate (hard/soft/specialiști)	3	B	<	Bugetare de fonduri de contingență, pentru menținerea fluxului de implementare și disponibilității sistemului, și pentru mentenanță în caz de avarii peste cele normal estimate. Estimarea și implementarea necesarului de noduri descentralizate, pentru prevenirea întreruperilor în serviciu. Proiectarea, verificarea periodică și menținerea gata de lansare a unor noduri de rezervă, în cloud comercial contra cost sau pe echipamente de putere mai mică dar mai ieftine, pentru funcționare în mod de avarie a serviciului (timp de răspuns crescut, dar finit).
5.6	Formarea a unui număr prea mic de specialiști și personal	2	C	>	Construirea unei rețele de specialiști și menținerea lor la zi cu starea curentă a sistemului, ca să poată interveni în termen scurt, la cererea instituțiilor operatoare. Pregătirea formatorilor de formatori, crearea și introducerea materialului didactic aferent în programa școlară de la cât mai multe nivele educaționale.

Prioritate	Risc	Probabilitate	Severitate	Detectabilitate	Plan de contingență / reziliență
					Alocarea de resurse pentru programe de training de utilizare a aplicațiilor client ale sistemului.
6. Riscuri de planificare					
6.1	Depășire fonduri, termene limită	2	A	^	Monitorizare și control periodic și susținut, pe toată durata implementării și utilizării soluției.
6.2	Volatilitatea resursei materiale și a celei umane	3	B	>	Proiectarea sistemului cu resurse adiționale, redundante, atât materiale cât și umane. Bugetare pentru soluții de rezervă – hardware, specialiști, personal. Posibilă deschidere a aplicațiilor software client de verificare diplome, spre publicul larg – democratizarea verificării actelor.
7. Riscuri de schimbare a opțiunilor politice (riscuri decizionale)					
7.1	Încetarea susținerii pe termen lung	1	B	>	Asumarea, de către conducerea la nivel național, a politicilor pozitive pe termen mediu (implementare), și pe termen lung (mentenanță), indiferent de spectrul politic. Garantare voință instituțională pentru asigurarea fondurilor anuale de susținere a serviciului.
7.2	Schimbarea climatului politic favorabil pentru implementare și extindere	2	A	>	Pregătirea materialelor explicative, pentru factorii decizionali. Exemple convingătoare, din sisteme străine similare de succes, și rezultate pozitive naționale. Lobby susținut și periodic.
8. Riscuri legate de procedurile de achiziții publice					

Prioritate	Risc	Probabilitate	Severitate	Detectabilitate	Plan de contingență / reziliență
8.1	Nerespectarea regulamentelor	3	A	^	Monitorizare și control periodic și susținut, pe toată durata implementării și utilizării soluției. Implicarea unor specialiști în legislație, pentru consiliere și audit.
8.2	Furnizori care câștigă licitațiile, dar nu respectă cerințele din fișele tehnice hardware/software sau termenele de livrare și punere în funcțiune	3	C	^	Implicarea unor specialiști în achiziții publice, pentru conceperea și legalizarea contractelor. Pregătirea actelor și a proceselor de achiziție, incluzând soluții și furnizori de rezervă, în condițiile legii.
8.3	Firme care se retrag sau ajung în imposibilitatea de respectare a contractului	2	B	<	Pregătirea actelor și a proceselor de achiziție, incluzând soluții și furnizori de rezervă, în condițiile legii.
9. Riscuri legate de acuratețea informațiilor					
9.1	Imutabilitatea neagă posibilitatea de remediere	1	B	<	Digitalizarea – în curs – a proceselor de colectare a datelor, dar adițional, îmbunătățirea interfețelor grafice ale utilizatorilor-personal care pregătesc datele pentru tokenizare și înregistrare în blockchain. Limitarea variantelor de date care se pot introduce. Filtrarea lor contextuală. Conceperea și implementarea unor contracte inteligente care să valideze datele, înainte de imortalizarea lor în blockchain. Programe de conștientizare a importanței „first time right”, a calității la prima încercare, în rândul personalului care va înregistra diplomele pe blockchain.

Prioritate	Risc	Probabilitate	Severitate	Detectabilitate	Plan de contingență / reziliență
					Apare un risc adițional, care trebuie și poate fi evitat: câștigul de scurtare a lanțurilor ierarhice actuale pentru avizarea unor documente și procese, câștig ce se datorează creșterii democratizate a încrederii prin imuabilitatea datelor într-un blockchain, poate fi anulat de apariția necesității ca un for superior să aprobe datele pregătite pentru înregistrare în blockchain, deoarece ele nu vor mai putea fi schimbate. Cu pregătirea adecvată a personalului, înțelegerea corectă a importanței corectitudinii datelor, dar și prin dezvoltarea unor verificări automate adiționale asupra corectitudinii datelor, se poate păstra avantajul ce se naște din încrederea oferită de blockchain.
10. Riscuri reputaționale (influența opiniei publice)					
10.1	Neglijarea importanței diseminării soluțiilor noi, a pregătirii corecte a utilizatorilor	3	A	>	Se impune studiul grupurilor demografice care vor utiliza sistemul propus. În funcție de nivelul de cunoștințe și abilități specifice estimat, trebuie dezvoltate din timp materiale didactice, cursuri, formatori. De asemenea, nu doar pregătirea inițială a bazei de utilizatori este importantă, ci și îmbunătățirea sistemului de training, și adaptarea sa la tehnologiile noi, în sincron cu starea curentă a sistemului. Adițional, trebuie conștientizat publicul larg despre tehnologiile de bază și serviciile noi sau îmbunătățite.

Prioritate	Risc	Probabilitate	Severitate	Detectabilitate	Plan de contingență / reziliență
11. Riscuri de estimare a valorilor reziduale ale bunurilor					
11.1	Neglijarea uzurii fizice și morale a resurselor hardware/software	2	B	>	Deși sistemul blockchain are dependabilitate ridicată prin caracterul său descentralizat și replicat, nu trebuie neglijată importanța datelor stocate (diplome care acordă drepturi legale) și importanța disponibilității accesului la aceste date (înregistrare și verificare diplome). Echipamentele folosite, în special serverele pe care rulează nodurile, trebuie menținute în condiție bună și schimbate când li se termină durata de viață estimată de producător, înainte de expirarea timpului mediu de funcționare (MTBF) și defectarea propriu-zisă, pentru a le fi asigurată disponibilitatea continuă sau o „degradare grațioasă”, nu una dezastruoasă.
11.2	Neglijarea uzurii morale a materialului de formare	2	A	>	Documentația și materialele de instruire pentru specialiștii de mentenanță servere și blockchain, pentru dezvoltatorii aplicațiilor client, pentru personalul utilizator, precum și materialul pentru formatorii de formatori, poate deveni învechit în timp, neconform cu realitățile din sistemul educațional și al muncii. De aceea, aceste materiale trebuie evaluate periodic și reîmprospătate cu tehnologiile de suport actuale, păstrând compatibilitatea cu sistemul existent, în funcțiune.
12. Riscuri ale schimbărilor tehnologice					
12.1	Neglijarea continuității serviciului și a	3	A	>	Acesta este un risc aparte în cazul de față, deoarece toate înregistrările

Prioritate	Risc	Probabilitate	Severitate	Detectabilitate	Plan de contingență / reziliență
	interoperabilității, pe termen lung				începând cu blocul geneză (conținând înregistrarea inițială) din blockchain trebuie să fie inteligibile și autentificabile, pe întreaga perioadă de existență a blockchain-ului, care înseamnă decenii sau mai mult. Soluția posibilă constă în dezvoltarea de specificații detaliate ale stocării datelor și scrierii/citirii lor, a arhitecturii sistemului, a interfeței de acces, independente de tehnologia de implementare. O soluție adițională este înnoirea periodică a aplicațiilor server și client, a aplicațiilor, a materialului de instruire, cu tehnologii noi și testate, dar cu păstrarea datelor din sistem și a sistemului în funcțiune.
13. Riscuri ale volumului de activitate estimat					
13.1	Subestimarea necesarului de creștere a sistemului suport	3	C	^	Se impune dezvoltarea sistemului și a aplicațiilor suport în așa fel, încât să fie asigurată scalabilitatea și extensibilitatea sistemului, cu investiție viitoare rezonabilă, de resurse.

Relativ la **apetitul la risc** și **toleranța la risc**⁴⁸, se recomandă prudență. Deși cei doi indicatori variază în funcție de categoria de risc și instituție, este mai adecvat să se proiecteze o implementare sigură, cu variantă experimentală de jos în sus, dar cu reglementări de sus în jos care să clarifice calea de urmat și să asigure interoperabilitatea viitoare. Datorită faptului că este vorba de date și servicii care trebuie menținute pe termen foarte lung, tehnologiile și serviciile implicate trebuie bine puse la punct, pentru dăinuire.

⁴⁸ International Organization for Standardization. ISO 31000 Risk Management, 2021, <https://www.iso.org/iso-31000-risk-management.html> ; International Organization for Standardization. ISO Guide 73:2009 Risk management — Vocabulary, 2009, <https://www.iso.org/standard/44651.html> și Eric Marsden. The ISO 31000 standard on risk management, 2020, <https://risk-engineering.org/static/PDF/slides-ISO31000-risk-management.pdf>.

De aceea, sistemul poate fi comutat din experimental în producție doar când s-a ajuns stabil sub nivelul de toleranță la risc al actorilor participanți, chiar și doar în cadru intern instituțional, dar în speță la nivel național, european sau internațional.

Pe de altă parte, accesul la sistem din exterior, prin clienții înregistrați și verificatori de diplome, și/sau API pentru dezvoltări ulterioare, și/sau contracte inteligente, trebuie foarte bine controlat, refuzând deschiderea pentru actori cu apetit de risc ridicat, foloasele preconizate în servicii adiționale nesuținând scăderea robusteții sistemului.

Interacțiunea cu alte sisteme tehnice

Coexistența cu sistemele actuale (non-DLT) este previzionată pentru o perioadă de tranziție. Soluția – pentru verificatorii de diplome – poate fi acceptarea diplomelor atât în varianta veche, cât și prin intermediul sistemului nou, cu validare pe blockchain.

Deoarece o diplomă este utilă pentru titularul său pe toată perioada de viață profesională, trebuie asigurată continuitatea disponibilității serviciului de verificare a diplomelor, emise anterior implementării sistemului:

- Înregistrarea diplomelor vechi (pre-blockchain, posibil scanarea celor tipărite) în sistem, pentru cetățenii angajabili;
- Păstrarea sistemului vechi și reducerea resurselor alocate, în paralel cu sistemul nou, pentru toată durata angajabilității cetățenilor cu diplome pre-blockchain.

Aplicațiile verificatoare pot fi:

- Cu disponibilitate restricționată și acces la serviciu, strict controlat;
- Disponibil public, dar cu acces la serviciu, strict controlat;
- Disponibil public, cu specificații/API publice și acces deschis (dar limitat ca performanțe, pentru menținerea disponibilității serviciului).

În cazul din urmă, alte entități pot dezvolta aplicații alternative, sau chiar biblioteci software care se pot integra în alte sisteme, permițând verificarea automată a diplomelor care sunt colectate în acele sisteme, prin intermediul unor apeluri la sistemul blockchain implementat.

Interoperabilitatea cu alte sisteme similare, de verificare diplome, crește în importanță cu creșterea mobilității forței de muncă, mai ales în cadrul Uniunii Europene.

O caracteristică aparte a stocării înregistrărilor într-un blockchain este longevitatea stocării, pentru a păstra imuabilitatea maximă (de regulă, cu cât un blockchain este mai lung, cu atât devine mai dificil ca cineva să altereze cu succes datele stocate în el). De aceea, odată ce s-a început înregistrarea diplomelor emise, este indicat să se păstreze aceeași metodă de înregistrare a lor. Este necesară planificarea de la început a interoperabilității cu alte sisteme existente sau

proiectate, de exemplu „Diploma Accreditation Records” („Înregistrări de acreditări diplome”)⁴⁹ din cadrul EBSI a Comisiei Europene.

Deși deja există sisteme de înregistrare/verificare diplome educaționale, în producție, se recomandă ca dezvoltarea unui sistem nou să convergă la specificațiile propuse de Comisia Europeană, deoarece, în viitor, chiar și sistemele private⁵⁰, existente în domeniu, vor trebui să se alinieze și să fie interoperabile cu cel european.

Diagrama pentru implementare

Instituțiile educaționale cu cicluri multianuale emit diplome doar de câteva ori pe an (de ex. licențe iulie, licențe septembrie, licențe februarie). Instituțiile care oferă cursuri de formare sau reconversie profesională pot testa mai ușor (examene finale organizate la intervale de câteva luni sau mai frecvent per an).

În cazul lipsei de suport la nivel superior, se poate porni de jos în sus, cu riscul unor probleme de interoperabilitate în momentul viitor al integrării într-un sistem național, european sau internațional:

- nivel facultate/universitate/consorțiu de universități/minister/ministere/UE
- nivel instituție educațională/oraș/județ/țară/UE

Tabel 7: Diagrama GANTT pentru activitățile majore ale soluției propuse

Activitate			Rezultat	An implementare										
				1	1,5	2	2,5	3	3,5	4	4,5	5	6-9	10
Pregătire sistem național: 5 ani	2 ani: Proiectare, dezvoltare, implementare back-end și front-end		Sistem prototip verificat (TRL4 [31, 32])											
	0,5 ani: Formare personal și testare beta	0,5 ani: Formare personal, training pe sistemul dezvoltat	Tehnologie validată în mediu relevant (TRL5)											
		0,5 ani: Testare beta de către utilizatori	Tehnologie demonstrată în mediu relevant (TRL6)											
	1 an: „Smoke testing”, ucenic non-		Sistem model și prototip demonstrate în mediu											

⁴⁹ Marta Pastor. Diploma Accreditation Records, <https://ec.europa.eu/cefdigital/wiki/display/EBSIDOC/Diploma+Accreditation+Records>.

⁵⁰ BCdiploma. (2021). Success stories. <https://www.bcdiploma.com/en/customersSuccess> și BCdiploma. (2021). They certify with BCdiploma. <https://www.bcdiploma.com/en/issuersList/>.

	Activitate	Rezultat	An implementare										
			1	1,5	2	2,5	3	3,5	4	4,5	5	6-9	10
	producție/duplicat de probă, paralel cu sistemele existente	operațional (TRL7)											
	0,5 ani: Analiză comparativă rezultate sistem nou/sistem vechi	Sistem complet și validat (TRL8)											
	1 an: Optimizare/eliminarea defecte raportate de utilizatori	Sistem validat în mediul operațional, gata să înlocuiască sistemele actuale (TRL9)											
Înlocuire completă a sistemelor vechi, la nivel național: 5 ani	Alternativă cu aceleași drepturi ca sistemele existente, rulare în paralel cu ele, la alegere	Sistem de emiter/verificare diplome alternativ, digital, pe blockchain											
	Trecere pe sistemul nou, termen: cinci ani după TRL9.	Sistem de emiter/verificare exclusiv digitală, pe blockchain, a diplomelor nou emise											

Metodologia de management a proiectului și modelul de dezvoltare

În dezvoltarea soluției se vor folosi metode de management Agile, respectând cerințele legale și etice în vigoare.

Se propune API deschis, pentru extensibilitate – organizații terțe vor putea citi datele (parțial și respectând GDPR), pentru oferirea mai simplă a unor servicii, cetățenilor și mediului economic.

De notat este particularitatea proiectului în domeniul temporal. Diagrama de implementare este prezentată mai sus, însă dincolo de orizontul de timp prezentat, dezvoltările ulterioare și îmbunătățirile soluției, de aducere la zi cu tehnologiile viitorului, trebuie să respecte compatibilitatea înapoi, chiar până la prima înregistrare. Fiecare înregistrare-bloc este dependentă de cele dinainte, astfel că menținerea lanțului de înregistrări, nefracționată, de la prima diplomă înregistrată în el, până la cea mai proaspătă, asigură protejarea de modificări a datelor înregistrate. De aceea, modelul de dezvoltare trebuie să fie unul de bătaie lungă, susținut, fără reporniri ale lanțului.

Precondiții și factori critici pentru succes

Implementarea cu succes a sistemului propus este dependentă de factori dintre care particulari pentru acest proiect:

- Lipsește componenta legislativă care să acorde aceeași valoare diplomelor înregistrate pe blockchain, ca celor tipărite și semnate olograf;
- Numărul de specialiști dezvoltare/mentenanță blockchain este, deocamdată, insuficient;

- Lipsă consens asupra unui standard, sau a unui consens național/european/internațional pentru o soluție de diplome pe blockchain, agreată pe termen lung. Deși EBSI are propunere la nivel european în acest sens, aceasta este la nivel de „draft” (ciornă), la mijloc de 2021.

Indicatori pentru monitorizare și evaluare

Indicatori principali de ieșire:

- Hardware/software, sistem de emitere/înregistrare/validare diplome;
- Material de formare competențe în mentenanța și utilizarea sistemului;
- Diplome educaționale, înregistrate în blockchain;

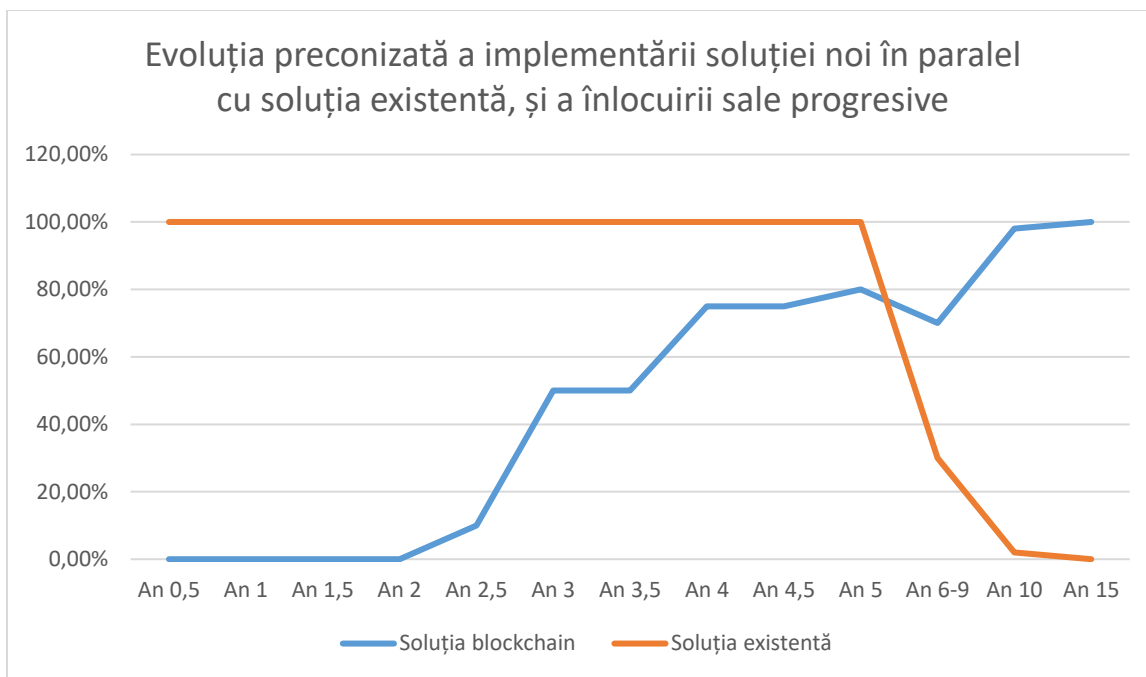
Indicatori principali de rezultat:

- Timp redus pentru înregistrarea și disponibilitatea diplomei, de la momentul absolvirii;
- Scurtarea traseului ierarhic de confirmare emitere/validitate diplomă;
- Găsirea și verificarea rapidă a diplomei;
- Proceduri simplificate de validare diplome;
- Flux de lucru simplificat.

Indicatori principali de impact:

- Eliminarea traficului cu diplome false;
- Reducerea timpului de obținere a diplomei.

Se are în vedere evaluarea periodică prin sondaj, în rândul emitenților de diplome, al angajatorilor și al absolvenților.



După dezvoltarea sistemului, testele de integrare și testele alfa, testele beta vor urmări emiterea diplomelor și în noul sistem, în duplicat celor emise în sistemul existent, referința legală rămânând diplomele emise prin sistemul existent. După fiecare fază de testare, crescător comprehensivă, se vor emite mai multe diplome-copie și în sistemul nou, până la corectarea eventualelor greșeli de funcționare și procedură, și eventuale îmbunătățiri modificatoare de rezultat, în sistem.

După auditul final al sistemului, i se vor acorda drepturi depline, din acest punct emițându-se diplome ori în sistemul vechi, ori în cel nou, ambele feluri cu aceeași valoare. Se estimează ca acest punct de cotitură să fie atins la cinci ani după inițierea implementării. Va începe scăderea ponderii diplomelor emise în sistemul vechi, instituțiile educaționale pornind cu mutarea emiterilor, spre sistemul nou. Totodată, testarea finalizându-se, inițial va scădea brusc numărul de diplome emise în sistemul nou, deoarece instituțiile emitente vor fi reticente în a emite diplome „reale” în noul sistem, oricât de bine ar fi aprofundat utilizarea soluției.

Nu în ultimul rând motivate de un termen cincinal impus de ministerele supraveghetoare, marea majoritate a instituțiilor educaționale vor trece pe sistemul nou, dar o mică parte va rămâne, o vreme. Ele vor încerca integrarea în noul sistem pentru recunoaștere națională sau europeană a diplomelor emise, însă vor emite diplome în sistemul vechi, din varii motive.

Referințe bibliografice

1. Digi24. *Fraudă universitară de proporții la "Spiru Haret" privind diplomele emise.*
<https://www.digi24.ro/stiri/actualitate/justitie/frauda-universitara-de-proportii-la->

- [spiru-haret-diicot-investigheaza-cum-au-fost-date-diplomele-false-1233377](#)
2. Alexandra Andronie. *Diplome false pentru asistenți de medicină dentară*.
<https://www.digi24.ro/stiri/actualitate/diplome-false-pentru-asistenti-de-medicina-dentara-programele-de-masterat-aveau-presupuse-colaborari-cu-universitati-din-europa-1624509>
 3. J.C. Cheng, N.Y. Lee, C. Chi, Y.H. Chen, *Blockchain and Smart Contract for Digital Certificate, the 4th IEEE International Conference on Applied System Innovation, ICASI*, Chiba, Japan, 13–17 April 2018.
 4. Kamišalić A., Turkanović M., Mrdović S., Heričko M. (2019) *A Preliminary Review of Blockchain-Based Solutions in Higher Education*. In: Uden L., Liberona D., Sanchez G., Rodríguez-González S. (eds) *Learning Technology for Education Challenges. LTEC 2019. Communications in Computer and Information Science*, vol 1011. Springer, Cham.
https://doi.org/10.1007/978-3-030-20798-4_11
 5. *The Times of India*. *Pakistani 'diploma mill' of fake degrees exposed*.
<https://timesofindia.indiatimes.com/world/uk/pakistani-diploma-mill-of-fake-degrees-exposed/articleshow/62528163.cms>
 6. Choi, D.; Chung, C.Y.; Seyha, T.; Young, J. *Factors Affecting Organizations' Resistance to the Adoption of Blockchain Technology in Supply Networks*. *Sustainability* **2020**, *12*, 8882.
<https://doi.org/10.3390/su12218882>
 7. Raritan. *Blockchain Infrastructure BlockOps*.
<https://www.raritan.com/landing/blockchain-infrastructure-blockops-wp/thanks>
 8. Bojana Koteska, Anastas Mishev, *Blockchain Implementation Quality Challenges: A Literature Review*, In: Z. Budimac (ed.): *Proceedings of the SQAMIA 2017: 6th Workshop of Software Quality, Analysis, Monitoring, Improvement, and Applications*, Belgrade, Serbia, 11-13.9.2017
 9. Castro RQ, Au-Yong-Oliveira M. *Blockchain and Higher Education Diplomas*. *Eur J Invest Health Psychol Educ*. 2021;11(1):154-167. Published 2021 Feb 19.
[doi:10.3390/ejihpe11010013](https://doi.org/10.3390/ejihpe11010013)
 10. Serranito D., Vasconcelos A., Guerreiro S., Correia M. *Blockchain Ecosystem for Verifiable Qualifications; Presented at the 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS*; Paris, France, 28–30 September 2020
 11. Fernando Richter Vidal, Feliz Gouveia, Christophe Soares, *Blockchain Application in Higher Education Diploma Management and Results Analysis, Advances in Science, Technology and Engineering Systems Journal* Vol. 5, No. 6, 871-882 (2020) *Distributed Ledger Technology (DLT) and Blockchain, FinTech Note* | No. 1
 12. Harish Natarajan et al. *Distributed Ledger Technology (DLT) and Blockchain*.
<http://documents1.worldbank.org/curated/pt/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>
 13. Josh Taubenheim. *Distributed Ledger Technology (DLT): 7 Benefits for IoT Applications*.
<https://www.machnation.com/2019/03/13/distributed-ledger-technology-dlt-7-benefits-for-iot-applications/>
 14. Ilker Koksall. *The Benefits Of Applying Blockchain Technology In Any Industry*.
<https://www.forbes.com/sites/ilkerkoksall/2019/10/23/the-benefits-of-applying->

[blockchain-technology-in-any-industry/?sh=716e820c49a5](#)

15. Prerna Singh. *Hyperledger vs Ethereum – Which Blockchain Platform Will Benefit Your Business?* <https://www.edureka.co/blog/hyperledger-vs-ethereum/>
16. Nitish Srivastava. *Ethereum Vs. Hyperledger: A Comprehensive Guide.* <https://www.blockchain-council.org/ethereum/ethereum-vs-hyperledger-a-comprehensive-guide/>
17. Institutul Național de Statistică. *Câștigul salarial mediu lunar.* <https://insse.ro/cms/ro/content/c%C3%A2%C8%99tigul-salarial-mediulunar-78>
18. DELL. *PowerEdge R750 Rack Server.* https://www.dell.com/en-us/work/shop/servers-storage-and-networking/poweredge-r750-rack-server/spd/poweredge-r750/pe_r750_tm_vi_vpsb?view=configurations&configurationid=55c6be4e-c931-49b0-ad82-d7c472eba2e5
19. Tom Coughlin. *LTO-9 Tape Products Now Available.* <https://www.forbes.com/sites/tomcoughlin/2021/09/15/lto-9-tape-products-now-available/>
20. TapeAndMedia. *IBM LTO Ultrium 9 Tape with Barium Ferrite.* <https://tapeandmedia.com/ibm-lto-9-tape-with-barium-ferrite-bafe-02XW568/>
21. The Linux Foundation. *Certified Hyperledger Fabric Developer.* <https://training.linuxfoundation.org/certification/certified-hyperledger-fabric-developer/>
22. Blockchain Training Alliance. *Ethereum Developer On Demand with CBDE Exam and retake.* <https://blockchaintrainingalliance.com/collections/instructor-led-classes/products/ethereum-developer-training-on-demand>
23. Kumutha K, S. Jayalakshmi, *The Impact of the Blockchain on Academic Certificate Verification System-Review*, EAI Endorsed Transactions on Energy Web, April 2021, <http://dx.doi.org/10.4108/eai.29-4-2021.169426>
24. Gwyneth Iredale. *Hyperledger Fabric Vs Ethereum: Head-To-Head Battle.* <https://101blockchains.com/ethereum-vs-hyperledger-fabric/>
25. *Hyperledger Architecture Working Group, HyperledgerArchitecture*, Volume 1, Hyperledger.org, vol. 1, p. 15, 2017.
26. Toshendra Kumar Sharma. *5 Skill Sets a Blockchain Developer Must Have.* <https://www.blockchain-council.org/blockchain/5-skill-sets-a-blockchain-developer-must-have/>
27. Robert Sheldon. *6 must-have blockchain developer skills.* <https://whatis.techtarget.com/feature/6-must-have-blockchain-developer-skills>
28. Alammary, A.; Alhazmi, S.; Almasri, M.; Gillani, S. *Blockchain-Based Applications in Education: A Systematic Review.* *Appl. Sci.* **2019**, *9*, 2400.
29. Mara-Florina Steiu. *Blockchain in education: Opportunities, applications, and challenges.* <https://firstmonday.org/ojs/index.php/fm/article/view/10654/9726>
30. Dr. M. R. Arun , Prof. M. R. Sheeba, Prof. F. Shabina Fred Rishma, *Comparing BlockChain with other Cryptographic Technologies (DAG, Hashgraph, Holochain)*, International Journal of Computer Engineering in Research Trends Multidisciplinary, Open Access, Peer-Reviewed and fully refereed Research Paper Volume-7, Issue-4, 2020

31. *European Union, Technology Readiness Levels*,
https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf
32. *The Welding Institute, Ce sunt Nivelurile de Pregătire Tehnologică*, <https://www.twi-global.com/locations/romania/ce-facem/intrebari-frecvente-faq/ce-este-trl-technology-readiness-level>
33. Marta Pastor. *Diploma Accreditation Records*,
<https://ec.europa.eu/cefdigital/wiki/display/EBSIDOC/Diploma+Accreditation+Records>
34. Valeriu Mina, Andreea Amorăritei, *Utilizarea semnăturii electronice în relațiile cu autoritățile și instituțiile publice*,
<https://www.lexology.com/library/detail.aspx?g=9f3bbff5-6288-4424-ad99-76bedb1d3288>
35. Andreea-Maria Maxim. *Scurte considerații privind semnătura electronică*,
<https://www.juridice.ro/680239/scurte-consideratii-privind-semnatura-electronica.html>
36. *, *Normele tehnice și metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică*, <https://www.certsig.ro/ro/depozitar/legislatie/norme-aplicare-lege-semnatura-electronica/>
37. *Parlamentul României. Înregistrarea operațiunilor comerciale prin mijloace electronice*,
https://static.anaf.ro/static/10/Anaf/legislatie/L_260_2007.pdf
38. *Guvernul României. Administrarea, funcționarea și implementarea sistemului național privind factura electronică RO e-Factura și factura electronică în România*,
<http://legislatie.just.ro/Public/DetaliiDocument/247243>
39. UNIC. (2021). *Publication of Academic Certificates*. <https://www.unic.ac.cy/iff/blockchain-certificates/>
40. UNIC. (2021). *The ONLY truly decentralized solution to secure PDF documents from fraud without intermediaries!*, <https://blog.block.co/what-differentiates-block-co-from-its-centralized-competitors/>
41. Patel, N. (2019). *Malta Pilots Blockchain-Based Credentials Program*.
<https://spectrum.ieee.org/tech-talk/computing/networks/malta-pilots-blockchainbased-credentials-program>
42. Worldometer. (2020). *Malta Population*. <https://www.worldometers.info/world-population/malta-population/>
43. Abas, A. (2018). *University consortium set up to authenticate degrees using blockchain technology*. <https://www.nst.com.my/news/nation/2018/11/429615/university-consortium-set-authenticate-degrees-using-blockchain>
44. BCdiploma. (2021). *Success stories*. <https://www.bcdiploma.com/en/customersSuccess>
45. BCdiploma. (2021). *They certify with BCdiploma*.
<https://www.bcdiploma.com/en/issuersList/>
46. Benay, A. (2019). *Securing the future of talent mobility in the Government of Canada*.
<https://tbs-blog.canada.ca/en/securing-future-talent-mobility-government-canada>
47. (2017). *Government of Canada: Talent cloud*. <https://talent.canada.ca/en>
48. Durant, E. (2017). *Digital Diploma debuts at MIT*. <https://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017>

49. *Senatul Universității Tehnice din Cluj-Napoca. Regulament privind organizarea și desfășurarea examenelor de finalizare a studiilor pentru ciclul I și II în Universitatea Tehnică din Cluj-Napoca (examene de licență/diplomă și disertație) pentru anul universitar 2020-2021, 2021,*
https://www.utcluj.ro/media/decisions/2021/03/30/Regulament_finalizare_studii.pdf
50. Simona Cimponeriu, Lidia-Ioana Fodorean. *Procedură operațională: comanda, gestionarea, completarea și eliberarea actelor de studii tipizate*, Biroul Acte de Studii UTCN, 2014,
https://www.utcluj.ro/media/page_document/148/Procedura%20Acte%20de%20studii.pdf
51. Yakob Mesengiser, Natalia Miloslavskaya. *Problems of Using Redactable Blockchain Technology*, 2021, DOI 10.1016/j.procs.2021.06.068
52. Giuseppe Ateniese et al. *Redactable Blockchain – or – Rewriting History in Bitcoin and Friends*, 2017, DOI 10.1109/EuroSP.2017.37
53. Damiano Sartori. *Redactable Blockchain : How to Change the Immutable and the Consequences of Doing So*, 2020, <http://purl.utwente.nl/essays/82755>
54. Bill Hagen, Tony VenGraitis. *Appropriate Use of the IEEE Prohibited Authors List*, 2015,
https://www.ieee.org/content/dam/ieee-org/ieee/web/org/pubs/appropriate_use_of_pal.pdf
55. *International Organization for Standardization. ISO 31000 Risk Management*, 2021,
<https://www.iso.org/iso-31000-risk-management.html>
56. *International Organization for Standardization. ISO Guide 73:2009 Risk management — Vocabulary*, 2009, <https://www.iso.org/standard/44651.html>
57. Eric Marsden. *The ISO 31000 standard on risk management*, 2020, <https://risk-engineering.org/static/PDF/slides-ISO31000-risk-management.pdf>
58. Digi România. *DIGI lansează internetul de 10 Gbps*, 2021,
<https://www.digi.ro/anunturi/digi-lanseaza-internetul-de-10-gbps-fiberlink-10-g-cel-mai-rapid-internet-din-romania-29465>



Proiect:

Proiect selectat în cadrul Programului Operațional Capacitate Administrativă cofinanțat de Uniunea Europeană, din Fondul Social European

Axa Prioritară 1: Administrație publică și sistem judiciar eficiente

Obiectivul specific 1.1: Dezvoltarea și introducerea de sisteme și standarde comune în administrația publică ce optimizează procesele decizionale orientate către cetățeni și mediul de afaceri, în concordanță cu SCAP.

Titlul proiectului: „Cadru strategic pentru adoptarea și utilizarea de tehnologii inovative în administrația publică 2021-2027 – soluții pentru eficientizarea activității”

COD: SIPOCA 704

Beneficiar: AUTORITATEA PENTRU DIGITALIZAREA ROMÂNIEI

Partener: UNIVERSITATEA TEHNICĂ DIN CLUJ – NAPOCA

Fundamentarea cazului de utilizare și studiu de evaluare ex-ante pentru Identitatea persoanelor, gestionarea și protecția datelor personale

Cuprins

Referințe	3
Acronime și abrevieri	6
Scopul intervenției	7
Părțile interesate.....	10
Beneficiile estimate.....	10
Factori critici în asociere cu cazurile de utilizare	11
Provocări tehnice în implementarea intervenției.....	12
Procese curente care ar putea fi afectate de dezvoltarea proiectului	13
Obiectivele funcționale	13
Obiectivele de performanță.....	13
Elementele de noutate	14
Criteriile de selecție	15
Descrierea în detaliu a cazului de referință	16
Opțiuni de îmbunătățire	16
Analiza comparativă.....	17
Constrângeri privind implementarea.....	21
Resurse tehnice pentru implementare	24
Resurse umane pentru implementare.....	25
Resurse financiare pentru implementare	26
Resurse logistice pentru implementare.....	28
Riscuri și planuri de contingență.....	28
Interacțiunea cu alte sisteme tehnice	30
Diagrama pentru implementare	31
Metodologia de management a proiectului și modelul de dezvoltare	32
Precondiții și factori critici pentru succes	32
Indicatori pentru monitorizare și evaluare	33
Referințe bibliografice	33

Referințe

Introducere

Conceptul de Blockchain este unul vast și oferă soluții pentru diverse probleme cu care societatea din ziua de azi se confruntă, oferind soluții de gestionare și stocare pentru multiple tipuri de date. Un raport realizat de EU Blockchain Forum a formulat cele 5 domenii în care aplicabilitatea aceste tehnologii a început să fie studiată, acestea fiind:

- *Gestiunea identității*
- *Gestiunea proprietății*
- *Domeniul sănătății*
- *Autentificarea documentelor (certificate, diplome)*
- *Procesul de vot.*

Un subiect pe care s-a pus accent este cel de gestiune a identității, având în vedere că politica de GDPR prezintă o mare sensibilitate în era cibernetică unde securitatea informației transmise este cel mai important aspect. GDPR are aplicabilitate în toate procesele de prelucrare a datelor cu caracter personal și în funcție de configurația sistemului Blockchain, există diferite mijloace de realizare a acesteia. Managementul identității este un element de bază pentru majoritatea soluțiilor și peisajelor software. Concurența cu soluțiile existente de gestionare a identității, conceptele bazate pe Blockchain și produsele au evoluat în contextul cererilor verificate și al identității auto-suverane. Tehnologia de bază a Blockchain este atât promițătoare, cât și complicată, iar adoptarea sistemului de identitate bazat pe Blockchain a fost destul de lentă, în ciuda așteptărilor mari și a pretențiilor de perturbare și progres. Pentru a reuși, abordările noi în materie de gestiune a identității trebuie să ofere beneficii substanțiale atât pentru utilizatorii finali, cât și pentru serviciile furnizorii de servicii. Aceste beneficii pot include securitatea, ușurința în utilizare, protecția datelor, transparență și, de asemenea, reducerea costurilor - luând în considerare costurile de migrare și de formare a utilizatorilor.

În cadrul unui Blockchain privat, participării sunt cunoscuți, ceea ce înseamnă că acordurile de prelucrare a datelor cu caracter personal pot fi încheiate cu ușurință. În cadrul unui Blockchain public, dificultatea crește, având în vedere că rolurile definite de GDPR de controlor, procesator și co-controlori nu sunt la fel de ușor de determinat și, în general, este mai dificil să se obțină un acord de prelucrare a datelor cu caracter personal între actori, de obicei, necunoscuți.

Cea mai mare problemă ridicată atât de Blockchain-ul public cât și de cel privat reiese din faptul că informațiile sunt distribuite fără necesitatea de oferire a unui acord către toți participanții din cadrul rețelei. Pe lângă acest aspect, un Blockchain public trebuie să ia în considerare că distribuie informații pe măsură ce acestea devin disponibile pentru oricine accesează lanțul.

Începând cu mai 2018 când a fost pus în aplicare Regulamentul general privind protecția datelor din UE au apărut o serie de comentarii cu privire la modul în care tehnologia Blockchain poate fi utilizată în acest domeniu. Câteva exemple relevante sunt:

- Autoritatea franceză de protecție a datelor - CNIL (*Commission nationale de l'informatique et des libertés*), a abordat în mod oficial aplicabilitatea GDPR la tehnologia Blockchain și a potențialele cazuri de utilizare într-un set specific de orientări¹;
- *EU Blockchain Observatory and Forum* - o inițiativă sponsorizată de Comisia Europeană care oferă analize și forumuri de discuții privind tehnologia Blockchain - a publicat un raport tematic, "Blockchain and the GDPR"²;
- Studiul "Blockchain și Regulamentul general privind protecția datelor. Pot fi compatibile registrele distribuite cu legislația europeană privind protecția datelor?"³ a fost redactat la solicitarea Grupului pentru viitorul științei și tehnologiei (STOA) din cadrul Secretariatului Parlamentului European.

Cazuri de utilizare

În ultima perioadă au fost implementate proiecte care abordează identitatea digitală în diferite țări sau pe arii restrânse. Interesul pentru acest subiect este tot mai mare, fiind unul ce atinge puncte sensibile precum datele cu caracter personal. Diferite cazuri de utilizare sunt prezentate în continuare:

- **Serviciile din Zug, Elveția**⁴: Orașul Zug a investit resurse în procesul de digitalizare a identității unei persoane, chiar dacă au existat piedici în acest demers. Câteva din problemele cu care s-au confruntat au fost faptul că datele cu caracter personal erau stocate în multiple servere și era dificilă o partajare a acestora între diferite instituții, dar de asemenea securitatea acestora putea fi compromisă din multiple părți. Totodată, demersuri anterioare au eșuat atunci când s-a pus problema digitalizării pașaportului elvețian și semnăturile digitale, deoarece sistemele nu se puteau scala și nu făceau față cererilor. Pentru a soluționa lipsa controlului și a securității, Institutul de Servicii Financiare din cadrul *Universității Lucerne* au creat un protocol pentru identitatea datelor cu ajutorul tehnologiei Blockchain. Guvernul orașului este partener în cadrul acestui proiect și locuitorii au opțiunea de a plăti serviciile guvernamentale cu Bitcoin încă din 2014.
- **Guvernul din Catalonia**⁵: Tehnologia Blockchain e utilizată în Catalonia în 6 domenii ale

¹ CNIL — Blockchain and the GDPR: Solutions for a responsible use of the Blockchain in the context of personal data, 6 November 2018, <https://www.cnil.fr/en/Blockchain-and-gdpr-solutions-responsible-use-Blockchain-context-personal-data>.

² https://www.euBlockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf.

³ [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf).

⁴ Caz utilizare Blockchain în Zug, Elveția, <https://blockchan.ge/blockchange-government-services.pdf>.

⁵ Caz utilizare Blockchain în Guvernul din Catalonia, <https://politiquesdigitals.gencat.cat/en/tic/estrategia->

sistemului precum: administrație, promovare, inovație, ecosistem, partea artistică și reglementări. Încă din Ianuarie 2020, ecosistemul din Catalonia conține 76 de companii care deservește acest demers. Toate demersurile sunt coordonate de Ministerul pentru Politici Digitale și Administrație Publică fiind vorba de informații confidențiale ce țin de identitatea locuitorilor orașului, accentul căzând pe modul de gestionare a acestora pentru a evita ca terțe părți să mai fie implicate și să aibă acces la aceste date.

- **Guvernul Spaniol** - Încă din 2019 a început demersuri în utilizarea tehnologiei Blockchain în domeniul public al țării. GDPR-ul face referire la o abordare bazată pe riscuri și formulează un test care ar trebui utilizat pentru a determina dacă datele sunt sau nu considerate personale, și anume dacă operatorul sau o altă persoană sunt în măsură să identifice persoana vizată. În conformitate cu acest lucru, Autoritatea spaniolă pentru protecția datelor a apreciat că hashing-ul utilizat în tehnologia Blockchain poate fi considerat o tehnică de anonimizare după efectuarea unei evaluări amănunțite a riscurilor care trebuie să includă, de asemenea, evaluarea măsurilor organizaționale care garantează eliminarea oricăror informații care permit reidentificarea, precum și garanția rezonabilă a robusteții sistemului dincolo de durata de viață utilă preconizată a datelor cu caracter personal.
- **Guvernul din Finlanda**⁶ – a întâmpinat dificultăți în ceea ce privește emigranții din cadrul țării care ajungeau fără documente în țară, iar existența lor nu putea fi consemnată în niciun mod. Fără acele acte era foarte greu de determinat vârsta și nu puteau să își întemeieze o locuință. Tehnologia Blockchain a oferit o soluție pentru această problemă, deoarece oferă posibilitatea de a urmări identitatea unei persoane într-un registru distribuit printr-o cheie unică, imutabilă și verificată independent, oferind astfel noi oportunități de a aborda această problemă. Această procedură este utilizată încă din anul 2015 prin intermediul unui proiect pilot ce a oferit tuturor refugiaților un card Mastercard ce era legat la identitatea lor. Tehnologia Blockchain, implementată prin Ethereum, menține o evidență a tuturor tranzacțiilor financiare efectuate cu acel card. Acest lucru le permite refugiaților să găsească un loc de muncă și să primească bani din locuri de muncă și, de asemenea, le permite să plătească facturile electronic - în cele din urmă, grăbindu-și procesul de stabilire în Finlanda.
- **Guvernul din Moldova**⁷ – Guvernul din Moldova s-a confruntat cu o problemă extrem de sensibilă o perioadă lungă de timp și anume traficul de minori ce erau scoși din țară și

[Blockchain/](#).

⁶ Caz utilizare Blockchain în Guvernul din Finlanda, <https://reliefweb.int/report/finland/how-finland-using-Blockchain-revolutionise-financial-services-refugees>.

⁷ Caz utilizare Blockchain în Guvernul din Moldova, <https://www.reuters.com/article/moldova-Blockchain-child-trafficking-idUKL8N1NK55K> și Cazuri utilizare Block Chain în Guvernul din Moldova, <https://ideas.unite.un.org/Blockchain4humanity/Page/ViewIdea?ideaId=390>.

ulteriorându-i în scopuri rău intenționate. Moldova caută să folosească Blockchain, instrumentul digital din spatele cripto-monedei Bitcoin, pentru a elimina traficul de copii cu ajutorul experților Națiunilor Unite. Datele biometrice sunt stocate în registre distribuite, fiind astfel simplificat procesul de identificare a acestora. Blockchain asigură invarianța datelor de intrare (modelul matematic garantează acest lucru), făcând imposibilă modificarea acestora în lanțul de evenimente – de exemplu, de a schimba data când documentul a fost creat, de a modifica datele despre trecerea frontierei sau eventual ștergerea datelor din sistem.

- **Guvernul din Franța⁸** – În prezent, doar autoritatea franceză de protecție a datelor - CNIL (*Commission nationale de l'informatique et des libertés*), a abordat în mod oficial aplicabilitatea GDPR la tehnologia Blockchain și potențialele cazuri de utilizare a acesteia într-un document de orientare specific. Documentul încorporează norme privind modul de determinare a controlurilor și procesatorilor de date în arhitecturile Blockchain, rolurile și obligațiile acestor actori, sfaturi privind modul în care se pot minimiza riscurile pentru datele persoanelor vizate atunci când prelucrarea este efectuată pe un Blockchain și metode de asigurare a exercitării efective a drepturilor persoanelor vizate.

Acronime și abrevieri

Abreviere sau acronim	Expresia completă	Explicație
GDPR	General Data Protection Regulation	Dispoziție legală ce are ca scop protejarea datelor cu caracter personal și delimitarea clară a modul în care acestea pot fi prelucrate.
DLT	Distributed Ledger Technology	Tehnologie de tip registru distribuit.
DIDs	Decentralized identifiers	Tip nou de identificador care permite o identitate digitală descentralizată și verificabilă.
EBSI	European Blockchain Services Infrastructure	Infrastructura europeană pentru servicii blockchain, promovată de Comisia Europeană.
IdM	Identity Management	Cadru de politici și tehnologii pentru a se asigura că utilizatorii potriviți (într-o întreprindere) au acces adecvat la resursele tehnologice.

⁸ CNIL — Blockchain and the GDPR: Solutions for a responsible use of the Blockchain in the context of personal data, 6 November 2018, <https://www.cnil.fr/en/Blockchain-and-gdpr-solutions-responsible-use-Blockchain-context-personal-data>.

WOT	web-of-trust	Este un concept utilizat în PGP, GnuPG și alte sisteme compatibile cu OpenPGP pentru a stabili autenticitatea legăturii dintre o cheie publică și proprietarul acesteia.
PGP	Pretty Good Privacy	Program de criptare care oferă confidențialitate criptografică și autentificare pentru comunicarea datelor.
POW	Proof-of-Work	O formă de dovadă criptografică în care o parte demonstrează altora munca pentru a fi remunerat.
RoEduNet	Romanian Education Network	Rețeaua națională pentru educație și cercetare: „asigură servicii de comunicații de date pentru instituțiile de cercetare și academice de toate gradele din România”. „Membru al consorțiului GEANT, rețeaua care interconectează toate rețelele pentru cercetare și educație din țările membre ale Uniunii Europene.”

Tabelul nr.1: Acronime și abrevieri.

Scopul intervenției

Definirea problemei

Așa cum a fost menționat anterior, conceptele de protecție a datelor cu caracter personal au fost evidențiate tot mai mult în contextul actual unde tehnologia permite realizarea de documente oficiale prin intermediul Internetului. Gestionarea acestor date implică un proces complex, neexistând o centralizare a datelor între instituțiile publice ale statului, implicit securitatea acestora poate fi compromisă mult mai ușor în acest mod. În ultimii ani, gestionarea identității a fost supusă unor perturbări din cauza incidentelor recurente de încălcare a securității datelor, care au dus la scurgeri de informații personale și la furtul de identitate. Apariția tehnologiei Blockchain a deschis calea pentru dezvoltarea identității auto-suverane - o nouă clasă de sisteme reziliente de gestionare a identității controlate de utilizatori, care sunt activate de tehnologia registrelor distribuite (DLT).

Un exemplu concret este cazul în care o persoană dorește să achiziționeze un imobil cu ajutorul unei bănci. Acesta trebuie să prezinte în nenumărate rânduri copii ale actului de identitate, copii ale proprietății pe care le deține, copii ale certificatului de naștere, copii ale certificatului de căsătorie dacă e cazul și alte documente ce conțin informații sensibile. Riscul ca una din acele copii să ajungă pe mâna unei persoane neautorizate este mult mai mare având în vedere că

acestea circulă între diferite instituții ale statului sau alte tipuri de instituții precum cele bancare. Problema se complică și mai mult când se ia în considerare faptul că angajații acelei instituții are acces la multiple acte ce conțin informații cu caracter personal.

O altă problemă cu care societatea din ziua de astăzi se confruntă este aceea a falsificării actelor oficiale, existând numeroase persoane ce dețin acte de identitate false sau chiar acte pentru proprietăți ce nu le aparțin. Stabilirea autenticității acestora nu este ușoară la prima vedere și necesită timp lucru care poate periclita chiar și siguranța societății și a instituțiilor publice.

Identitatea are o problemă. Dacă este pe suport de hârtie, cum ar fi certificatele de naștere care stau degeaba în subsolul unei primării, este expusă pierderii, furtului sau fraudei.

O identitate digitală reduce nivelul de birocrație și crește viteza proceselor din cadrul organizațiilor, permițând o mai mare interoperabilitate între departamente și alte instituții. Dar dacă această identitate digitală este stocată pe un server centralizat, ea devine o țintă pentru hackeri

Tehnologia Blockchain vine în ajutorul societății cu soluții pentru probleme de identitate a persoanelor și gestionarea și protecția datelor acestora prin caracteristicile pe care le oferă. Între acestea putem să enumerăm descentralizarea sistemului evitându-se astfel existența unui singur punct central care deține toate informațiile și care în cazuri extreme poate impacta toate ramurile societății, securitatea pe care poate să o ofere pentru multiple tipuri de date, trasabilitatea informațiilor, imutabilitatea acestora și consensul pe care îl implică.

Principalele beneficii pe care le aduce tehnologia Blockchain în domeniul GDPR-ului sunt:

- O gestiune mai bună a datelor ce țin de identitatea unei persoane prin rețeaua descentralizată.
- O securitate mai mare a datelor ce țin de identitatea unei persoane prin algoritmi de criptare ce păstrează informațiile din Blockchain, dar și prin modul de stocare a acestora.
- O validare mai ușoară a documentelor ce țin de identitate, proprietăți, etc.
- Eliminarea practicilor frauduloase cu privire la falsificarea documentelor.
- Eliminarea practicilor de furt de identitate.
- Eliminarea necesității distribuirii de copii a documentelor ce conțin date cu caracter personal unor terțe părți.

Obiectivele generale

Obiectivele generale urmărite prin adoptarea unei soluții bazate pe tehnologia Blockchain pentru identitatea persoanelor, gestionarea și protecția datelor personale sunt următoarele:

- Îmbunătățirea încrederii interne și internaționale în documentele ce conțin informații cu caracter personal în sectorul public.
- Gestionarea mai bună a datelor ce țin de identitatea unei persoane prin rețeaua descentralizată.
- Securitatea datelor prin modul de stocare a acestora în rețeaua Blockchain.

- Digitalizarea datelor cu caracter personal și eliminarea solicitării instituțiilor publice a copiilor xerox a documentelor importante; acest lucru vine în sprijinul cetățenilor și da un impuls pentru reformarea și modernizarea administrației publice.
- Verificarea mai ușoară a documentelor pentru a determina validitatea acestora.
- Asigurarea interoperabilității semantice și sintactice cu sistemele informaționale din Uniunea Europeană și nu numai.

Obiectivele specifice

Obiectivele specifice urmărite prin adoptarea unei soluții bazate pe tehnologia Blockchain pentru identitatea persoanelor, gestionarea și protecția datelor personale sunt următoarele:

- Înregistrare în Blockchain, la emitere a documentelor de identitate;
- Alocarea responsabilității pentru conformitate;
- Principiile de minimizare a datelor și de limitare a scopului;
- Tehnicile de anonimizare a datelor cu caracter personal;
- Transferurile între instituții a datelor într-un mod securizat;
- Transferurile transfrontaliere de date într-un mod securizat.

Obiectivele operaționale

Obiectivele operaționale urmărite prin adoptarea unei soluții bazate pe tehnologia Blockchain pentru identitatea persoanelor, gestionarea și protecția datelor personale sunt următoarele:

- Asigurarea unei infrastructuri tehnologice și organizaționale la nivel de domeniu public;
- Asigurarea unei infrastructuri tehnologice și organizaționale pentru publicul larg;
- Asigurarea interoperabilității semantice și sintactice cu instituțiile publice din Uniunea Europeană și nu numai în vederea identității persoanelor dintr-o societate;
- Asigurarea interoperabilității semantice și sintactice cu instituțiile publice din Uniunea Europeană și nu numai cu scopul gestionării datelor cu caracter personal dintr-o societate;
- Asigurarea interoperabilității semantice și sintactice cu instituțiile publice din Uniunea Europeană și nu numai în vederea protecției datelor cu caracter personal dintr-o societate.

Granițele de utilizare

- Domeniul public unde se țin acte referitoare la proprietățile unei persoane sau la datele sale personale;
- Instituțiile publice ce prelucrează sau gestionează date cu caracter personal.

Părțile interesate

Părțile interesate în implementarea unei soluții bazate pe tehnologia Blockchain pentru identitatea persoanelor, gestionarea și protecția datelor personale pot fi clasificate în două mari categorii: *beneficiarii*, respectiv *utilizatorii* soluției dezvoltate.

Potențialii beneficiari ai unei astfel de soluție sunt:

- Ministerul economiei, antreprenorialului și turismului, Ministerul muncii și Solidarității sociale.
- Ministerul Apărării Naționale.
- Autoritatea națională de supraveghere a prelucrării datelor cu caracter personal.
- Administrația publică locală (primării).
- Instituțiile bancare.
- Instituțiile publice/firmele/persoane care oferă servicii ce presupun oferirea de date cu caracter personal.
- Instituțiile de învățământ.
- Angajatorii din mediul privat.

Potențiali utilizatori ai unei astfel de soluții sunt:

- Angajați ai departamentelor de resurse umane din cadrul companiilor/organizațiilor responsabile cu recrutarea angajaților.
- Angajați ai firmelor specializate în recrutare de personal.
- Angajați ai birourilor primăriilor.
- Angajați ai instituțiilor bancare.
- Angajați ai diferitor ministere unde se gestionează și se prelucrează aceste date (justiție, afaceri, muncii etc.).

Beneficiile estimate

Principalele beneficii care ar putea fi obținute prin adoptarea unei soluții bazate pe tehnologia Blockchain pentru identitatea persoanelor, gestionarea și protecția datelor personale sunt:

- Verificarea rapidă a datelor în momentul în care se apropie de perioada de expirare a documentelor de identitate.
- Securitatea și siguranța datelor.
- Reducerea nevoii de creare de copii xerox a documentelor oficiale ale unei persoane.
- Posibilitatea stabilirii rapide a numărului de locuitori, nupțialitate, natalitate, mortalitate etc.
- Reducerea pierderii informațiilor prin terțe părți.
- Reducerea necesității multiplicării documentelor în instituții precum bănci, școli, justiție, afaceri etc.

- Reducerea necesității refacerii documentelor oficiale în cazuri de pierdere/furt.
- Reducerea costurilor prin eliminarea documentelor printate pe foi.
- Utilizarea de diferite mecanisme criptografice, combinate cu adoptarea unui registru distribuit ce oferă un nivel ridicat de securitate tuturor documentelor cu date cu caracter personal.

Factori critici în asociere cu cazurile de utilizare

Factorii care afectează adoptarea tehnologiei Blockchain în dezvoltarea unei soluții pentru identitatea persoanelor, gestionarea și protecția datelor personale pot fi împărțiți în următoarele categorii: (a) *Factori critici privind cerințele tehnice*, (b) *Factori critici de cost*, (b) *Factori critici privind calitatea*, (d) *Factori critici privind ușurința execuției*, (e) *Factori critici sub aspect economic*, (f) *Factori critici sub aspect legal*. În continuare vor fi prezentați factorii critici identificați pentru fiecare din cele șase categorii.

(a) **Factori critici privind cerințele tehnice:**

- Necunoscutele determinate de faptul că tehnologia este una relativ nouă.
- Lipsa de experți naționali și internaționali.
- Nevoia unei rețele distribuite care să ofere stabilitate și securitate.
- Nevoia de scalabilitate a rețelei.
- Nevoia de un număr mare de resurse hardware pentru construirea rețelei.
- Nevoia de a oferi o capacitate mare de stocare de date, fiind vorba de datele de identificare a tuturor persoanelor.
- Nevoia creării unui standard în limbajele de programare ce ar trebui să susțină un astfel de sistem.

(b) **Factori critici de cost**

- Costul înlocuirii infrastructurii existente cu una bazată pe tehnologia Blockchain.
- Costul formării personalului specializat.
- Costul de energie mare pentru determinarea calculelor criptografice.
- Costurile pentru asigurarea de securitate pe termen lung, mai ales în cazul în care apar noi metode ce ar putea perturba protecția datelor.
- Costurile pentru gestionarea optimă a datelor unei persoane, atât datele de identificare, cât și cele referitoare la proprietăți.
- Costuri ce țin de educația populație pentru creșterea gradului de încredere în utilizarea noii tehnologii.

(c) **Factori critici privind calitatea**

- Posibilitatea de atacuri cibernetice.
- Necesitatea unui sistem ce are un grad ridicat de valabilitate.
- Necesitatea unui sistem sigur.

- Necesitatea recuperării datelor în cazuri de forță majoră când acestea ar putea fi considerate pierdute.

(d) Factori critici privind ușurința execuției

- Lipsa de personal avizat.
- Lipsa de standarde privind limbajele de programare.
- Lipsa de cunoștințe tehnice, fiind vorba de un domeniu relativ nou care este într-o continua cercetare.
- Lipsa unei comunicări între instituțiile care pregătesc personal în acest domeniu și sectorul public unde se dorește aplicarea lui.

(e) Factori critici sub aspect economic

- Necesitatea de fonduri pentru crearea infrastructurii sistemului.
- Necesitatea de fonduri pentru instruirea de personal avizat.
- Necesitatea de fonduri pentru mentenanța sistemului din punct de vedere hardware și software.
- Necesitatea de fonduri pentru studierea în continuare a domeniului și a noilor metode ce pot îmbunătăți sistemul.

(f) Factori critici sub aspect legal

- Necesitatea unor cadre legale pentru tehnologia Blockchain.
- Necesitatea unei autorități care să gestioneze părțile interesate de participarea activă la un sistem bazat pe Blockchain.
- Necesitatea unei structuri juridice care să protejeze personale de furt de identitate.
- Necesitatea creării unor standarde referitoare la modul în care trebuie gestionată confidențialitatea și protecția datelor.
- Imutabilitatea datelor în cadrul tehnologiei Blockchain încalcă dreptul oamenilor de a fi șterși dintr-un sistem ce deține date cu caracter personal.

Provocări tehnice în implementarea intervenției

Principalele provocări tehnice în implementarea unei soluții bazate pe Blockchain pentru identitatea persoanelor, gestionarea și protecția datelor personale sunt:

- Realizarea unui sistem ce permite introducerea de date cu caracter personal pentru actele existente în prezent în format fizic, cât și introducerea de date noi cu caracter personal.
- Mentenanța unui sistem ce suportă servicii ce performează operații asupra datelor cu caracter personal într-un mod sigur.
- Construirea infrastructurii hardware.
- Construirea infrastructurii software.
- Crearea de personal avizat din punct de vedere tehnic care să poată menține un astfel de

sistem.

- Crearea unui cadru legislativ pentru implementarea unui astfel de sistem.
- Elaborarea unor standarde minime atât pentru partea hardware cât și pentru partea software.

Procese curente care ar putea fi afectate de dezvoltarea proiectului

- Procesul de dobândire de acte de identitate/carnet de șofer.
- Procesul de dobândire de documente referitoare la proprietate.
- Procesul de verificare a validității buletinelor și a documentelor oficiale.
- Procesul de verificare a validității documentelor de proprietate.

Utilizarea tehnologiei Blockchain în procesele menționate anterior impune noi pași în realizarea acestora, deoarece întreg procesul va fi automatizat și distribuit între celelalte Instituții. Având în vedere că toate celelalte Instituții trebuie să poată utiliza acele informații, este important să fie stabilite precondițiile impuse de sistem. Un exemplu de precondiție este referitor la formatul datelor care trebuie să fie uniform, dar în același timp este vorba de date cu caracter personal ce țin de identitatea unei persoane și care nu trebuie expuse unor terțe părți din principii de securitate. O codificare a acestora este necesară, iar cheia de decodificare trebuie expusă celorlalți participanți la rețea, dar într-un mod controlat și monitorizat. Toate procesele trebuie să ofere vizibilitate și transparență asupra tranzacțiilor pentru ca persoana vizată să poată conștientiza cine utilizează datele sale.

Obiectivele funcționale

Funcționalități dorite a fi regăsite în cadrul soluției tehnice/tehnologiei:

- Emiterea de documente oficiale în mod digitalizat și distribuit în sistem.
- Emiterea de documente persoanele în format digital.
- Verificarea ușoară a documentelor personale și a documentelor oficiale.
- Posibilitatea de partajare rapidă a documentelor între instituțiile statului și nu numai.

Obiectivele de performanță

Caracteristicile de performanță tehnică ale soluției propuse sunt rezultate din avantajele pe care un sistem bazat pe tehnologia Blockchain îl poate avea în ceea ce privește identitatea persoanelor, gestionarea și protecția datelor personale.

Aceste caracteristici sunt:

- **Gestionare mai ușoară a datelor cu caracter personal**, având în vedere că tehnologia Blockchain utilizează un registru distribuit ce face posibilă partajarea directă a datelor sau a unor token-uri între părțile din cadrul sistemului într-un mod descentralizat ce elimină astfel posibilitatea unei căderi în lanț într-o situație de urgență.
- **O securitate mai bună a datelor cu caracter personal**, având în vedere că un sistem centralizat are un singur punct de acces, iar în cazul în care acela nu este disponibil, întreg sistemul este afectat și nu mai este funcțional. Așa cum a fost menționat anterior, tehnologia Blockchain presupune o rețea distribuită ce menține sistemul funcțional chiar și în cazuri extreme, iar datele sunt copiate identic pe toate nodurile sistemului.
- **O încredere între părțile participante în gestionarea datelor cu caracter personal**, având în vedere că entitățile se cunosc.
- **Imutabilitate în ceea ce privește informațiile confidențiale referitoare la identitatea unei persoane**, având în vedere că toate acțiunile sunt înregistrate și nu pot fi șterse, fiind destul de ușor de găsit cine/când/ce a accesat sau chiar modificat.
- **Validitatea datelor cu caracter personal și a părților care le utilizează**, având în vedere că toate informațiile înregistrate în Blockchain sunt validate din mai multe perspective
- **Eficiența sistemului**, având în vedere că tehnologia Blockchain are la baza un registru distribuit care permite o automatizare a proceselor și o utilizare directă a datelor prin lipsa părților terțe ce erau intermediari în procesarea datelor.
- **Confidențialitatea datelor cu caracter personal**, având în vedere că tehnologia Blockchain permite verificarea execuțiilor dintr-un bloc într-un mod confidențial datorită protocoalelor de securitate pe care le adaugă peste informații.
- **Transparența gestionării datelor cu caracter personal**, având în vedere că toate tranzacțiile sunt înscrise într-un bloc din registrul distribuit și se poate determina ce terțe părți au acces la date cu caracter personal și acțiunile pe care le execută asupra acestora.

Elementele de noutate

Elementele de noutate aduse de tehnologia Blockchain în dezvoltarea unei soluții pentru identitatea persoanelor, gestionarea și protecția datelor personale sunt:

- Eliminarea documentelor de identitate false.
- Reducerea timpului necesar eliberării documentelor de identitate.
- Partajarea datelor cu alte instituții publice precum bănci, universități etc.
- Reducerea timpului de verificare și validitate autenticității documentelor de identitate.
- Reducerea timpului de verificare și validitate autenticității documentelor de proprietate.
- Control asupra partajării informațiilor.
- Securitatea datelor.
- Digitalizarea datelor ceea ce implică în mod automat și o centralizare a lor.

Criteriile de selecție

Pentru a determina ce tip de Blockchain trebuie utilizat pentru identitatea persoanelor, gestionarea și protecția datelor personale s-a realizat o comparație a unui Blockchain ce are ca mod de operare public (Ethereum) cu un Blockchain ce are ca mod de operare o rețea privată (Hyperledger). Comparația va urmări ca și criterii de selecție platforma pe care o utilizează, modul în care operează o astfel de rețea, nivelul de confidențialitate pe care poate să o ofere, securitate pe care o asigură, mecanismul de consens și scalabilitatea acesteia.

Din punct de vedere al platformei utilizare, Ethereum este destinată mediului afacerilor și a fost introdus cu scopul de a facilita contracte inteligente. Pe de altă parte, Hyperledger este destinată sectorului industrial și a fost concepută pentru a oferi un grad ridicat de securitate și scalabilitate prin arhitectura flexibilă. Din această perspectivă, pentru procesul de identitate a persoanelor, gestionare și protecție a datelor cu caracter personal un Blockchain cu o rețea privată se mapează mai mult pe caracteristicile urmărite.

Dacă se urmărește modul de operare a celor două tipuri de rețea, în Ethereum modul de operare este public așa cum a fost menționat anterior și nu necesită acordarea de permisiuni în accesarea datelor, pe când Hyperledger are un mod de operare privat și accesul este permis doar participanților autorizați. Având în vedere faptul că datele gestionate sunt date cu caracter personal ce nu trebuie distribuite unor terțe părți, Hyperledger reprezintă alegerea potrivită.

Nivelul de confidențialitate este un alt aspect foarte important atât din perspectiva procesului pentru identitatea persoanelor, gestionarea și protecția datelor personale. În cadrul unei rețele Blockchain de tip public, Ethereum, tranzacțiile oferă transparență și sunt vizibile pentru toți participanții la rețea, pe când într-o rețea Blockchain de tip privat, Hyperledge, doar membrii autorizați pot urmări tranzacțiile efectuate în cadrul acesteia, de aceea o rețea privată este alegerea potrivită.

Atât în cadrul rețelelor Blockchain cu operare publică, cât și a celor cu operare privată, datele implicate în tranzacții sunt păstrate într-un mod sigur și sunt utilizați algoritmi de hash-ing pentru gestionarea și păstrarea lor, de aceea oricare dintre acestea reprezintă o alegere potrivită. Mai mult decât atât, o rețea Blockchain este decentralizată ceea ce presupune că nu există un singur punct de control ce conține toate informațiile, iar acestea nu pot fi pierdute în cazul în care sistemul nu funcționează corespunzător.

Pe de altă parte, mecanismul de consens este diferit în cazul celor două tipuri de rețea Blockchain. În Ethereum toate nodurile trebuie să ajungă la un consens în ceea ce privește acțiunile următoare, pe când în Hyperledger nu este necesar un consens între acestea ci doar un protocol de acord prin care câteva sau toate părțile implicate pot să stabilească o cheie ce va influența rezultatul, oferind astfel scalabilitate sistemului și o confidențialitate a datelor, caracteristici necesare într-un sistem ce prelucrează, gestionează și securizează datele de identificare a unei persoane.

Scalabilitatea unui sistem de gestionare a datelor de identificare a unei persoane este foarte importantă având în vedere că populația globului este într-o continuă creștere și nevoia de creare a unui sistem ce permite înregistrarea acestora într-un sistem digitalizat reprezintă o necesitate în contextul actual. În Ethereum, fiecare nod al rețelei are un rol bine stabilit, de aceea

În cazul în care unul dintre acestea nu funcționează corespunzător, întreg sistemul este afectat. În Hyperledger, tranzacția nu este cunoscută de toate nodurile de aceea o scalabilitate a sistemului se poate realiza foarte ușor.

Ținând cont de toate aspectele discutate anterior, pentru un sistem de prelucrare, gestionare și securizare a datelor cu caracter personal, o rețea Blockchain cu un mod de operare privat este alegerea potrivită.

Descrierea în detaliu a cazului de referință

Datele cu caracter personal sunt gestionate și prelucrate de primării, Instituții bancare, Instituții din sectorul public, școli și Universități, dar acestea nu pot fi partajate într-un mod optim între acestea. Pentru înregistrarea datelor în oricare dintre aceste Instituții, este necesar oferirea documentelor în original și copie pentru a putea fi validate manual de un angajat și anexate la dosarele vizate. Implicarea unei terțe părți în verificarea datelor cu caracter personal poate ridica probleme de securitate și poate presupune erori umane în procesele aferente.

În prezent, bazele de date care conțin aceste informații referitoare la identitate unei persoane sunt locale pentru fiecare Instituție și prezintă diferite proceduri de verificare a acestora, spre exemplu ANAF, dar în același timp nu sunt în totalitate digitalizate, iar accesul este restricționat angajaților acelei Instituții. Realizarea unui sistem centralizat între aceste Instituții în ceea ce privește datele cu caracter personal, ar permite rezolvarea parțială a problemelor existente în prezent. Lipsa unui standard în modul în care aceste date sunt prelucrate și gestionate în prezent poate îngreuna crearea unui sistem care să le cuprindă pe toate.

Totodată, un sistem centralizat prezintă probleme atunci când apar erori în cadrul acestuia și nu oferă securitatea dorită atunci când vorbim de date sensibile. De exemplu, în cazul cărților de muncă, care sunt ținute într-un format electronic, centralizat. Deși sistemul este securizat și protejat, în cazul unui atac cibernetic, ar produce o problemă majoră. Mai mult decât atât, în cazuri extreme când vorbim de pierderea documentelor ce atestă identitatea unei persoane precum cartea de identitate, pașaportul, carnetul de șofer, diplomele de absolvire, carduri bancare, titluri de proprietate, cărți de muncă și așa mai departe presupune multiple drumuri pentru refacerea acestora și pentru certificarea că persoana care solicită acele date este persoana căreia îi aparțin acele informații.

Opțiuni de îmbunătățire

Așa cum a fost discutat la punctul anterior, sistemul existent în prezent prezintă lacune atât din perspectiva gestionării datelor cu caracter personal, Instituțiile neavând posibilitatea de a partaja informațiile între ele într-un mod securizat care să nu implice participarea la tranzacție a altor părți, cât și a prelucrării acestora, neexistând un standard pentru formatul datelor. De asemenea, un sistem centralizat peste cel existent nu ar putea soluționa toate problemele

ridicate. Alternativa vine prin utilizarea tehnologiei Blockchain în sectorul public, ce presupune o rețea descentralizată unde comunicarea se face prin intermediul nodurilor de rețea. Fiind vorba de informații ce țin de identitatea persoanelor, o rețea Blockchain cu un mod de operare privat este necesară, așa cum a fost prezentat anterior.

Un Blockchain privat este o rețea ce pune accent pe confidențialitate atât a tranzacțiilor pe care le execută, cât și a membrilor acesteia. Nodurile acesteia sunt validate și selectate anterior adăugării lor în executarea unei tranzacții, acestea participând de bună voie și nu din motive monetare. Accesul la o astfel de rețea este limitat pentru membrii ei și nu există posibilitatea unei coliziuni între resursele care execută validarea, deoarece rolul fiecăruia este bine cunoscut și stabilit în prealabil.

Un Blockchain privat în procesele pentru identitatea persoanelor, gestionarea și protecția datelor personale în sectorul public prezintă următoarele îmbunătățiri:

- Prelucrarea eficientă a datelor de identificare într-un mod digitalizat.
- Realizarea unui standard în modul de prelucrare a datelor cu caracter personal.
- Gestionare eficientă a datelor de identificare prin posibilitatea partajării acestora într-un mod securizat.
- Securizarea datelor cu caracter personal prin eliminarea părților asociate în procesele de partajare a acestora între diferite Instituții.
- Securizarea datelor cu caracter personal prin eliminarea necesității validării informațiilor în mod manual de către un angajat prin compararea actelor oficiale în original cu cele foto-copiate.
- Reducerea timpului de așteptare pentru obținerea de acte oficiale ce conțin date cu caracter personal.

Analiza comparativă

În prezent se folosesc numeroase soluții pentru managementul identității persoanelor bazate pe tehnologia Blockchain. Acestea se folosesc pentru creșterea caracteristicii de descentralizare și pentru un control îmbunătățit asupra documentelor.

În continuare vom analiza trei modele folosite pentru managementul identității și protecției datelor personale (vezi *tabelul nr. 2.*):

Tipul platformei	Arhitectura folosită
1. uPort Este o platformă open source bazată pe SSI permițând utilizatorilor să-și înregistreze propriile identități în Ethereum.	o Aplicație Uport Mobile: -Pentru crearea unei identități noi, -interacționează cu Ethereum, -aplicația Uport generează cheile -cheia privată este stocată pe dispozitivul utilizatorului -în cazul pierderii sau furtului dispozitivului mobil, utilizatorul își menține identificatorul

	(uPortID) -utilizatorul trebuie să nominalizeze uPortID-urile mandatarilor (persoane fizice sau instituții) care pot vota pentru înlocuirea cheii publice cu cea nouă propusă de utilizator. o Contracte inteligente: Uport are integrate două modele de contracte inteligente: -contract pentru controller și contract proxy. Fiecare include uPortID. Ori de câte ori utilizatorul dorește să interacționeze cu un contract de aplicare, de pe dispozitivul mobil, se trimite o tranzacție, semnată cu cheie, prin proxy. o Biblioteci pentru dezvoltatori: Posibilitatea părților interesate să integreze în uPort aplicațiile lor.
2. Sovrin Este un tip de Blockchain fără permisiune prealabilă. Sovrin este un registru autorizat cu un set cunoscut de validatori de noduri, denumite stewards, care ajung la un consens asupra registrului distribuit. Sovrin folosește identificatori descentralizați (DID) . Arhitectura Sovrin are trei layere.	o Sovrin Ledger: -este componenta cheie al proiectului Sovrin. -nodurile steward ale acestui registru rulează protocolul Plenum care este o versiune îmbunătățită a Protocolului redundant Byzantine ce este tolerant la erori. o Agenți Sovrin: -utilizatorii interacționează cu Sovrin prin intermediul agenților care acționează ca noduri de capăt adresabile -agentul Sovrin are multe funcții în rețea, cum ar fi schimburile de mesaje P2P (point to point). -stocarea și partajarea datelor criptate etc. o Clienți Sovrin: -aplicații operate pe dispozitive (smartphone, laptop, etc) pentru a asigura comunicarea cu agenții Sovrin -gestionarea registrelor în care se efectuează tranzacțiile de identitate.
3. ShoCard este o platformă care permite crearea de	o Bootstrapping: -este pornit prin instalarea aplicației SchoCard

identități pentru a asigura o unificare și identificare al utilizatorilor din diferite regiuni. Conceptul acestei soluții este combinația de Blockchain, tehnologia mobilă și biometria pentru a crea un sistem unitar pentru a asigura confidențialitatea și securitatea datelor personale. Infrastructura ShoCard se bazează pe Bitcoin Blockchain și are trei componente.	care generează o nouă pereche de chei pentru utilizatori și le scanează acreditările folosind camera dispozitivului. -datele legate de acreditările utilizatorului împreună cu un poză tip buletin a acestuia sunt criptate și stocate pe dispozitivul mobil, în timp ce hash-ul acestor date este scris pe Blockchain-ul Bitcoin securizat cu SchoCard și asociat cu numărul de tranzacții corespunzătoare ShoCardId-ului utilizatorului. o Certificare: -după faza de înregistrare, utilizatorul începe procesul de certificare în momentul interacționării cu un furnizor de certificat sau document oficial pentru a-și putea confirma identitatea. -utilizatorul furnizează, printr-un “plic” digital securizat, o legătură digitală, corespunzătoare informațiilor utilizatorului, la furnizor de act oficial, care la rândul lui verifică acreditările și face modificările în Blockchain. o Validare: -faza de validare are loc atunci când o autoritate acreditată trebuie să verifice certificarea utilizatorului pentru a determina dacă un respectivul are dreptul de a accesa un serviciu.
--	--

Tabelul nr. 2: Modele folosite pentru managementul identității și protecției datelor personale.

Alegerea unei platforme blockchain pentru dezvoltarea și integrarea unor aplicații folosite pentru gestionarea și protecția datelor personale depinde de mulți factori. Trebuie analizate atât aspectele tehnice cât și cele care țin de administrarea resurselor, securizarea datelor, software.

Un alt aspect în alegerea unei soluții este reprezentat de tipul platformei folosite (publică sau privată), cerințele hardware și tipul de algoritm de consens folosit de sistemul respectiv (să nu consume multe resurse). Costurile privind adoptarea, implementarea și întreținerea tehnologiei Blockchain pentru dezvoltarea soluției propuse.

Pentru a evalua cele trei platforme populare în prezent folosind tehnologia Blockchain, ne putem baza pe cele șapte legi ale identității digitale ale lui Cameron⁹ (vezi *Tabelul nr. 3.*), care

⁹ Cele șapte legi ale identității digitale ale lui Cameron, <https://www.identityblog.com/?p=1065>.

sunt:

- controlul utilizatorului și consimțământ,
- vizibilitate minimă pentru utilizare securizată,
- părți interesate,
- identitate securizată,
- arhitectură pentru operare în paralel și tip de tehnologie folosit,
- interfațarea cu utilizatorul,
- experiență în utilizare.

Toate cele trei soluții descrise mai sus au caracteristici speciale și unice și fiecare are beneficiile și dezavantajele sale. Cu toate acestea, în ciuda avantajelor aplicării DLT-ului (*Distributed Ledger Technology*) în managementul și securitatea datelor există o lipsă vizibilă de înțelegere contextuală în ce privește utilizatorul. În plus, chiar dacă principalul scop de a adopta o tehnologie Blockchain ca infrastructură pentru Managementul identității este înlăturarea autorității centrale, acesta poate să nu fie un obiectiv realist în aplicațiile IdM din cauza lipsei profunde de încredere.

Cerințe	Uport	Sorvin	ShoCard
Controlul utilizatorului și consimțământul	X	✓	✓
Vizibilitate minimă pentru utilizare securizată	✓	✓	✓
Părți interesate	X	✓	X
Identitate securizată	✓	✓	✓
Arhitectură pentru operare în paralel și tipul de tehnologie folosită	✓	✓	X
Interfațarea cu utilizatorul	X	✓	X
Experiență în utilizare	✓	X	

Tabelul nr. 3: Analiză comparativă bazată pe cele șapte legi ale identității digitale ale lui Cameron.

Concluzia la care s-a ajuns pe baza analizei platformelor Blockchain descrise mai sus, a fost că Sorvin poate fi văzut ca și o alegere viabilă în ceea ce privește implementarea unei soluții bazate pe Blockchain pentru gestionarea și protecția datelor personale.

Motivele sunt următoarele:

- se bazează pe platforma de tip Blockchain cu validatori de noduri (stewards), foarte stabilă și sigură,
- combină facilitățile tehnologiei foarte bine pentru securizarea tranzacțiilor,
- folosește registru distribuit de tip privat și public,
- are o arhitectură scalabilă, oferă suport pentru protejarea și gestionarea cheilor digitale,
- tranzacțiile care au loc în rețea sunt vizibile de către toți membrii.

Sovrin¹⁰ oferă utilizatorului un control total asupra identității lui cu posibilitatea de a alege atributele pe care le dorește a le pune la dispoziția părților interesate. Verificarea acestora din urmă rămâne o provocare, care este parțial abordată prin așa numitul “web-of-trust”. Utilizatorii interacționează cu Sovrin printr-o aplicație mobilă și software de control. Agentul poate fi rulat pe serverul utilizatorului sau pe serverele specializate care acționează în numele utilizatorului.

Atât identificatorii omnidirecționali, cât și unidirecționali sunt acceptați, iar utilizatorii pot publica și utiliza diferiți identificatori criptografici cu fiecare parte cu care interacționează.

Constrângeri privind implementarea

Sistemele Blockchain au apărut pentru a sprijinii sistemele de tranzacții financiare (monedă digitală) și, prin urmare, nu este surprinzător faptul că principalele proprietăți non-funcționale sunt cele care sunt esențiale în acest domeniu: integritatea și non-repudierea (inclusiv imutabilitatea datelor și transparența). Fiind un depozit de date foarte distribuit și redundant, sistemele Blockchain pot, de asemenea, permite niveluri ridicate de disponibilitate pentru citirea datelor.

Unele limitări ale proprietăților / cerințelor non-funcționale sunt inerente la tehnologie, însă altele sunt doar limitări actuale și ar putea fi depășite în viitorul apropiat. În cele ce urmează o să discutăm despre aceste limitări.

- **Cost**

Una dintre limitările proprietăților / cerințelor non-funcționale este costul monetar al implementării și operării sistemelor de tip Blockchain. Acestea sunt distribuite masiv, cu multe noduri de procesare redundante, și asigură integritatea datelor cu privire la întregul istoric al tranzacțiilor. Acest lucru are un impact inevitabil asupra costului de utilizare a Blockchain și înseamnă ca are un model de cost diferit față de infrastructura convențională (Cloud sau internă).

De exemplu, un studiu recent a comparat costurile de executare a proceselor de operare pe Blockchain cu cele de execuție a proceselor în Cloud¹¹. Blockchain a fost cu două ordine de mărime mai scump decât Cloud -ul clasic. Cu toate acestea, timpul de păstrare a stocării în Blockchain este plătit o singură dată într-o taxă de tranzacție pentru bucăți mici de date tranzacționate, în timp ce stocarea în Cloud necesită taxe lunare permanente.

- **Performanță**

¹⁰ Sovrin, <https://sovrin.org/overview/>.

¹¹ P. Rimba, A. B. Tran, I. Weber, M. Staples A. Ponomarev, X. Xu, Comparing Blockchain and Cloud Services for Business Process Execution, In Proc. International Conference on Software Architecture (ICSA 2017).

Performanța în funcție de timp înseamnă o varietate de lucruri pentru sistemele software. De fapt, rata de transfer reprezintă numărul de tranzacții pe care un sistem le poate procesa într-o fereastră de timp, în timp ce latența este timpul necesar pentru a răspunde la o singură tranzacție. Un sistem cu o latență scăzută nu are neapărat un debit ridicat (rata de transfer mare). Acest lucru poate depinde, de exemplu, și de scalabilitatea sistemului, care se referă la relația dintre utilizarea resurselor și performanța pe măsură ce crește cererea asupra sistemului.

Atunci când datele au fost scrise anterior în Blockchain, *latența de citire* reprezintă timpul de răspuns pentru accesarea datelor istorice de către un client Blockchain. Latența de citire poate fi mult mai rapidă pe Blockchain decât în cazul tehnologiilor convenționale, deoarece clienții pot păstra o copie locală completă a bazei de date, și astfel se pot evita întârzierile de rețea.

Solicitarea de a scrie date într-un Blockchain se face prin trimiterea unei tranzacții în rețea. *Latența de scriere* este una probabilistică și există mai multe surse de incertitudine. Toate Blockchain-urile vor avea mici întârzieri de rețea. De asemenea, în cazul Blockchain-urilor cu consens Nakamoto¹², nu se poate ști sigur că cel mai recent bloc inclus va fi inclus și ulterior. Pentru a ne spori încrederea că datele au fost introduse cu succes în Blockchain, putem aștepta un număr de blocuri de confirmare. Așteptarea mai multor blocuri de confirmare va crește latența de scriere. Din această cauză apar elementele de „timp de includere” (momentul în care vedem o tranzacție inclusă într-un bloc) și „timp de confirmare” (momentul în care am văzut un număr prestabilit de blocuri de confirmare).

- **Securitatea**

Proprietățile clasice de securitate sunt **confidențialitatea**, **integritatea** și **disponibilitatea**¹³.

Confidențialitatea înseamnă că nu are loc o divulgare neautorizată a informațiilor¹⁴. De obicei, acest lucru este mai greu de stabilit în sistemele bazate pe Blockchain, deoarece, în mod implicit, informațiile sunt vizibile pentru toată lumea din rețea. Informațiile pot fi criptate: asimetric cu cheia publică a unei anumite părți, astfel încât numai această parte o poate decripta; sau simetric cu o cheie secretă partajată, astfel încât grupul de părți care au acces la cheia secretă o poate decripta. În acest din urmă caz este nevoie de un mijloc sigur de schimb al cheii secrete în afara lanțului. Cu toate acestea, odată ce informațiile trebuie procesate prin contracte inteligente, aceste

¹² Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, disponibil la <https://bitcoin.org/bitcoin.pdf>.

¹³ P. Rimba, A. B. Tran, I. Weber, M. Staples A. Ponomarev, X. Xu, Comparing Blockchain and Cloud Services for Business Process Execution, In Proc. International Conference on Software Architecture (ICSA 2017).

¹⁴ Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, disponibil la <https://bitcoin.org/bitcoin.pdf>.

informații trebuie decriptate. Acest lucru se datorează faptului că codul contractului inteligent rulează pe toate nodurile rețelei și, prin urmare, oricare dintre acestea trebuie să fie capabil să proceseze datele de intrare. Acest lucru este necesar pentru a obține un consens cu privire la rezultatele execuției contractului inteligent. Încorporarea cheilor într-un contract inteligent ar dezvălui cheia tuturor participanților. Datele sensibile pot fi în pericol dacă sunt partajate pe un Blockchain, chiar dacă se utilizează criptarea. Blockchain-urile private operate prin rețele private pot oferi un anumit nivel de control al accesului, dar acest lucru nu va asigura confidențialitatea “comercială” între concurenții care operează în comun un Blockchain privat. Unele Blockchain-uri (Corda, Fabric) pot oferi un control mai fin al accesului la citire dar realizează integritatea globală numai reintroducând dependența de organizații terțe ca notarii. Există tehnologii interesante la orizont, care ar putea atenua unele dintre aceste probleme. De exemplu, metodele de verificare a cunoașterii (zk-Snark), pot fi utilizate pentru a ascunde conținutul unei tranzacții, permițând în același timp validarea independentă a integrității tranzacției respective. În ceea ce privește calculul pe date criptate, acesta este obiectivul unor tehnici precum criptarea homomorfică și calculul confidențial. Cu toate acestea, astfel de abordări nu au fost încă utilizate pentru contractele inteligente, în parte din cauza faptului că cerințele de calcul semnificativ mai mari decât cele ale calculului obișnuit.

Integritatea reprezintă absența modificărilor necorespunzătoare (nevalabile și neautorizate) ale sistemului și este un atribut esențial pentru Blockchain. Odată ce o tranzacție este inclusă într-un Blockchain și confirmată pentru o perioadă suficientă de timp, aceasta devine parte integrată a registrului de evidență efectiv imuabil și nu poate fi alterată. Acest lucru este valabil și pentru contractele inteligente: codul lor byte este implementat într-o tranzacție și este supus aceluiași garanții de integritate. Proprietatea cheie de integritate Bitcoin este dată de faptul că adresele nu pot cheltui banii pe care îi au. Proprietatea de integritate Ethereum este mai complicată, deoarece necesită funcționarea corectă a unui limbaj de programare a contractelor inteligente de tip Turing. Cu toate acestea, pentru aplicațiile client, Ethereum oferă o putere semnificativă, permițând implementarea condițiilor de integritate definite de utilizator ca precondiții verificate și comportamente definite în contractele inteligente. Integritatea ridicată și non-repudierea nu sunt întotdeauna ideale. De exemplu, uneori datele istorice trebuie șterse sau modificate. În cazul în care o intrare de registru vexatorie sau necorespunzătoare a fost creată, o instanță poate ordona registrului să modifice registrul pentru a elimina acea intrare (ca și cum nu ar fi fost creată niciodată).

Disponibilitatea și fiabilitatea. Disponibilitatea este capacitatea de a asigura un serviciu corect, în timp ce fiabilitatea este continuitatea serviciului corect. Mai mult, în contextul sistemelor bazate pe Blockchain, disponibilitatea se referă la capacitatea de a invoca funcții ale sistemului, în timp ce fiabilitatea se referă la primirea constantă a rezultatelor corecte în urma acestor invocări. Funcționarea Blockchain-urilor publice poate implica sute sau mii de noduri de procesare independente. Fiecare nod deține o instanță replicată integral a istoricului tranzacțiilor din Blockchain și poate funcționa

pentru utilizatori ca o interfață de tranzacție cu rețeaua Blockchain. Din cauza acestei redundanțe masive, în mod naiv ne-am putea aștepta ca un sistem Blockchain să aibă o disponibilitate extrem de ridicată. Putem presupune că componentele locale ale unui sistem bazat pe Blockchain sunt conectate la un nod local complet al rețelei Blockchain. Trimiterea unei tranzacții către o rețea Blockchain se face prin intermediul nodului full local, care transmite acest lucru tuturor nodurilor la care este conectat. Disponibilitatea unui nod complet accesibil la nivel local depinde, așadar, în mare măsură de organizația care operează un sistem bazat pe Blockchain. Pentru Blockchain, există circumstanțe în care distincția dintre fiabilitate și disponibilitate poate fi neclară, deoarece nu există un moment specificat la nivel global până la care o tranzacție ar trebui să se finalizeze. În cazul în care un sistem Blockchain nu include o tranzacție, acest lucru va fi un eșec atât din punct de vedere al disponibilității cât și al fiabilității.

- **Mentenabilitatea**

Mentenabilitatea se referă la capacitatea unui sistem de a fi supus modificărilor și reparațiilor. În sistemele bazate pe Blockchain care utilizează contracte inteligente, acest lucru este mai greu de implementat pentru contractele inteligente decât în sistemele distribuite obișnuite. Acest lucru se datorează faptului că contractele inteligente cuprind un cod care reglementează interacțiunile dintre părți care nu se încred în ele; încrederea este derivată din faptul că codul nu poate fi modificat cu ușurință. Un avantaj distinctiv al sistemelor bazate pe Blockchain este că nu există o singură parte care să controleze sistemul. Cu toate acestea, acest lucru creează în mod inerent provocări pentru guvernanta: gestionarea evoluției sistemelor bazate pe Blockchain. Modificările pot fi făcute pentru a corecta defecte, pentru a adăuga caracteristici sau pentru a migra către noi contexte IT. Cu toate acestea, într-un sistem cu mai multe părți, fără un singur proprietar, gestionarea acestor modificări seamănă mai mult cu diplomația decât cu gestionarea tradițională a riscurilor sau cu gestionarea convențională a modificărilor tehnice sau a produselor. Lecțiile pot fi trase din programele soft open-source, care se confruntă cu provocări similare în materie de dezvoltare. Cu toate acestea, guvernanta unui Blockchain nu este doar o problemă de dezvoltare de software - este, de asemenea, o problemă de implementare și de operațiuni. Atât pentru sistemele Blockchain publice, cât și pentru cele private, principalele părți interesate includ utilizatorii Blockchain-ului, dezvoltatorii de software cu autoritate morală sau contractuală asupra bazei de cod, minerii sau nodurile de procesare din ecosistemul Blockchain, precum și autoritățile guvernamentale de reglementare din industriile conexe.

Resurse tehnice pentru implementare

Resursele tehnice sunt de două categorii: hardware și software. Dar la acestea se adaugă componenta cea mai importantă, personalul calificat care face instalările și întreținerea pe

termen lung al sistemelor. Resursele pentru menținerea funcționalității rețelei Blockchain și de utilizare la capacitate optimă după implementare sunt și ele cruciale, deoarece este vorba despre o investiție continuă pe termen lung. Utilizatorii au nevoie de acces facil și securizat pentru exploatarea eficientă a sistemului.

De aceea, resursele se pot împărți în trei categorii principale:

1. Resurse hardware:

- servere,
- echipamente de rețelistică,
- echipamente de firewall,
- infrastructură pentru internet, soluții de Dark fiber, rețele de interconectare precum RoEduNet.

2. Resurse software:

- sisteme de operare pentru servere,
- proiectarea, dezvoltarea și testarea soluției,
- aplicații pentru înregistrarea datelor în Blockchain,
- aplicații pentru verificarea datelor.

3. Resurse pentru funcționarea Blockchain-ului propriu-zis:

- middleware,
- noduri Blockchain (server),
- mentenanță noduri (tehnicieni),
- mentenanța aplicațiilor utilizatorilor.

Resurse umane pentru implementare

Resursele umane necesare implementării se pot împărți în patru categorii:

- specialiștii care dezvoltă și implementează sistemul.
- specialiștii care instruiesc personalul care deservește sistemul.
- tehnicienii de mentenanță.
- utilizatorii.

1. Specialiștii care dezvoltă și implementează sistemul trebuie să creeze atât partea de server, „back-end”-ul Blockchain -ului, cât și aplicațiile „front-end” prin intermediul cărora se va face administrarea sistemului și se pot autentifica utilizatorii. Acești utilizatori pot fi persoane fizice, juridice, instituții care prin intermediul aplicației „front-end” pot emite documente oficiale, sau verifica autenticitatea documentelor. Pentru transparență, acesta trebuie să de tip public.

Din păcate, deși sunt mulți specialiști IT pe piață, deoarece tehnologia Blockchain este

relativ nouă, sunt foarte puțini cei specializați în acest domeniu. Partea bună este ca se pot specializa relativ ușor astfel de specialiști chiar dacă prețul unor cursuri poate fi ridicat iar acești specialiști vor trebui plătiți destul de bine.

Aceștia trebuie să aibă cunoștințe aprofundate în programare, criptografie, stocare distribuită, contracte inteligente, stocare distribuită și interoperabilitate.

Dacă API-ul sistemului server este dezvoltat corect, atunci dezvoltatorii aplicațiilor client nu au nevoie de multe cunoștințe despre Blockchain, sau chiar deloc. Aceștia trebuie doar să realizeze interfața utilizator și astfel de specialiști sunt ușor de găsit.

2. Specialiștii care instruiesc personalul care deservește sistemul Blockchain propriu-zis. Chiar dacă puțin diferite de cele pentru dezvoltarea sistemului, acești specialiști trebuie să dețină abilități specifice DLT și Blockchain iar acești specialiști sunt la fel de greu de găsit.

3. Tehnicienii de mentenanță trebuie să se ocupe de păstrarea în funcțiune și depanarea hardware-ului și software-ului, al aplicațiilor client. Menținerea la zi al sistemului este tot sarcina lor, precum și monitorizarea atât al părții hard cât și soft. Ei trebuie să raporteze orice problemă sau defect de sistem specialiștilor pentru a putea fi remediat în cel mai scurt timp. Pentru această parte există specialiști bine pregătiți, cu experiență, care gestionează astfel de sisteme chiar și acum, pentru diverse soluții software.

4. Utilizatorii care se ocupă de gestionarea și protecția datelor pe Blockchain, respectiv care verifică validitatea lor, emitenții sunt utilizatorii finali ai sistemului propus. Menținerea aplicațiilor client pentru această categorie nu sunt o problemă și sunt specialiști buni pentru asta. Softul client trebuie să fie ușor de utilizat iar accesul la Blockchain să se facă într-un mod transparent.

Resurse financiare pentru implementare

Implementarea unui proiect pilot pentru utilizarea tehnologiei Blockchain în identificarea unei persoane, cât și pentru gestiunea și protecția datelor cu caracter personal va implica o serie de costuri semnificative având în vedere că numeroase Instituții utilizează astfel de date. Pentru a putea partaja datele într-un mod responsabil și securizat, toate acestea trebuie să implementeze sistemul și să facă parte din rețea.

Diferite tipuri de categorii de costuri implicate într-un astfel de proiect sunt:

- Costuri de analiză și cercetare a proiectului din punct de vedere tehnic.
- Costuri de dezvoltare software a sistemului.
- Costuri de infrastructură hardware.
- Costuri de integrare a acestuia cu sistemele existente.
- Costuri pentru resursele umane care vor utiliza sistemul.

- Costuri pentru testarea sistemului.
- Costuri pentru mentenanța sistemului.
- Costuri pentru monitorizarea sistemului.

O estimare a acestor costuri a fost enunțată în continuare (vezi tabelul nr. 4):

Tip cost	Necesar estimat	Suma estimată
Costuri de analiză și cercetare a proiectului din punct de vedere tehnic	Salariu mediu lunar brut pentru: - Expert Coordonator - Expert ADR - Expert Securitate - Expert Documentare	2800 RON (65 RON/h -> 42 ore/luna) per Expert timp de 1 an de zile până sunt dezvoltăți toți pașii
Costuri dezvoltare software	Salariu mediu lunar brut dezvoltator software ¹⁵ Sistem de operare: open-source/gratuit (Linux/BSD). Software blockchain: open-source/gratuit. Software gestiune server/sistem de operare/blockchain: open-source/gratuit.	13586 RON (85 RON/h) per dezvoltator, iar costurile pot fi mai mari fiind vorba de o tehnologie nouă Sistem de operare: 0 RON Software: 0 RON.
Costuri de infrastructură hardware	Server: 10 bucăți, câte două per locație (cu echilibrare de sarcină). Stocare online: 1TB/server, în configurație RAID cu disponibilitate ridicată. Stocare offline (copii de rezervă): discuri hot-swap sau unități de bandă LTO. Conectivitate rețea: abonament de bandă largă și disponibilitate ridicată.	Server cu discuri în RAID incluse: 70000 RON/server , 700000 RON/10 servere. Stocare offline pe cartușe LTO-9: 722 RON/cartuș (16 RON/TB), 17000 RON/unitate de scriere/citire (estimare 2022). Conectivitate Internet, fibră optică 10Gbps: 50-100 RON/lună (preconizat 2022).
Costuri pregătire resurse	Cel puțin un utilizator cu pregătire	Creare și diseminare

¹⁵ Institutul Național de Statistică. Câștigul salarial mediu lunar.
<https://insse.ro/cms/ro/content/c%C3%A2%C8%99tigul-salarial-mediulunar-78>.

umane	în domeniu, per Instituție.	materiale instructionale online: 1500 RON.
Costuri mentenanță / monitorizare	Soft, hard, sysadmin, specialist blockchain. Electricitate server x 10. Costuri adiționale (clădire, administrație, altele).	Salariu brut lunar administrator de sistem: 13586 RON (85 RON/h). Salariu brut lunar specialist blockchain: 13586 RON (85 RON/h). Electricitate server: 500 RON/server/lună, 5000 RON/lună/zece servere. Depanarea/înlocuirea componentelor care se defectează: în medie aproximativ 5% din costul lunar de funcționare.

Tabelul nr. 4: Estimarea costurilor implementării.

Resurse logistice pentru implementare

Din punct de vedere logistic, sistemul propus presupune anumite cerințe și acestea sunt determinate de caracteristica distribuită a unui sistem Blockchain, de scopul acestuia, de actorii diverși pe care îi implică (Instituții, angajați publici și privați, etc). Această inițiativă presupune o colaborare strânsă între diferite Instituții, colaborare ce nu există în momentul de față. Necesarul de coordonare și interoperabilitate tehnică este de asemenea un punct important în aceste demers.

Totodată, utilizarea unui sistem bazat pe tehnologia Blockchain necesită pregătirea în prealabil a personalului pentru a putea utiliza noul sistem în realizarea de acte ce conțin date cu caracter personal, acestea fiind informații cu o sensibilitate mare. O pregătire corespunzătoare este necesară.

Riscuri și planuri de contingență

O soluție bazată pe tehnologia Blockchain pentru identificarea persoanelor, gestionarea și protecția datelor cu caracter personal presupune numeroase riscuri fiind vorba de o tehnologie nouă ce presupune un proiect nou. Câteva dintre posibile riscuri sunt următoarele:

- **Riscuri de finanțare:**
 - Diminuarea fondurilor de implementare.
 - Depășirea termenelor de predare a proiectului.
- **Riscuri legislative:**
 - Lipsa unei autorități legale de reglementare a utilizării tehnologiei Blockchain.
 - Lipsă de coordonare între autorități de reglementare naționale / internaționale.
- **Riscuri ale costurilor de întreținere:**
 - Diminuarea/Încetarea fondurilor de implementare pe termen lung.
 - Lipsa personalului calificat.
- **Riscuri de ocupare:**
 - Lipsa personalului.
 - Lipsa specialiștilor.
- **Riscuri operaționale:**
 - Probleme de securitate.
 - Probleme tehnice.
 - Probleme de scalabilitate.
 - Probleme de valabilitate.
 - Probleme de mentenanță.
- **Riscuri de planificare:**
 - Posibilitatea depășirii fondurilor alocate inițial.
 - Posibilitatea depășirii termenelor limită.
 - Volatilitatea resurselor umane.
- **Riscuri de schimbare a opțiunilor politice (riscuri decizionale):**
 - Diminuarea/Încetarea fondurilor de implementare pe termen lung.
 - Schimbarea climatului politic favorabil realizării proiectului.
- **Riscuri legate de procedurile de achiziții publice:**
 - Nerespectarea regulamentelor.
 - Încălcarea legilor privind datele cu caracter personal.
 - Nerespectarea standardelor.
- **Riscuri legate de acuratețea informațiilor:**
 - Implementare defectuoasă a sistemului.
 - Expunerea de date cu caracter personal.
- **Riscuri reputaționale (influența opiniei publice):**
 - Pierderea încrederii în sistem.
 - Reticență în folosirea sistemului.

- **Riscuri ale schimbărilor tehnologice:**
 - Compatibilitatea cu sistemul anterior poate genera probleme.
 - Probleme de autenticitate.
 - Probleme de securitate în utilizarea datelor cu caracter personal.
 - Lipsa documentației sistemului actual.
 - Incompatibilitate a datelor.
- **Riscuri ale volumului de activitate estimat:**
 - Imposibilitatea scalării aplicației.
 - Căderea/Blocarea sistemului.

Interacțiunea cu alte sisteme tehnice

Deoarece țara noastră face parte din UE, sistemul tehnic ce urmează a fi implementat trebuie să respecte directivele EBSI referitoare la acest domeniu. Arhitectura EBSI va fi construită în jurul unor principii puternice (cu respectarea deplină a reglementărilor UE) pentru a asigura flexibilitate pentru multitudinea de domenii ce vor fi implementate în infrastructura europeană.

Cele șase reguli stabilite de EBSI sunt:

- sisteme de tip "public permissioned" unde se cunoaște identitatea tuturor participanților din noduri.
- sistem obligatoriu descentralizat unde fiecare membru trebuie să își ruleze propriul cod sau set de noduri.
- scalabilitate, prin care se poate crește numărul de noduri ușor și acomodarea multor utilizatori.
- open source cu licență publică și liber de orice drept de proprietate intelectuală.
- sustenabil și fără POW.
- interoperabilitate, să se bazeze pe standarde bine cunoscute și specificații tehnice compatibile cu alte sisteme existente.

Având aceste constrângeri, sistemul propus trebuie să îndeplinească aceste caracteristici, cea mai importantă fiind **interoperabilitatea**. O caracteristică aparte a stocării înregistrărilor într-un blockchain este longevitatea stocării și imposibilitatea ștergerii sau alterării. De aceea, este necesară interoperabilitatea cu alte sisteme similare folosite pentru gestionarea datelor în cadrul Uniunii Europene.

Este necesară planificarea de la început a interoperabilității cu alte sisteme existente sau proiectate din cadrul EBSI a Comisiei Europene.

EBSI își propune să se impună în „practic” fiecare sector public care poate beneficia de tehnologia blockchain. Acest lucru va fi realizat cu o rețea de noduri distribuite în toată Europa, incluzând un număr tot mai mare de aplicații care acum sunt specializate pe cazuri specifice

(diplome academice, evidența populației, etc.).

Compatibilitate cu reglementările existente referitoare la protecția datelor și GDPR.

Următoarea figură (*figura nr.1*) este o ilustrare vizuală a rolurilor și acordurilor cheie din cadrul legal al platformei Sovrin pentru conformitatea reglementărilor privind protecția datelor. Deși folosește termeni din GDPR, este destinat respectării reglementărilor privind protecția datelor în general.

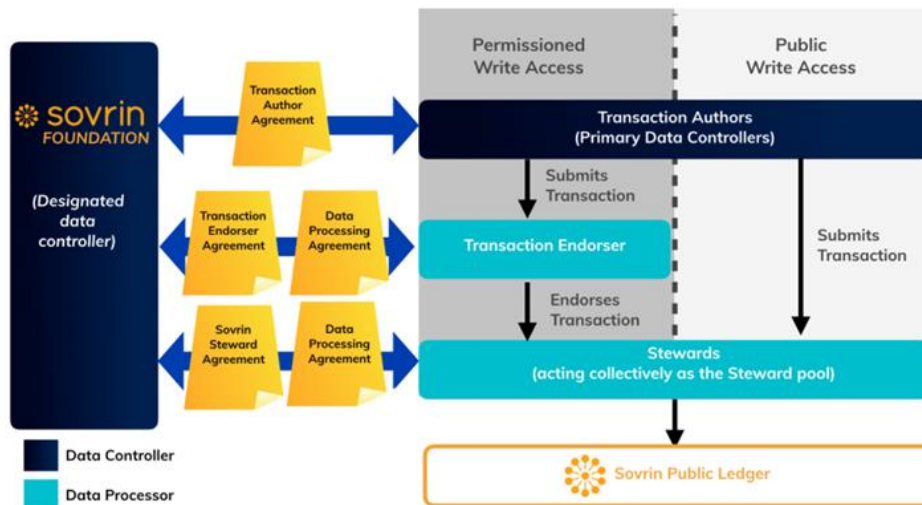


Figura nr.1: Infrastructura platformei Sovrin¹⁶.

Diagrama pentru implementare

Activitățile principale de implementare a soluției menționate anterior în vederea realizării unui sistem pentru identitatea persoanelor, gestionarea și securitatea datelor cu caracter personal cu ajutorul tehnologiei Blockchain sunt prezentate în tabelul următor (*figura.nr. 5.*):

Activitate	Perioadă, ani						
	1	2	3	4	5	6	>10
Planificarea proiectului și proiectare sistem, interfață utilizator, cod sursă							
Planificarea interfeței utilizator și realizarea codului sursă							
Dezvoltare și testare sistemului							
Formare și instruire personal							

¹⁶ Sovrin, <https://sovrin.org/overview/>.

Implementare pe platforme de tip "cloud", livrare, aplicații							
Migrare soluție existentă pe platforma blockchain							
Întreținere, actualizare, testare							
Actualizare, optimizare funcții noi, contracte inteligente							

Tabelul nr. 5: Diagrama pentru implementare.

Metodologia de management a proiectului și modelul de dezvoltare

Un astfel de proiect ce presupune multiple dependențe începând de la resurse umane până la resurse fizice trebuie să ofere vizibilitate și transparență. Sistemul propus este de tip public, deschis, conform cu recomandările EBSI. Uniunea Europeană dorește construirea unui blockchain paneuropean de servicii publice. Astfel, organizațiile terțe, instituțiile, organizațiile care se ocupă de identitatea persoanelor, gestionarea și protecția datelor personale pot citi datele din blockchain. Desigur, modalitatea de gestionare al acestor date sensibile trebuie să respecte reglementările GDPR.

Precondiții și factori critici pentru succes

Precondițiile implementării proiectului sunt condiționate de factorii următori:

- existența unui cadru legislativ pentru tehnologia bazată pe blockchain.
- colaborarea autorităților de reglementare și al factorilor de decizie pentru asigurarea acestui cadru legislativ favorabil.
- alinierea la standardele internaționale existente în acest domeniu și mai ales la condițiile impuse de EBSI privind tipul de Blockchain agreat la nivel european.

Factorii critici care împiedică realizarea cu succes al proiectului sunt:

- respectarea bugetului planificat și a criteriilor de timp.
- respectarea obiectivelor și direcțiilor de urmat care sunt definite în proiect.
- limitări privind competența membrilor echipei de proiect.
- dificultatea găsirii și angajării specialiștilor care sunt indispensabili pentru demararea și derularea proiectului.
- rolurile și responsabilitățile definite clar și asumate de părțile implicate.
- comunicarea și consultarea cu părțile implicate pentru implementarea cu succes al unui astfel de proiect.
- lipsa componentei legislative care să permită demararea unui astfel de proiect.

- nu există încă un consens asupra unui standard european clar definit pentru acest domeniu, deși EBSI are propuneri la nivel european în acest sens, aceasta este doar la nivel de idee.

Indicatori pentru monitorizare și evaluare

1. **Indicatori de ieșire:** “ produse ” intenționate (sau neintenționate) ale intervenției. Acestea pot fi atât componente fizice (servere, rețelistică), cât și software (interfețe pentru utilizatori, middleware, sisteme de validare în rețeaua de noduri blockchain).
2. **Indicatori de rezultat:** modificări comportamentale la nivel individual sau instituțional ca urmare a intervenției. Transparență, timp redus pentru validarea documentelor și verificarea lor. Un flux de documente realizate prin transparență, siguranță, dar și o încredere reciprocă. Identificare rapidă a documentelor în sistem. Utilizare facilă și proceduri simplificate.
3. **Indicatori de impact:** îmbunătățiri sustenabile la nivelul grupului țintă / al beneficiarilor direcți și indirecti. Eliminarea fraudelor. Reducerea timpului necesar pentru emiterea sau verificarea unui document sau al unei identități.

După recepția sistemului, acesta va funcționa cu drepturi depline, dar se vor folosi o perioadă și sistemele vechi. Acest lucru se datorează în primul rând faptului că vor exista reticente inevitabile din partea părților, datorită noutății sistemului și al modului cum funcționează. A doua cauză este faptul că sistemul fiind în teste, vor exista erori inevitabile, de aceea, se vor folosi sistemele vechi ca rezervă de siguranță. Trecerea și migrarea totală la sistemul bazat pe blockchain va fi atins în câțiva ani de la lansarea propriu-zisă.

Referințe bibliografice

1. CNIL — *Blockchain and the GDPR: Solutions for a responsible use of the Blockchain in the context of personal data*, 6 November 2018, <https://www.cnil.fr/en/Blockchain-and-gdpr-solutions-responsible-use-Blockchain-context-personal-data>
2. https://www.euBlockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf
3. [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf).
4. *Caz utilizare Blockchain în Zug, Elveția*, <https://blockchan.ge/blockchange-government-services.pdf>.
5. *Caz utilizare Blockchain în Guvernul din Catalonia*, <https://politiquesdigitals.gencat.cat/en/tic/estrategia-Blockchain/>
6. *Caz utilizare Blockchain în Guvernul din Finlanda*, <https://reliefweb.int/report/finland/how-finland-using-Blockchain-revolutionise->

[financial-services-refugees](#) .

7. Caz utilizare Blockchain în Guvernul din Moldova,
<https://www.reuters.com/article/moldova-Blockchain-child-trafficking-idUKL8N1NK55K>.
8. Cazuri utilizare Block Chain în Guvernul din Moldova,
<https://ideas.unite.un.org/Blockchain4humanity/Page/ViewIdea?ideaid=390>
9. Cele șapte legi ale identității digitale ale lui Cameron,
<https://www.identityblog.com/?p=1065>.
10. Sovrin, <https://sovrin.org/overview/>.
11. P. Rimba, A. B. Tran, I. Weber, M. Staples A. Ponomarev, X. Xu, *Comparing Blockchain and Cloud Services for Business Process Execution*, In Proc. International Conference on Software Architecture (ICSA 2017).
12. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, disponibil la <https://bitcoin.org/bitcoin.pdf>.
13. Stan, O.P.; Enyedi, S.; Corches, C.; Flonta, S.; Stefan, I.; Gota, D.; Miclea, L. *Method to Increase Dependability in a Cloud -Fog-Edge Environment*. *Sensors* 2021, 21, 4714, <https://doi.org/10.3390/s21144714>.
14. A. Avizienis. J.-C.. Laprie, B. Randell, and C. Landwehr, *Basic concepts and taxonomy of dependable and secure computing*, *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, Jan 2004.
15. Institutul Național de Statistică. *Câștigul salarial mediu lunar*.
<https://insse.ro/cms/ro/content/c%C3%A2%C8%99tigul-salarial-mediu-lunar-78>.



Proiect:

Proiect selectat în cadrul Programului Operațional Capacitate Administrativă cofinanțat de Uniunea Europeană, din Fondul Social European

Axa Prioritară 1: Administrație publică și sistem judiciar eficiente

Obiectivul specific 1.1: Dezvoltarea și introducerea de sisteme și standarde comune în administrația publică ce optimizează procesele decizionale orientate către cetățeni și mediul de afaceri, în concordanță cu SCAP.

Titlul proiectului: „Cadru strategic pentru adoptarea și utilizarea de tehnologii inovative în administrația publică 2021-2027 – soluții pentru eficientizarea activității”

COD: SIPOCA 704

Beneficiar: AUTORITATEA PENTRU DIGITALIZAREA ROMÂNIEI

Partener: UNIVERSITATEA TEHNICĂ DIN CLUJ - NAPOCA

Fundamentarea cazului de utilizare și studiu de evaluare ex-ante pentru Managementul proprietății intelectuale

Cuprins

Acronime și abrevieri	3
Scopul intervenției	4
Părțile interesate.....	5
Beneficiile estimate.....	5
Factori critici în asociere cu cazurile de utilizare	6
Provocări tehnice în implementarea intervenției.....	7
Procese curente care ar putea fi afectate de dezvoltarea proiectului	7
Obiectivele funcționale	7
Obiectivele de performanță.....	8
Elementele de noutate	9
Criteriile de selecție	9
Descrierea în detaliu a cazului de referință	10
Opțiuni de îmbunătățire	11
Analiza comparativă.....	12
Constrângeri privind implementarea.....	15
Resurse tehnice pentru implementare	15
Resurse umane pentru implementare.....	16
Resurse financiare pentru implementare.....	17
Resurse logistice pentru implementare.....	18
Riscuri și planuri de contingență.....	18
Interacțiunea cu alte sisteme tehnice	19
Diagrama pentru implementare	20
Metodologia de management a proiectului și modelul de dezvoltare	20
Precondiții și factori critici pentru succes	21
Indicatori pentru monitorizare și evaluare	22
Referințe bibliografice	22

Acronime și abrevieri

Abreviere sau acronim	Expresia completă	Explicație
ORDA	Oficiul Român pentru Drepturile de Autor	
OSIM	Oficiul de Stat pentru Invenții și Mărci	
WIPO	World Intellectual Property Organization	
EUIPRO	European Union IP Office	
DLT	Distributed Ledger Technology	Tehnologie de tip registru distribuit.
DIDs	Decentralized identifiers	Tip nou de identificator care permite o identitate digitală descentralizată și verificabilă.
EBSI	European Blockchain Services Infrastructure	Infrastructura europeană pentru servicii blockchain, promovată de Comisia Europeană.
IdM	Identity Management	Cadru de politici și tehnologii pentru a se asigura că utilizatorii potriviți (într-o întreprindere) au acces adecvat la resursele tehnologice.
WOT	web-of-trust	Este un concept utilizat în PGP, GnuPG și alte sisteme compatibile cu OpenPGP pentru a stabili autenticitatea legăturii dintre o cheie publică și proprietarul acesteia.
EVM	Ethereum Virtual Machine	
PGP	Pretty Good Privacy	Program de criptare care oferă confidențialitate criptografică și autentificare pentru comunicarea datelor.
POW	Proof-of-Work	O formă de dovadă criptografică în care o parte demonstrează altora munca pentru a fi remunerat.
PBFT	Practical Byzantine Fault Tolerance	Un sistem care are un nod primar și noduri secundare. Aceste noduri lucrează împreună pentru a ajunge la un consens, făcând din acest sistem una dintre soluțiile la Problema Generalilor Bizantini.
PCT	The International Patent System	

Scopul intervenției

Proprietatea intelectuală privită sub cele două componente ale sale, **proprietatea industrială** pe de o parte și **drepturile de autor** și **drepturile conexe** pe de altă parte, este una dintre pârgurile de bază ale dezvoltării economice, sociale și culturale ale națiunii¹.

În acest context se poate aprecia că protecția drepturilor de proprietate intelectuală este de o mare importanță, esența, scopul și finalitatea acesteia fiind protejarea produsului inteligenței umane și, în același timp, garantarea beneficiului consumatorilor de a se folosi de acest produs.

Strâns legată de acest domeniu este activitatea de cercetare – dezvoltare și inovare care constituie o componentă strategică, hotărâtoare pentru dezvoltarea economică și pentru progresul social.

Astfel, știința, tehnologia și inovarea reprezintă domenii care generează constant progres tehnologic, asigurând durabilitatea dezvoltării și competitivitatea economică de perspectivă a României.

Platformele blockchain creează un lanț de informații transparent și (probabil) imuabil (adică neschimbabil). Aceste caracteristici ar putea oferi birourilor de proprietate intelectuală (PI) oportunitatea de a transforma înregistrarea drepturilor de proprietate intelectuală, făcând procesul mai rentabil, mai rapid, mai precis și mai sigur. În plus, tehnologia ar putea oferi o oportunitate de a transforma eficiența și transparența informațiilor de gestionare a drepturilor.²

Obiectivele generale

- Creșterea eficienței și a transparenței informațiilor de gestionare a drepturilor de PI folosind tehnologia blockchain.

Obiectivele specifice

- Înregistrarea drepturilor de PI prin tehnologia blockchain;
- Verificarea autenticității drepturilor de PI;
- Stabilirea drepturilor de autor folosind tehnologia blockchain.

Obiectivele operaționale

- Determinarea capacității de creație, dovada proprietății și originea operelor creative;

¹ EURAXESS ROMANIA, Working in Europe | Intellectual Property Rights | Romania. Accesat online în Noiembrie 2021, <https://www.euraxess.gov.ro/ro/romania/informatii-si-asistenta/proprietate-intelectuala>.

² Anne Rose, Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights, WIPO Magazine, 2020. Accesat online în Noiembrie 2021, https://www.wipo.int/wipo_magazine_digital/en/2020/article_0002.html.

- Folosirea tehnologiei blockchain ca un registru distribuit de PI;
- Gestionarea drepturilor de PI și practicile de transfer și comercializare.

Care sunt granițele de utilizare/aplicabilitate avute în vedere?

- Puterea de procesare necesară a blockchain-urilor;
- Compatibilitatea și interoperabilitatea diferitelor platforme blockchain;
- Problemele legale, cum ar fi proprietatea datelor, confidențialitatea, răspunderea și jurisdicția.

Părțile interesate

Beneficiarii realizării unui registru distribuit de PI ar putea fi:

- Principalele instituții de specialitate responsabile cu protecția PI (OSIM și ORDA)
- Societăți comerciale;
- Deținătorii drepturilor de autor și utilizatorii acestora.

Câteva caracteristici ale tehnologiei blockchain, în special capacitatea sa de a cripta datele și de a stoca și partaja informații în siguranță, o fac, de asemenea, potrivită pentru protejarea și aplicarea secretelor comerciale. Tehnologia blockchain poate ajuta la diferite etape ale ciclului de viață al unui secret comercial, în special când vine vorba de „măsura rezonabilă a protecției” și aplicarea unui secret comercial, adică capacitatea de a dovedi că informațiile au fost păstrate secrete în cazul unei deturnări³.

Crearea unui inventar de secrete comerciale și înregistrarea celor care au avut acces la informații au fost în mod tradițional considerate ca făcând un „pas rezonabil” pentru a menține confidențialitatea, iar înregistrarea unui secret comercial pe o platformă blockchain ar putea îndeplini această cerință în conformitate cu Directiva UE privind secretele comerciale și legile echivalente⁴.

Părțile interesate vor fi consultate permanent în procesul de luare a deciziilor cu privire la soluția propusă. Acest lucru se va realiza prin organizarea de sondaje pe bază de chestionare și prin dezbateri publice, la care sunt invitați să participe toate părțile interesate.

Beneficiile estimate

³ Dr. Birgit Clark, Baker McKenzie and Ruth Burstall, Johnson & Johnson
Crypto-Pie in the Sky? How Blockchain Technology is Impacting Intellectual Property Law,
Stanford Journal of Blockchain Law & Policy, June 2019.

⁴ Dr. Birgit Clark, Baker McKenzie and Ruth Burstall, Johnson & Johnson
Crypto-Pie in the Sky? How Blockchain Technology is Impacting Intellectual Property Law,
Stanford Journal of Blockchain Law & Policy, June 2019.

Potențialul de a utiliza tehnologia blockchain pentru gestionarea drepturilor de PI este vast. Înregistrarea drepturilor de PI într-un registru distribuit, mai degrabă decât într-o bază de date tradițională, le-ar putea transforma efectiv în „drepturi de IP inteligente”⁵. Capacitatea de a urmări întregul ciclu de viață al unui drept ar avea multe beneficii, cum ar fi:

- Audituri mai fluide ale drepturilor de PI;
- Simplificarea exercițiilor de verificare a antecedentelor care sunt necesare pentru tranzacțiile cu PI, de exemplu în cazul fuziunilor și achizițiilor;
- Preocupările de confidențialitate din partea deținătorilor IP ar putea fi rezolvate printr-o schemă de înscriere;
- Eficientizarea procesului de înregistrare a modelelor și mărcilor comerciale prin reducerea unora dintre procese și proceduri;
- Crearea unui registru de drepturi de PI neînregistrate, cum ar fi drepturile de proiectare neînregistrate și drepturile de autor, deoarece poate furniza cu ușurință dovezi ale momentului creării, informații despre gestionarea drepturilor (dacă este cazul) și cerințele juridictionale;
- Costuri scăzute prin reducerea numărului de interacțiuni complexe cu guvernele locale și naționale;
- Dezvoltarea unui proces de înregistrare a drepturilor de PI complet automatizat, care ar face posibilă afirmarea drepturilor de PI fără intervenția umană sau chiar fără necesitatea unui instituții.

Factori critici în asociere cu cazurile de utilizare

- Pentru informațiile care nu sunt native pentru blockchain, nu se poate garanta autenticitatea acestora în momentul înregistrării.
- Neclaritatea rezolvării conflictelor (fără o parte terță de încredere) în cazul introducerii incorecte a informațiilor despre proprietatea drepturilor de autor.
- Înregistrările din registru nu mai oferă un certificat de încredere de proprietate dacă PI este transferată în afara rețelei.
- Instabilitatea metodelor de plată pentru gestionarea descentralizată a drepturilor de autor, deoarece criptomodele nu sunt încă suficient de stabile.
- Publicitatea negativă din jurul blockchain-urilor existente (adică, criptomonede) și care afectează rata de adoptare a tehnologiei de bază în aproape fiecare sector.
- Tehnologia blockchain, în general, este destul de complexă și adesea greu de înțeles în termeni tehnici, ceea ce ridică suspiciunea publicului larg și rezistența pe care o întâmpină adesea astfel de tehnologii.

⁵ Anne Rose, Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights, WIPO Magazine, 2020. Accesat online în Noiembrie 2021, https://www.wipo.int/wipo_magazine_digital/en/2020/article_0002.html.

- Dimensiunea mare a datelor create dacă gestionarea drepturilor de autor ar fi realizată prin utilizarea tehnologiei blockchain.
- Dintr-o perspectivă juridică, cea mai dificilă provocare pentru adoptarea tehnologiei blockchain pentru managementul PI pare să fie reglementarea acestei tehnologii.

Provocări tehnice în implementarea intervenției

Principalele provocări de natură tehnică în implementarea unui registru distribuit pentru managementul PI, folosind tehnologia blockchain, sunt⁶:

- Dificultatea de a explica și înțelege complexitatea tehnologiei în sine.
- Deoarece utilizatorii unui sistem blockchain sunt, de asemenea, nodurile sistemului într-un blockchain, fiecare utilizator ar trebui să stocheze cantități masive de date.
- Este adesea dificil să se determine ce legi și reglementări ale jurisdicțiilor se aplică unei anumite aplicații blockchain, deoarece nodurile unui registru descentralizat se pot întinde pe mai multe locații din întreaga lume, rezultând un număr mare de legi și reglementări care s-ar putea aplica tranzacțiilor într-un sistem bazat pe blockchain.
- În ceea ce privește contractele inteligente în special, dacă există ambiguitate în ceea ce privește locația în care a fost încheiat contractul, instanțele vor trebui să găsească o metodă de definire și stabilire a locului de încheiere a contractului inteligent.
- În plus, faptul că contractele inteligente nu necesită neapărat aplicarea legii le poate face atractive pentru tranzacțiile ilegale.

Procese curente care ar putea fi afectate de dezvoltarea proiectului

Principalele procese curente care ar putea fi afectate de utilizarea unui sistem de gestiune a drepturilor de PI, bazat pe tehnologia blockchain, sunt următoarele:

- Procesul de înregistrare a drepturilor de PI;
- Procesul de gestionare a drepturilor de PI;
- Procesul de recompensare a deținătorilor drepturilor de PI.

O detaliere a modului în care procesele curente ar putea fi afectate de folosirea tehnologiei blockchain, pentru gestionarea drepturilor de PI, este prezentată în subcapitolele 15 și 17.

Obiectivele funcționale

⁶ Hauck R. (2021) Blockchain, smart contracts and intellectual property. Using distributed ledger technology to protect, license and enforce intellectual property rights. Legal Issues in the Digital Age, no 1, pp. 17–41.

Procesul de înregistrare poate fi ușurat semnificativ prin adoptarea și recunoașterea tehnologiei blockchain ca registru. Tehnologia blockchain ar putea fi folosită ca o bază de date unificată care permite oricui să ajungă la informațiile imuabile și de încredere stocate acolo. Cu ajutorul unor aplicații care să ruleze pe aceste structuri blockchain înregistrarea s-ar putea realiza fără implicarea unei autorități și eliminarea unui proces de aplicare. Natura globală a tehnologiei blockchain ar permite depășirea cerinței de **înregistrare a drepturilor de PI în diferite legislații** și de a face față diferitelor proceduri ale acestora.

Deoarece procesul ar fi efectuat într-un mod relativ automatizat, **s-ar reduce semnificativ taxele și cheltuielile.**

Construirea unui sistem, în care deținătorii de drepturi pot controla modul în care își gestionează PI în ceea ce privește contractarea și colectarea redevențelor poate **stimula în mod semnificativ motivația din spatele creației și invențiilor** și poate juca un rol important în direcționarea consumatorilor de la produsele contrafăcute către produsele originale prin **îmbunătățirea accesibilității PI originale pentru consumatori**⁷.

Obiectivele de performanță

Principalele caracteristici de performanță tehnică ale soluției propuse sunt⁸:

- **Imuabilitatea** înseamnă ceva care nu poate fi schimbat sau alterat. Aceasta este una dintre caracteristicile de top ale blockchain-ului care ajută la asigurarea faptului că tehnologia va rămâne așa cum este - o rețea permanentă, inalterabilă.
- Rețeaua este **descentralizată**, ceea ce înseamnă că nu are nici o autoritate de guvernare sau o singură persoană care se ocupă de cadru. Mai degrabă un grup de noduri menține rețeaua făcând-o descentralizată.
- **Securitate sporită** deoarece nu există o autoritate centrală, nimeni nu poate schimba pur și simplu orice caracteristică a rețelei în beneficiul său. Utilizarea criptării asigură un alt nivel de securitate pentru sistem.
- **Registre contabile distribuite.** Acest lucru se datorează faptului că registrul în rețea este întreținut de toți ceilalți utilizatori ai sistemului. Puterea de calcul este distribuită între computere pentru asigurarea un rezultat mai bun.
- Fiecare blockchain prosperă datorită algoritmilor de **consens**. Arhitectura este proiectată inteligent, iar algoritmii de consens sunt în centrul acestei arhitecturi. Fiecare blockchain are un consens pentru a ajuta rețeaua să ia decizii.

⁷ Gönenç Gürkaynak, İlay Yılmaz, Burak Yeşilaltay, Berk Bengi, Intellectual property law and practice in the blockchain realm, Computer Law & Security Review, Volume 34, Issue 4, 2018, Pages 847-862, ISSN 0267-3649, doi.org/10.1016/j.clsr.2018.05.027.

⁸ Gwyneth Iredale, 6 Key Blockchain Features You Need To Know Now, Nov. 2020. Accesat online în Noiembrie 2021, <https://101blockchains.com/introduction-to-blockchain-features/>.

- **Decontare mai rapidă.** Sistemele bancare tradiționale sunt destul de lente. Uneori, procesarea unei tranzacții poate dura câteva zile după finalizarea tuturor decontărilor. De asemenea, poate fi coruptă destul de ușor. Blockchain oferă o decontare mai rapidă în comparație cu sistemele bancare tradiționale.
- Un alt aspect foarte promițător al blockchain-ului este conceptul de **contract inteligent**. Contractele inteligente sunt aplicate din punct de vedere tehnic pe blockchain în loc de aplicarea legală tradițională a legilor sau instanțele de arbitraj. Acestea definesc regulile și penalitățile în jurul unui acord și pun în aplicare automat aceste obligații⁹.

Elementele de noutate

Platformele blockchain sunt **descentralizate** și **imuabile** prin însăși natura tehnologiei de bază. Prin urmare, aceste caracteristici oferă oficiilor de PI, organizațiilor guvernamentale și instanțelor o oportunitate de a-și îmbunătăți operațiunile și procedurile, prin folosirea tehnologiei blockchain pentru a realiza o evidență mai rapidă și mai rentabilă într-un mediu mai sigur.

În plus, tehnologia blockchain este capabilă și potrivită pentru a rezolva o serie de probleme cu privire la aplicarea drepturilor de PI. Deoarece tehnologia în cauză oferă o modalitate ușoară de a demonstra și dovedi **existența** și **unicitatea** unui produs, ea permite, de asemenea, autorităților de aplicare a legii să detecteze cu ușurință produsele contrafăcute.

De asemenea, este de remarcat faptul că tehnologia blockchain poate fi folosită în cooperare cu o altă tehnologie promițătoare, **inteligența artificială** (IA), în special IA specifică domeniului. În domeniul drepturilor de PI, o astfel de cooperare poate permite ca **procesul de înregistrare** să fie finalizat de către sistemul însuși, aproape fără implicare sau aport uman.

Anumite evaluări ale PI, cum ar fi evaluarea „probabilității de confuzie” în cazurile privind mărcile comerciale sau evaluarea „existenței unei acțiuni inventive” într-o **cerere de brevet**, pot fi efectuate de software bazat pe IA. Având la îndemână toate fișierele în format electronic ale drepturilor de PI înregistrate și disponibile pentru utilizare pe blockchain, software-ul menționat mai sus va avea toate informațiile necesare pentru a face o astfel de evaluare cu **rapiditate** și **acuratețe**.

Criteriile de selecție

Criteriile de selecție pentru alegerea platformei blockchain sunt următoarele:

- **Restricții de permisiune** – Restricțiile de permisiune decid dacă procesatorii de tranzacții (minerii) care trimit date și sunt eligibili pentru a crea blocuri de date pot face acest lucru

⁹ Riviere, Jean. “Blockchain technology and IP - investigating benefits and acceptance in governments and legislations.” (2018).

fără permisiune sau sunt restricționați să facă acest lucru și au nevoie de permisiunea unei autorități centrale.

- **Acces la date** – Aceasta se referă la cine poate vizualiza (citi) datele tranzacțiilor din rețeaua blockchain.
- **Anonimat** – Se referă dacă identitatea utilizatorului este în mod deschis transparentă.
- **Debitul tranzacțiilor** – Se referă la viteza cu care un blockchain procesează tranzacțiile, care este de obicei exprimat în tranzacții pe secundă
- **Reglementare centralizată (guvernanță)** – Guvernanța se referă la gradul în care puterea de decizie este distribuită în comunitatea blockchain (cine poate lua ce decizii pe o platformă blockchain).
- **Mecanism de consens** – Mecanismul de consens este un mijloc de a determina un consens cu privire la toate tranzacțiile și starea curentă a sistemului. Mecanismul asigură că tranzacțiile vor fi adăugate în blockchain numai dacă sunt valide și nu sunt înregistrate niciodată de mai multe ori.
- **Contracte inteligente** – Este de fapt un sistem contractual acționabil care poate automatiza procesul oricăror contracte între părți.

Descrierea în detaliu a cazului de referință

Una dintre posibilele aplicații ale tehnologiei blockchain este legată de **gestionarea drepturilor de autor**. Odată ce o creație sau o lucrare care este supusă dreptului de autor (cum ar fi o piesă muzicală sau o scriere), este creat automat și un pachet de drepturi de proprietate intelectuală, iar aceste drepturi pot fi deținute de identități juridice diferite. După crearea (și de-a lungul anilor de existență) a acestor drepturi, **difficultatea de identificare a titularilor** lor de drept și de calculare a diferitelor sume de plăți datorate fiecărui titular de drept atunci când este utilizată creația/opera constituie o mare provocare pentru titularii de drepturi și licențiații operei protejate prin drepturi de autor. Înregistrările relevante în prezent sunt deținute fie de organisme guvernamentale, fie de companii private, fie de organizațiile deținătorilor de drepturi. Cu toate acestea, aceste baze de date nu sunt în mare parte interoperabile și nici nu sunt întotdeauna publice. **Costul menținerii unei baze de date publice și interoperabile** poate depăși și resursele disponibile ale unora dintre aceste organizații. **Securitatea acestor înregistrări** este, de asemenea, pusă sub semnul întrebării, iar drepturile de PI sunt în mare parte gestionate de părți externe (adică, nu de către deținătorii de drepturi înșiși). Ca urmare, **gestionarea acestor drepturi este costisitoare, complicată și consumatoare de timp**¹⁰.

Pentru **licențierea și transferul** drepturilor de PI înregistrate, înregistrarea în sine a acordului de licență/transfer este, de asemenea, o problemă ale cărei reguli **variază între jurisdicții**, în funcție de legislația aplicabilă. De exemplu, în Uniunea Europeană, această

¹⁰ Gönenç Gürkaynak, İlay Yılmaz, Burak Yeşilaltay, Berk Bengi, Intellectual property law and practice in the blockchain realm, Computer Law & Security Review, Volume 34, Issue 4, 2018, Pages 847-862, ISSN 0267-3649, doi.org/10.1016/j.clsr.2018.05.027.

problemă este reglementată de capitolul III al Convenției privind Brevetele Europene pentru Brevete. Conform acestei secțiuni, Oficiul European de Brevete, la cererea unei părți interesate, va înregistra un transfer sau o licență unui brevet. Pentru contractele de licență privind modelele, articolul 32/4 din Regulamentul (CE) nr. 6/2002 a propus o reglementare similară.

În România, asigurarea protecției proprietății intelectuale se realizează în principal prin două instituții de specialitate: **Oficiul de Stat pentru Invenții și Mărci** (OSIM) – în domeniul proprietății industriale și **Oficiul Român pentru Drepturile de Autor** (ORDA) – în domeniul dreptului de autor și al drepturilor conexe¹¹.

Opțiuni de îmbunătățire

O soluție la problemele menționate mai sus ar putea fi posibilă prin adoptarea unui **sistem de înregistrare blockchain**, în care drepturile legate de lucrarea protejată prin drepturi de autor ar constitui un bloc în lanț. Crearea unui astfel de sistem de la zero ar fi mai ieftină și mai ușoară (în ceea ce privește depășirea provocărilor sale tehnice) în comparație cu transformarea sistemului actual într-unul public, interoperabil. În plus, informațiile aflate în blockchain ar fi **disponibile pentru toată lumea**. Cu alte cuvinte, fiecare persoană care deține aplicația blockchain ar deveni un nod și, deși ar putea vedea întregul lanț, ar contribui, de asemenea, la securitatea sistemului, acționând ca un nod (și un server) fără a suporta costuri de server. Prin urmare, **costurile asociate** cu identificarea deținătorilor de drepturi ar fi reduse considerabil, deoarece timpul necesar pentru procesarea acestor informații ar putea fi doar de câteva minute, deoarece toate înregistrările ar fi stocate, de exemplu, într-un telefon inteligent sau într-o aplicație desktop, iar securitatea sistemului ar putea fi menținută și la un cost semnificativ mai mic¹².

Un alt beneficiu esențial al acestui sistem este că drepturile de PI ar fi **gestionate de proprietarii** lor înșiși, mai degrabă decât de părți externe. Pe lângă crearea operei și a drepturilor sale de PI, deținătorii de drepturi ar putea, de asemenea, să producă **contractele inteligente** care ar fi utilizate în eventualele tranzacții viitoare privind creația protejată prin drepturi de autor. Având astfel de contracte rulând pe un blockchain, procesarea unor astfel de tranzacții ar fi mult mai simplă și, prin acest sistem, proprietarii de drepturi ar putea să-și mărească câștigurile considerabil, deoarece costurile de tranzacție ar fi reduse substanțial¹³.

¹¹ EURAXESS ROMANIA, Working in Europe | Intellectual Property Rights | [Romania](https://www.euraxess.gov.ro/ro/romania/informatii-si-asistenta/proprietate-intelectuala). Accesat online în Noiembrie 2021, <https://www.euraxess.gov.ro/ro/romania/informatii-si-asistenta/proprietate-intelectuala>.

¹² Gönenç Gürkaynak, İlay Yılmaz, Burak Yeşilaltay, Berk Bengi, Intellectual property law and practice in the blockchain realm, Computer Law & Security Review, Volume 34, Issue 4, 2018, Pages 847-862, ISSN 0267-3649, doi.org/10.1016/j.clsr.2018.05.027.

¹³ Gönenç Gürkaynak, İlay Yılmaz, Burak Yeşilaltay, Berk Bengi, Intellectual property law and practice in the blockchain realm, Computer Law & Security Review, Volume 34, Issue 4, 2018, Pages 847-862, ISSN 0267-3649, doi.org/10.1016/j.clsr.2018.05.027.

Pentru ca tehnologia blockchain să poată fi aplicată cu succes în gestionarea drepturilor de PI, ar trebui să existe un set de standarde agreeat și susținut la **nivel internațional**. Va fi important ca autoritățile de reglementare și factorii de decizie să colaboreze pentru a contribui la modelarea implementării acestei tehnologii în legătură cu înregistrarea drepturilor de PI¹⁴.

Analiza comparativă

Pentru a înțelege mai bine aplicabilitatea potențială și valoarea tehnologiei blockchain pentru protecția IP, vom lua în considerare **înregistrarea unui model sau a unei mărci comerciale** în Uniunea Europeană (UE) și/sau Regatul Unit (Regatul Unit), în **situația actuală**. Înainte de a înregistra un design sau o marcă comercială, trebuie decis unde se dorește protejarea, de exemplu, în UE și/sau Regatul Unit. În al doilea rând, trebuie să se ia în considerare problemele de înregistrare. Pentru un design, este: (i) „nou”; și (ii) are un caracter individual (adică dă o impresie generală diferită unui utilizator informat în comparație cu orice modele anterioare care sunt deja în domeniul public)? Pentru o marcă comercială, se ia în considerare dacă marca comercială este distinctă și poate fi înregistrată, precum și produsele și/sau serviciile pentru care se dorește să se obțină protecție. De asemenea, se va dori ștergerea oricăror drepturi anterioare potențial conflictuale, efectuând căutări adecvate. În prezent, se poate utiliza aplicația Design View și TMView ale Oficiului de PI al Uniunii Europene (în engleză European Union IP Office – EUIPO) pentru a verifica starea desenelor și a mărcilor comerciale în statele membre ale UE, dar poate fi necesar să se efectueze căutări mai ample de autorizare, de exemplu, utilizând bazele de date cu mărci și baza de date globală ale WIPO sau prin efectuarea de căutări comerciale. În cele din urmă, trebuie să se plătească taxa de aplicare și să se depună cererea la EUIPO și/sau la Oficiul IP din Regatul Unit (în engleză, UK IP Office). Presupunând că nu există obiecții din partea Registrului sau opoziții ale terților, drepturile de desen sau model pot fi înregistrate în câteva zile de la data cererii, iar mărcile pot fi înregistrate în termen de patru luni de la data cererii¹⁵.

Tehnologia blockchain ar putea **eficientiza procesul de înregistrare** a modelelor și mărcilor comerciale prin reducerea unora dintre aceste procese și proceduri. Pentru unele cereri de marcă, de exemplu, în care nu este posibil să se demonstreze că marca este în mod inerent distinctiv, va fi necesar să se demonstreze că marca a dobândit caracter distinctiv prin utilizare. Presupunând că s-au făcut modificările necesare în lege pentru a permite ca utilizarea efectivă a unei mărci (de exemplu) să fie adăugată și înregistrată în registrul oficial, dovezile și informațiile privind utilizarea efectivă a unei mărci în comerț, precum și frecvența o astfel de utilizare, ar putea fi partajată cu ușurință și disponibilă pentru toată lumea să vadă pe un blockchain. Dacă

¹⁴ Anne Rose, Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights, WIPO Magazine, 2020. Accesat online în Noiembrie 2021, https://www.wipo.int/wipo_magazine_digital/en/2020/article_0002.html.

¹⁵ Anne Rose, Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights, WIPO Magazine, 2020. Accesat online în Noiembrie 2021, https://www.wipo.int/wipo_magazine_digital/en/2020/article_0002.html.

proprietarii mărcilor ar decide să pună la dispoziție gratuit astfel de informații, acest lucru ar economisi timp și costuri semnificative¹⁶.

Pentru a stabili și a **menține drepturile asupra mărcii comerciale** în UE și Regatul Unit după înregistrare, poate deveni important pentru un titular de drept să demonstreze utilizarea autentică într-o anumită perioadă. Capacitatea de a furniza dovezi ale utilizării continue sau anterioare a unei mărci comerciale poate fi un proces laborios care implică colectarea îndelungată și costisitoare a înregistrărilor relevante pentru a demonstra utilizarea unei mărci comerciale¹⁷.

Pentru a ajuta acest proces, s-ar putea implementa un **contract inteligent** pe un blockchain (adică un cod de calcul cu auto-execuție care își procesează automat intrările atunci când este declanșat). Un astfel de contract ar putea oferi **dovada unei mărci temporale a primei utilizări sau a utilizării ulterioare a unei mărci comerciale**, care ar putea fi apoi prezentată (dacă este acceptată) instanței ca dovadă¹⁸.

În continuare se va realiza o analiză comparativă între două platforme blockchain pe care se pot implementa aplicații pentru managementul PI (vezi tabelul 1).

Tabelul 1: Compararea caracteristicilor blockchain¹⁹

	Ethereum	Hyperledger Fabric
Tip registru	Fără permisiuni	Cu permisiuni
Acces la date	Public sau privat	Privat
Anonimat	Pseudonim, fără criptare a datelor tranzacției	Pseudonim, cu criptare a datelor tranzacției
Orientare pe industrie	Intersectorial	Intersectorial
Guvernață	Dezvoltatorii Ethereum	Fundația Linux
Criptomonedă	Ether (ETH)	Fără
Mecanism de consens	Proof of Work (PoW)	Mecanism conectabil
Throughput	~ 20 tps	> 2000 tps
Contracte inteligente	✓	✓

¹⁶ Anne Rose, Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights, WIPO Magazine, 2020. Accesat online în Noiembrie 2021, https://www.wipo.int/wipo_magazine_digital/en/2020/article_0002.html.

¹⁷ Anne Rose, Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights, WIPO Magazine, 2020. Accesat online în Noiembrie 2021, https://www.wipo.int/wipo_magazine_digital/en/2020/article_0002.html.

¹⁸ Anne Rose, Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights, WIPO Magazine, 2020. Accesat online în Noiembrie 2021, https://www.wipo.int/wipo_magazine_digital/en/2020/article_0002.html.

¹⁹ Gwyneth Iredale, Hyperledger Fabric Vs Ethereum: Head-To-Head Battle. Accesat online în Noiembrie 2021, <https://101blockchains.com/ethereum-vs-hyperledger-fabric/>.

Limbaj de programare	Solidity	NodeJS, Golang, Java
Tip aplicație	Gamă largă	Gamă largă

O soluție de gestionare a drepturilor de PI ar putea fi folosirea platformei blockchain **Hyperledger Fabric**, care este unul dintre proiectele populare ale companiei Hyperledger blockchain. Această platformă vine cu registre, contracte inteligente, protocoale care ajută toți utilizatorii să ia parte la procesul de tranzacție. În arhitectura Hyperledger Fabric, pentru a se obține acces la sistem, trebuie să se devină membru al rețelei²⁰.

În continuare sunt prezentate principalele considerente pentru care această platformă ar fi potrivită pentru gestionarea drepturilor de PI²¹:

- **Consensul** Hyperledger Fabric este de fapt un model flexibil. În plus, vine cu o gamă largă de algoritmi de consens, opțiuni conectabile, mai multe formate de registru.
- Altă caracteristică interesantă a arhitecturii Hyperledger Fabric este că permite crearea unor canale separate care pot oferi opțiuni de **tranzacție privată**.
- Platforma este **open-source**, ceea ce înseamnă că oricine poate folosi platforma în beneficiul companiei sale.
- Proiectul Hyperledger Fabric vine într-adevăr cu un set de **coduri de calitate**. În fiecare nouă adăugare, ei se asigură că au cea mai înaltă calitate de pe piață. Înainte de fiecare lansare, ei tind să-și respecte codurile cu atenție pentru probleme de securitate. Mai mult decât atât, ei fac și teste riguroase pentru codificarea lor.
- Arhitectura tehnologiei este cea care îi oferă un impuls masiv în **eficiență**. Mai mult decât atât, toate nodurile din cadrul sistemului vin cu atribuții diferite. Așadar, separarea proceselor de tranzacție de alte procese de comandă ajută ca acestea să se realizeze la timp.
- O caracteristică atractivă a proiectului Hyperledger Fabric este **designul modular**. Prin aceasta, ne referim la faptul că pot folosi mai multe funcții în sistem. Se poate schimba consensul Hyperledger Fabric, tipurile de registru, adăugarea altor funcționalități etc.

O altă soluție pentru managementul drepturilor de PI ar putea fi utilizarea platformei **Ethereum**, care este o platformă globală și open-source pentru toate aplicațiile descentralizate. Mecanismul de consens Ethereum utilizează o versiune actualizată a algoritmului PoW. În realitate, mecanismul de consens Ethereum este destul de robust și eficient. Cu toate acestea, problema este că necesită multe resurse și poate încetini²².

Majoritatea proceselor trec prin Ethereum Virtual Machine (EVM). Practic, ceea ce face este că execută anumite scripturi într-o rețea distribuită de dispozitive. Mai mult decât atât,

²⁰ Gwyneth Iredale, Hyperledger Fabric Vs Ethereum: Head-To-Head Battle. Accesat online în Noiembrie 2021, <https://101blockchains.com/ethereum-vs-hyperledger-fabric/>.

²¹ Gwyneth Iredale, Hyperledger Fabric Vs Ethereum: Head-To-Head Battle. Accesat online în Noiembrie 2021, <https://101blockchains.com/ethereum-vs-hyperledger-fabric/>.

²² Gwyneth Iredale, Hyperledger Fabric Vs Ethereum: Head-To-Head Battle. Accesat online în Noiembrie 2021, <https://101blockchains.com/ethereum-vs-hyperledger-fabric/>.

permite, de asemenea, executarea de contracte inteligente și stochează totul, de la organizații autonome descentralizate (în engleză, DAO – Decentralized Autonomous Organization) până la reglementările privind contractele inteligente. În realitate, pe arhitectura Ethereum se pot dezvolta aplicații descentralizate.

Principalele caracteristici ale platformei Ethereum sunt:

- **Imuabilitate:** este evident că nu se poate face nici o modificare în registru. Deci, orice terță parte nu va avea acces la el, chiar dacă este un domeniu public.
- **Dovada de corupție:** nimeni nu poate efectua activități de corupție în sistem fără ca cineva să-l observe. Dacă cineva încearcă chiar să modifice orice fel de documente, sistemul va primi alerte, iar toți utilizatorii vor primi, de asemenea, alerte despre asta.
- **Securitate:** Fiind o platformă publică deschisă, partea de securitate este vitală, totul fiind transparent. Și această transparență adaugă un nivel de securitate pentru fiecare utilizator. De asemenea, oferă o mulțime de tactici, cum ar fi diverse forme de criptografie și altele.
- **Fără timp de nefuncționare:** tot ce rulează în rețeaua Ethereum nu va avea timp de nefuncționare. Așadar, aplicațiile, contactele inteligente, tranzacțiile nu se vor confrunta cu probleme și vor fi întotdeauna disponibile oricui.

Constrângeri privind implementarea

Principalele constrângeri care ar trebui luate în considerare pentru implementarea unei soluții de gestionare a drepturilor de PI pe o platformă blockchain sunt următoarele²³:

- Lipsa unei legislații adecvate la nivel internațional.
- Proveniența imuabilă și perfectă oferită de registrele blockchain amenință confidențialitatea utilizatorilor.
- Natura descentralizată, rezistentă la cenzură a stocării blockchain înseamnă că conținutul dăunător sau ilegal, nu poate fi eliminat.
- Contractele inteligente și micro-plățile ar putea fi utilizate pentru a limita accesul celor care au capacitatea de a plăti pentru conținut, mai degrabă decât pentru a încuraja creația.
- Dacă informațiile despre o lucrare sunt invalide la punctul de intrare în blockchain, poate fi dificil de corectat.

Resurse tehnice pentru implementare

²³ COALA, How Blockchains can Support, Complement, or Supplement Intellectual Property. Accesat online în Noiembrie 2021, https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4307/529.

Resursele tehnice necesare implementării unei soluții de management al drepturilor de PI sunt, în principal, de două tipuri: hardware și software.

Resursele tehnice necesare:

- Resurse pentru proiectarea, dezvoltarea și testarea experimentală a soluției
 - Partea de server (hardware/software server și platforme de dezvoltare)
 - Consumatori
- Aplicații pentru înregistrare date în blockchain
- Aplicații pentru verificare a datelor
- Resurse pentru funcționarea propriu-zisă:
 - Noduri blockchain (servele)
 - Infrastructura de alimentare și interconectare a nodurilor
 - Mentenanță noduri
 - Mentenanță aplicații consumator

Resurse umane pentru implementare

Resursele umane necesare implementării soluției bazate pe tehnologia blockchain pentru gestionarea drepturilor de PI se pot împărți în două categorii: dezvoltatori de sistem și specialiști pentru mentenanță.

Dezvoltatorii de sistem trebuie să realizeze atât partea de server „back-end” (nodurile și interconectarea lor în blockchain), cât și aplicațiile „front-end” capabile să înregistreze/gestioneze drepturile de PI. Aceștia au nevoie de aptitudini²⁴ în:

- Programare
- Criptografie
- Structuri de date și stocare distribuită
- Arhitecturi software
- Aplicații web
- Contracte inteligente
- Interoperabilitate.

Pentru a putea fi acceptate și utilizate la scară largă, aplicațiile ar trebui să fie realizate cu interfețe simple și ușor de utilizat.

Specialiștii pentru mentenanța sistemului blockchain trebuie să se ocupe de trei aspecte principale:

²⁴ Toshendra Kumar Sharma. 5 Skill Sets a Blockchain Developer Must Have. <https://www.blockchain-council.org/blockchain/5-skill-sets-a-blockchain-developer-must-have/> si Robert Sheldon. 6 must-have blockchain developer skills, <https://whatistechtarget.com/feature/6-must-have-blockchain-developer-skills>.

- Păstrarea în funcțiune a hardware-ului și software-ului peste care rulează sistemul blockchain.
- Păstrarea în funcțiune și eventual extinderea/scalarea părții software caracteristice sistemului blockchain.
- Menținerea în funcțiune a aplicațiilor client.

Resurse financiare pentru implementare

Costurile asociate cu implementarea blockchain în managementul PI constă în dezvoltarea platformei blockchain, integrarea personalului pentru a afla modul de utilizare a noului sistem, costurile continue în operațiuni, costurile de întreținere a platformei și costurile suportate pentru monitorizarea operațiunilor (vezi tabelul 2)²⁵.

Tabelul 2: Resurse financiare pentru implementare

Costuri	Observații	Beneficii
Costuri de dezvoltare	Costurile inițiale de dezvoltare a platformei variază în funcție de tipul de platformei blockchain	• Registre de conținut securizate • Arhive de conținut descentralizate de încredere, care nu pot pierde informații și nu sunt vulnerabile la cenzură de către autorități de orice fel
Costuri de integrare a soluției	Costuri de instruire și documentare pentru a acorda accesul necesar utilizatorilor în rețea	
Costuri curente/continue	Costuri pentru taxa de licență a furnizorului de servicii blockchain, angajat cu normă întreagă pentru asistența tehnică a platformei blockchain și educația continuă	• Micro-plăți către creatori pentru fiecare utilizare a lucrărilor lor • Contracte inteligente automatizate pentru vânzări, licențiere și utilizări noi ale lucrărilor • Forme noi de colaborare și creație care permit oamenilor care nu se cunosc sau nu au încredere unul în altul să lucreze împreună
Costuri de mentenanță	Costurile întreținere depind de costul anual al mașinilor virtuale, care este o emulare a unui sistem informatic utilizat de nodurile complete pentru a verifica tranzacțiile blockchain	
Costuri de monitorizare	Costurile de monitorizare ale unui sistem bazat pe blockchain constă în revizuirea tranzacțiilor și evaluarea rețelei	

²⁵ Abdul Haseeb Sahaak, Cost-Benefit Analysis of Blockchain-based Global Payments. Master's thesis, Programme International Business Administration, Tallinn 2021.

Resurse logistice pentru implementare

Resursele logistice ale sistemului propus rezultă atât din caracteristicile sistemelor blockchain, cât și din scopului acestui sistem, și implică actori diferiți – instituții de specialitate (naționale și internaționale) responsabile cu protecția drepturilor de PI, deținătorii drepturilor de autor și organisme de reglementare.

Principalele resurse logistice necesare adoptării unei astfel de soluții ar putea fi următoarele:

- Sisteme de calcul adecvate.
- Echipamente software și hardware.
- Soluții tehnice pentru coordonarea administrativă între părțile implicate.
- Materiale educaționale.

Riscuri și planuri de contingență

Riscurile adoptării unei soluții bazate pe tehnologia blockchain pentru gestionarea drepturilor de PI pot fi clasificate în următoarele categorii:

- **Riscuri de finanțare**
 - Riscul de oprire/diminuare a fondurilor pentru implementarea de sus în jos a sistemului propus la nivel național, în oricare fază a sa.
- **Riscuri legislative**
 - Lipsa unei autorități legale de reglementare a utilizării tehnologiei blockchain;
 - Lipsă de coordonare între autorități de reglementare naționale / internaționale.
- **Riscuri ale costurilor de întreținere**
 - Încetarea finanțării susținute pe termen lung.
- **Riscuri operaționale**
 - Probleme de securitate.
 - Probleme de disponibilitate (hard/soft/specialiști).
 - Probleme de scalabilitate.
- **Riscuri de planificare**
 - Depășirea fondurilor sau a termenelor limită.
 - Volatilitatea resursei materiale și a celei umane.
- **Riscuri de schimbare a opțiunilor politice (riscuri decizionale)**
 - Încetarea finanțării susținute pe termen lung.

- Schimbarea climatului politic favorabil pentru implementare și extindere.
- **Riscuri legate de procedurile de achiziții publice**
 - Nerespectarea regulamentelor.
 - Furnizori care câștigă licitațiile, dar se nu respectă cerințele din fișele tehnice hardware/software sau termenele de livrarea și punere în funcțiune.
 - Firme care se retrag sau ajung în imposibilitatea de respectare a contractului.
- **Riscuri reputaționale (influența opiniei publice)**
 - Neglijarea importanței diseminării soluțiilor noi, a pregătirii corecte a utilizatorilor.
- **Riscuri ale schimbărilor tehnologice**
 - Acesta este un risc aparte în cazul de față, deoarece toate înregistrările începând cu blocul geneză (conținând înregistrarea inițială) din blockchain trebuie să fie inteligibile și autentificabile, pe întreaga perioadă de existență a blockchain-ului, care înseamnă decenii sau mai mult. Soluția posibilă constă în dezvoltarea de specificații detaliate ale stocării datelor și scrierii/citirii lor, a arhitecturii sistemului, a interfeței de acces, independente de tehnologia de implementare. O soluție adițională este înnoirea periodică a aplicațiilor server și client, a aplicațiilor, a materialului de instruire, cu tehnologii noi și testate, dar cu păstrarea datelor din sistem și a sistemului în funcțiune.
- **Riscuri ale volumului de activitate estimat**
 - Subestimarea necesarului de creștere a sistemului suport. Se impune dezvoltarea sistemului și a aplicațiilor suport în așa fel, încât să fie asigurată scalabilitatea și extensibilitatea sistemului.

Interacțiunea cu alte sisteme tehnice

Soluția propusă ar putea interacționa cu următoarele platforme/baze de date din Rețeaua Uniunii Europene pentru PI:

- **TMview** – Mărcile tuturor oficiilor oficiale de mărci care participă la nivel național și internațional, precum și la nivelul UE.
- **Designview** – Punct de acces centralizat la informațiile despre desenele sau modelele industriale înregistrate, deținute de oficiile naționale participante.
- **TMclass** – Portalul unic de clasificare cu acces la baza de date armonizată aplicată în UE și la baze de date din toată lumea.
- **Similarity** – Evaluarea similitudinii dintre produse și servicii de către oficiile de proprietate intelectuală din UE.
- **DesignClass** – Comparați bazele de date de clasificare a desenelor și modelelor industriale ale oficiilor participante.

Alte sisteme internaționale cu care platforma propusă ar putea interacționa pot fi:

- **Global IP Platform** – platforma globală a Organizației Mondiale a Proprietății Intelectuale (în engleză, WIPO).
- **WIPO|PCT** – Sistemul internațional de brevete (în engleză, The International Patent System – PCT).
- Portalul bazei de date pentru mărci comerciale WIPO.

Diagrama pentru implementare

Principalele activități de implementare a soluției propuse, pentru realizarea unui sistem blockchain de gestiune a drepturilor de PI sunt prezentate în *tabelul 3*.

Tabelul 3: Diagrama Gantt a activităților de implementare

Activitate	Perioadă, ani				
	1	2	3	4	5
Planificare, proiectare sistem, interfață utilizator, cod sursă					
Dezvoltare și testare					
Formare și instruire personal					
Implementare pe platforme de tip "cloud", livrare, aplicații					
Migrare soluție existentă pe platforma blockchain					
Întreținere, actualizare, testare					
Actualizare, optimizare funcții noi, contracte inteligente					

Metodologia de management a proiectului și modelul de dezvoltare

Pentru dezvoltarea soluției propuse se va folosi o Metodologie Agilă de management a proiectului, deoarece această metodologie insistă pe feedback din partea utilizatorilor ceea ce va alimenta inovația.

Utilizarea tehnologiei blockchain pentru un sistem de management al PI asigură integritatea și securitatea datelor privind drepturile. Acestea includ drepturile de autor și drepturile conexe, cum ar fi drepturile morale, precum și mărcile comerciale, modelele și brevetele. În cazul în care drepturile sunt înregistrate, o soluție ar putea fi un blockchain hibrid public/privat, care utilizează datele de la biroul de PI relevant ca sursă unică²⁶.

²⁶ Rosie Burbidge, Using blockchain technology to manage IP rights, Oct. 2018. Accesat online în Noiembrie 2021, <https://gunnercooke.com/using-blockchain-technology-to-manage-ip-rights/>.

Blockchain-ul poate fi utilizat ca parte a unui model de licențiere deschis mai larg, care ar putea permite terților să identifice rapid oportunitățile de licență și, eventual, să negocieze licențe simple ca „contracte inteligente”, în care acțiunile contractuale sunt determinate digital și efectuate automat atunci când un anumit eveniment sau pragul este atins. Pentru drepturile neînregistrate, cum ar fi drepturi de autor și modele neînregistrate, blockchain-ul poate fi deosebit de util pentru companii pentru a urmări crearea de noi lucrări cu drepturi de autor sau modele neînregistrate²⁷.

Principalul beneficiu al blockchain-ului este ușurința cu care informațiile pot fi partajate și urmărite. Acest lucru poate crește încrederea în sistem și se asigură că toți artiștii au o înregistrare clară și în timp real a modului în care au fost calculate contribuțiile lor la redevențe.

De asemenea, este ușor de urmărit drepturile auxiliare, cum ar fi drepturile morale, și să se identifice unde s-au acordat derogări de drepturi morale și, în cazul în care nu au fost furnizate, natura și amploarea permisiunilor care au fost acordate. Pe termen lung, blockchain-ul ar trebui să fie de neprețuit pentru arhive, deoarece ar trebui să reducă probabilitatea ca lucrările să devină orfane²⁸.

Precondiții și factori critici pentru succes

Principalele **precondiții** care trebuie avute în vedere pentru implementarea cu succes a proiectului sunt:

- Reglementarea tehnologiei blockchain.
- Colaborarea autorităților de reglementare și factorii de decizie pentru a contribui la modelarea implementării acestei tehnologii.
- Definirea unui set de standarde agreeat și susținut la nivel internațional.

Dintre **factorii** cu cel mai mare impact în realizarea cu succes a proiectului îi putem menționa pe următorii:

- Respectarea bugetului planificat și a criteriilor de timp și performanță.
- Obiectivele și direcțiile clar definite.
- Competența membrilor echipei de proiect.
- Rolul și responsabilităților clar definite.
- Comunicarea și consultarea cu părțile implicate.

²⁷ Rosie Burbidge, Using blockchain technology to manage IP rights, Oct. 2018. Accesat online în Noiembrie 2021, <https://gunnercooke.com/using-blockchain-technology-to-manage-ip-rights/>.

²⁸ Rosie Burbidge, Using blockchain technology to manage IP rights, Oct. 2018. Accesat online în Noiembrie 2021, <https://gunnercooke.com/using-blockchain-technology-to-manage-ip-rights/>.

Indicatori pentru monitorizare și evaluare

Pentru definirea sistemelor de monitorizare și evaluare se propun următorii indicatori, definiți pe următoarele niveluri:

Indicatori de ieșire:

- Sistem(e) de gestionare a drepturilor de PI funcționând pe o platforma blockchain.
- Documentație referitoare la dezvoltarea, implementare, întreținerea și monitorizarea unei platforme blockchain pentru gestionarea drepturilor de PI.

Indicatori de rezultat:

- Proceduri simplificate de înregistrare a unui drept de PI.
- Posibilitatea de a urmări crearea de noi lucrări cu drepturi de autor sau modele neînregistrate.
- Posibilitatea creatorilor și deținătorilor de drepturi de a-și revendica drepturile și a-și monetiza lucrările proprii.
- O mai bună gestionare a activelor netangibile care se dovedesc unice.
- Reducerea costurilor pentru protejarea drepturilor de PI.

Indicatori de impact:

- Eliminarea sau diminuarea opoziției furnizorilor de conținut în a adopta noi modele de licențiere, în cazul modelele de afaceri inovative.
- Reducerea pirateriei cauzate de zona geografică în care se află potențialii utilizatori ai unor conținuturi protejate prin drepturi de autor.
- Relații îmbunătățite ale partenerilor pe un registru transparent.

În viitor, ciclul de viață al drepturilor de PI va asigura că activele sunt atribuibile la creare, protejate de fraudă și funcționează într-o rețea care promovează eficiența operațională și inovarea produselor²⁹.

Referințe bibliografice

1. EURAXESS ROMANIA, Working in Europe | Intellectual Property Rights | Romania. Accesat online în Noiembrie 2021, <https://www.euraxess.gov.ro/ro/romania/informatii-si-asistenta/proprietate-intelectuala>.

²⁹ Ernst & Young Global Ltd. (2019), How blockchain can impact the intellectual property life cycle. Accesat în Noiembrie 2021, https://www.ey.com/en_gl/consulting/how-blockchain-can-impact-the-intellectual-property-life-cycle.

2. Anne Rose, *Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights*, WIPO Magazine, 2020. Accesat online în Noiembrie 2021, https://www.wipo.int/wipo_magazine_digital/en/2020/article_0002.html.
3. Dr. Birgit Clark, Baker McKenzie and Ruth Burstall, Johnson & Johnson *Crypto-Pie in the Sky? How Blockchain Technology is Impacting Intellectual Property Law*, Stanford Journal of Blockchain Law & Policy, June 2019.
4. Gönenç Gürkaynak, İlay Yılmaz, Burak Yeşilaltay, Berk Bengi, *Intellectual property law and practice in the blockchain realm*, Computer Law & Security Review, Volume 34, Issue 4, 2018, Pages 847-862, ISSN 0267-3649, doi.org/10.1016/j.clsr.2018.05.027.
5. Gwyneth Iredale, *6 Key Blockchain Features You Need To Know Now*, Nov. 2020. Accesat online în Noiembrie 2021, <https://101blockchains.com/introduction-to-blockchain-features/>.
6. Riviere, Jean. *Blockchain technology and IP – investigating benefits and acceptance in governments and legislations* (2018).
7. Gwyneth Iredale, *Hyperledger Fabric Vs Ethereum: Head-To-Head Battle*. Accesat online în Noiembrie 2021, <https://101blockchains.com/ethereum-vs-hyperledger-fabric/>.
8. COALA, *How Blockchains can Support, Complement, or Supplement Intellectual Property*. Accesat online în Noiembrie 2021, https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4307/529.
9. Hauck R. (2021) *Blockchain, smart contracts and intellectual property. Using distributed ledger technology to protect, license and enforce intellectual property rights. Legal Issues in the Digital Age*, no 1, pp. 17–41.
10. Toshendra Kumar Sharma. *5 Skill Sets a Blockchain Developer Must Have*. <https://www.blockchain-council.org/blockchain/5-skill-sets-a-blockchain-developer-must-have/>.
11. Robert Sheldon. *6 must-have blockchain developer skills*, <https://whatis.techtarget.com/feature/6-must-have-blockchain-developer-skills>.
12. Abdul Haseeb Sahaak, *Cost-Benefit Analysis of Blockchain-based Global Payments*. Master's thesis, Programme International Business Administration, Tallinn 2021.
13. Rosie Burbidge, *Using blockchain technology to manage IP rights*, Oct. 2018. Accesat online în Noiembrie 2021, <https://gunnercooke.com/using-blockchain-technology-to-manage-ip-rights/>.
14. Ernst & Young Global Ltd. (2019), *How blockchain can impact the intellectual property life cycle*. Accesat în Noiembrie 2021, https://www.ey.com/en_gl/consulting/how-blockchain-can-impact-the-intellectual-property-life-cycle.



Proiect:

Proiect selectat în cadrul Programului Operațional Capacitate Administrativă cofinanțat de Uniunea Europeană, din Fondul Social European

Axa Prioritară 1: Administrație publică și sistem judiciar eficiente

Obiectivul specific 1.1: Dezvoltarea și introducerea de sisteme și standarde comune în administrația publică ce optimizează procesele decizionale orientate către cetățeni și mediul de afaceri, în concordanță cu SCAP.

Titlul proiectului: „ Cadru strategic pentru adoptarea și utilizarea de tehnologii inovative în administrația publică 2021-2027 – soluții pentru eficientizarea activității”

COD: SIPOCA 704

Beneficiar: AUTORITATEA PENTRU DIGITALIZAREA ROMÂNIEI

Partener: UNIVERSITATEA TEHNICĂ DIN CLUJ - NAPOCA

Fundamentarea cazului de utilizare și studiu de evaluare ex-ante pentru Managementul votului electronic

Cuprins

Acronime și abrevieri	3
Scopul intervenției	3
Părțile interesate.....	6
Beneficiile estimate.....	7
Factori critici în asociere cu cazurile de utilizare	9
Provocări tehnice în implementarea intervenției.....	11
Procese curente care ar putea fi afectate de dezvoltarea proiectului	12
Obiectivele funcționale.....	12
Obiectivele de performanță.....	12
Elementele de noutate	14
Criteriile de selecție	15
Descrierea în detaliu a cazului de referință	18
Opțiuni de îmbunătățire	20
Analiza comparativă.....	20
Constrângeri privind implementarea.....	21
Resurse tehnice pentru implementare	21
Resurse umane pentru implementare.....	21
Resurse financiare pentru implementare	22
Resurse logistice pentru implementare.....	23
Riscuri și planuri de contingență.....	23
Interacțiunea cu alte sisteme tehnice	25
Diagrama pentru implementare	26
Metodologia de management a proiectului și modelul de dezvoltare	27
Precondiții și factori critici pentru succes	28
Indicatori pentru monitorizare și evaluare	28
Referințe bibliografice	29

Acronime și abrevieri

Abreviere sau acronim	Expresia completă	Explicație
DLT	Distributed Ledger Technology	Tehnologie de tip registru distribuit.
DIDs	Decentralized identifiers	Tip nou de identificator care permite o identitate digitală descentralizată și verificabilă.
EBSI	European Blockchain Services Infrastructure	Infrastructura europeană pentru servicii blockchain, promovată de Comisia Europeană.
IdM	Identity Management	Cadru de politici și tehnologii pentru a se asigura că utilizatorii potriviți (într-o întreprindere) au acces adecvat la resursele tehnologice.
WOT	web-of-trust	Este un concept utilizat în PGP, GnuPG și alte sisteme compatibile cu OpenPGP pentru a stabili autenticitatea legăturii dintre o cheie publică și proprietarul acesteia.
EVM	Ethereum Virtual Machine	
PGP	Pretty Good Privacy	Program de criptare care oferă confidențialitate criptografică și autentificare pentru comunicarea datelor.
POW	Proof-of-Work	O formă de dovadă criptografică în care o parte demonstrează altora munca pentru a fi remunerat.
PBFT	Practical Byzantine Fault Tolerance	Un sistem care are un nod primar și noduri secundare. Aceste noduri lucrează împreună pentru a ajunge la un consens, făcând din acest sistem una dintre soluțiile la Problema Generalilor Bizantini.

Scopul intervenției

Definirea problemei

Conform raportului intitulat „Society at a Glance 2019: OECD Social Indicators”¹ al *Organizației pentru Cooperare și Dezvoltare Economică* (OCDE), interesul cetățenilor în politica națională reprezintă un factor important al coeziunii sociale. În același timp, oamenii politici și reprezentanții instituțiilor statului trebuie să facă eforturi pentru a-i convinge pe cetățeni să fie interesați și implicați în viața politică.

¹ <https://www.oecd.org/social/society-at-a-glance-19991290.htm>

Prezența la vot în cadrul alegerilor naționale din România este, cu mici excepții, foarte mică, mai ales în rândul persoanelor tinere, cu vârste între 18 și 34 de ani – o categorie de populație foarte activă care ar trebui să aibă un cuvânt puternic de spus în viața publică. Mai exact, conform datelor *Biroului Electoral Central*², la ultimele cinci rânduri de alegeri (parlamentare 2016, europarlamentare 2019, prezidențiale 2019, locale 2020 și parlamentare 2020), media de prezență a tinerilor a fost de doar 35,61%, vârful fiind reprezentat de alegerile europarlamentare din 2019, când au votat 43,21% din tinerii de pe listele electorale permanente.

Se pot identifica motive multiple³ pentru care mulți tineri din România nu participă la votul electoral, inclusiv lipsa generală de interes sau încredere în sistemul politic sau necunoașterea condițiilor necesare pentru exercitarea dreptului de vot. În multe cazuri, însă, apar și probleme logistice, cauzate de faptul că persoanele care se mută în alt oraș nu pot obține întotdeauna în timp util o viză de flotant sau un act de identitate care să le permită să voteze în județul sau orașul respectiv, lucru care îi elimină automat pe aceștia din procesul de vot, puțini fiind dispuși să călătorească până în localitatea de domiciliu doar pentru a vota.

Mai mult, un număr semnificativ de cetățeni români locuiesc în străinătate, având în continuare dreptul de a vota în alegerile naționale, însă mulți dintre ei, chiar dacă își doresc să participe la proces, întâmpină dificultăți în a-și exprima votul din cauza limitelor logistice precum distanța mare față de cea mai apropiată secție de vot din statul în care fie locuiesc permanent, fie lucrează sau studiază în perioada respectivă.

În acest context, introducerea unui sistem de vot electronic ar putea avea un efect semnificativ asupra prezenței la vot, mai ales în rândul tinerilor, dar și în rândul altor grupe de vârstă, înlăturând problemele de ordin logistic.

Tehnologia blockchain se numără printre soluțiile tehnice cele mai promițătoare care să stea la baza implementării unui sistem de vot electronic sigur, transparent și integru, datorită proprietăților inerente ale tehnologiei (imuabilitate, descentralizare, securitate crescută, transparență, anonimitate, non-repudiare etc.).

În 2017, Consiliul Europei⁴ a elaborat o serie de recomandări pentru statele membre ale Uniunii Europene în privința implementării sistemelor de vot electronic, inclusiv a aparatelor electronice pentru vot în cadrul secțiilor, scannerelor de buletine de vot, stilourilor digitale sau a sistemelor de vot de la distanță prin internet.

Toate sistemele digitale menționate mai sus pot fi susținute și securizate cu ajutorul tehnologiei blockchain, însă doar votul electronic de la distanță poate rezolva problemele logistice care îi împiedică pe mulți cetățeni să-și exprime votul în alegerile naționale, deoarece celelalte metode ar implica în continuare deplasarea la o secție de vot.

² <https://www.edupedu.ro/analiza-doar-25-dintre-tinerii-de-pe-listele-electorale-au-votat-la-parlamentare-cea-mai-scazuta-prezenta-de-la-alegerile-din-ultimii-4-ani/>

³ <https://republica.ro/tinerii-de-18-24-de-ani-o-dezamagire-in-2016-dar-o-speranta-in-2020>

⁴ <https://rm.coe.int/168071bc84>

Obiectivele generale

Obiectivele generale ale intervenției sunt:

- Creșterea ratei de participare în procesul de vot, în special a persoanelor tinere și active economic;
- Reducerea riscului de fraudă electorală prin posibilitatea ca fiecare votant să-și poată urmări votul și să poată confirma că acesta a fost contorizat în mod corespunzător în numărătoarea finală;
- Creșterea încrederii în procesul de vot și în autoritățile publice.

Obiectivele specifice

Obiectivele specifice ale acestei intervenții sunt:

- Dezvoltarea unui sistem de vot electronic bazat pe tehnologia blockchain care să poată fi accesat de oriunde, de pe dispozitive web/mobile;
- Conectarea sistemului de vot la sistemele naționale de identificare/autentificare digitală (identitate digitală);
- Pilotarea sistemului de vot electronic bazat pe blockchain în cadrul unui scrutin de vot național viitor, cu un număr limitat de participanți de pe teritoriul național și din diaspora.
 - Ținând cont de complexitatea sistemului și istoricul dezvoltării altor sisteme tehnologice naționale (proces relativ anevoios, birocratic și de lungă durată), un termen realist pentru pilotarea sistemului de vot electronic ar fi 2028, an în care vor avea loc alegeri europarlamentare, locale și parlamentare în România.
 - Având în vedere faptul că instituțiile europene s-au arătat interesate de tehnologia blockchain, inclusiv de aplicarea ei în cadrul proceselor de vot electronic, dar și existența unor standarde pentru un astfel de sistem publicate de către Consiliul Europei în 2017⁵, considerăm că alegerile europarlamentare din 2028 ar fi cele mai potrivite pentru pilotarea acestui sistem.
- Analizarea și auditarea rezultatelor pilotului și elaborarea unor concluzii referitoare la eficiența, fezabilitatea și potențialul de extindere a sistemului utilizat în cadrul proiectului-pilot la nivel general în cadrul unor alegeri naționale viitoare (post-2030).

Obiectivele operaționale

⁵ https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f

Obiectivele operaționale ale intervenției sunt:

- Dezvoltarea infrastructurii tehnologice necesare pentru implementarea proiectului pilot în cadrul alegerilor europarlamentare din 2028;
- Dezvoltarea unor programe de informare și educare a publicului larg în legătură cu sistemul de vot electronic, beneficiile sale și modul de utilizare;
- Dezvoltarea grupurilor de lucru și echipelor de management în cadrul instituțiilor interesate pentru organizarea, implementarea și monitorizarea rezultatelor proiectului pilot;
- Dezvoltarea unei metodologii de evaluare a rezultatelor proiectului pilot în vederea luării unei decizii privind posibila extindere a sistemului în cadrul tururilor de alegeri naționale viitoare (post-2028).

Care sunt granițele de utilizare/aplicabilitate avute în vedere?

Acest document face referire la elaborarea unui proiect pilot pentru testarea cazului de utilizare a tehnologiei blockchain în domeniul votului electronic, în cadrul alegerilor europarlamentare din 2028.

Doar un număr limitat de cetățeni vor fi implicați ca votanți, însă proiectul pilot va implica toate instituțiile relevante care ar putea fi mai târziu implicate și în implementarea pe scară largă a unui astfel de sistem de vot electronic, tocmai pentru a planifica, observa și ulterior, dacă este cazul, optimiza modul de colaborare dintre aceste instituții pentru ca proiectul pe scară largă să poată avea cele mai bune rezultate.

Din punct de vedere tehnic, proiectul pilot va avea ca scop principal evaluarea fezabilității operaționale/financiare, a eficienței și a performanței tehnologiei blockchain într-un astfel de caz de utilizare.

Părțile interesate

Beneficiarii soluției dezvoltate vor fi:

- Autoritatea Electorală Permanentă (AEP).
- Ministerul Afacerilor Interne (MAI).
- Biroul Electoral Central (BEC).
- Serviciul de Telecomunicații Speciale (STS).
- Autoritatea pentru Digitalizarea României (ADR).
- Cetățenii români cu domiciliul în țară.
- Cetățenii români cu domiciliul în străinătate.

Utilizatorii soluției tehnice vor fi:

- Cetățeni români cu domiciliul în țară.
- Cetățeni români cu domiciliul în străinătate.
- Specialiștii desemnați de către instituțiile publice implicate în organizarea și monitorizarea procesului de vot (menționate mai sus).

Beneficiarii și utilizatorii soluției tehnice dezvoltate pentru implementarea proiectului pilot vor fi consultați permanent în procesul de luare a deciziilor cu privire la soluția propusă. Acest lucru se va realiza prin organizarea de sondaje pe bază de chestionare la care sunt invitate să participe toate părțile interesate. Promovarea chestionarelor se va face prin trimiterea de e-mail-uri către personalul instituțiilor publice vizate, către cetățenii care își declară interesul prin intermediul platformelor online ale instituțiilor care își asumă rolul de promotori ai proiectului, dar și prin rețelele sociale.

Beneficiile estimate

Natura oportunității de a dezvolta soluția tehnică/tehnologia

Decizia României de a dezvolta și testa o soluție de vot electronic online bazat pe tehnologia blockchain în următorii 5 ani ar putea poziționa țara ca pe un lider al inovației în regiune și în lume și un exemplu pentru alte țări care ar putea să adopte sisteme similare, în cazul în care acesta se dovedește a fi un succes.

Chiar și o concluzie nefavorabilă legată de adopția pe scară largă a unui astfel de sistem de vot ar putea totuși avea efecte pozitive asupra reputației României, deoarece informațiile și observațiile strânse în cadrul unui proiect-pilot de această natură ar putea fi revelatorii pentru lumea tehnologică și pentru experții în sisteme electorale la nivel internațional.

În acest moment, foarte mulți experți în tehnologie și în metode și sisteme de vot din toată lumea se opun ideii de vot online, inclusiv a votului online bazat pe tehnologia blockchain, argumentând că deși aceasta ar putea securiza anumite părți ale procesului de vot și ar putea garanta anumite caracteristici fundamentale ale votului, rămân nerezolvate o serie de probleme legate de securitatea cibernetică pe care sistemul le-ar putea suferi chiar înainte ca tehnologia blockchain măcar să își intre în rol⁶, iar acele probleme ar putea fi greu de detectat și foarte răspândite în interiorul sistemului în același timp.

Cu toate acestea, guvernele și organizațiile internaționale continuă să vadă votul electronic online ca fiind următoarea piatră de hotar pentru democrație, așa că putem fi siguri că vor mai apărea experimente, proiecte și propuneri în diverse state ale lumii în următorii ani.

⁶ <https://www.coindesk.com/tech/2020/11/16/new-mit-paper-roundly-rejects-blockchain-voting-as-solution-to-election-woes/>

În acest context, România ar putea să fie unul dintre statele care să desfășoare o cercetare practică și bine fundamentată a unui astfel de sistem utilizând cele mai avansate instrumente și soluții tehnice disponibile pe piață, aducând astfel o actualizare la literatura existentă și căutând soluții la fiecare dintre problemele – reale și importante – ridicate de experți de-a lungul timpului în legătură cu fezabilitatea votului electronic.

Mai mult, având în vedere că utilizarea tehnologiei blockchain nu reprezintă un scop în sine a dezvoltării unui sistem de vot electronic, ci este soluția tehnică acceptată ca având cel mai bun potențial de a rezolva anumite limitări ale sistemelor de vot online care nu au putut fi rezolvate până acum, elaborarea proiectului și parcurgerea pașilor de investigare a soluțiilor tehnice și a alternativelor ar putea rezulta în descoperirea unor abordări chiar mai potrivite decât tehnologia blockchain sau a unor soluții complementare care să permită rezolvarea problemelor tehnice pe care blockchain-ul nu le-ar putea rezolva de unul singur, dar care poate nu vor fi fost luate în considerare până la momentul respectiv. Așadar, acest demers ar putea genera un produs extrem de inovativ care ar putea fi dezvoltat mai departe și preluat și în alte contexte sau sisteme.

Beneficiile implementării unui sistem de vot electronic pe scară largă în urma unui proiect pilot desfășurat cu succes în 2028 ar include:

- **Creșterea prezenței la vot.** Exprimarea votului într-un sistem online crește posibilitatea ca un număr mai mare de cetățeni să voteze în alegerile naționale, inclusiv mai multe persoane tinere, care vor fi printre cele mai atrase de un astfel de sistem de vot, dar și mulți cetățeni care în ziua votului fie se află în călătorii în afara localității/județului de domiciliu, fie locuiesc în regim temporar sau permanent în străinătate și care în multe cazuri nu au acces ușor la o secție de vot din statul respectiv sau nu au timpul necesar pentru a vota prin corespondență, activitate ce implică o înregistrare prealabilă și un număr mai mare de acțiuni din partea votantului decât un vot exprimat online.
- **Reducerea riscului de fraudă/erori umane.** Un sistem electronic de vot conectat la registrele electorale va însemna o precizie mai mare în ceea ce privește înregistrarea votanților, evitarea înregistrărilor duble și, în cazul în care sistemul de vot este conectat la un sistem de identitate digitală, poate simplifica și procesul de eliminare a cetățenilor care rămân fără drept de vot din diverse motive (ex. renunță la cetățenie) sau decedează.
- **Creșterea încrederii în procesul de vot și în autoritățile publice.** Un sistem de vot electronic cu o bază tehnică sigură și riguros testată înainte de aplicarea pe scară largă va crește încrederea cetățenilor în autoritățile statului și va încuraja o mai bună colaborare între acești actori.
- **Rezultate mai rapide.** Deși procesul de vot electronic va fi doar o alternativă la procesul tradițional, așadar se va desfășura în paralel cu acesta, voturile exprimate prin sistemul electronic vor fi numărate și contorizate aproape instantaneu după finalizarea intervalului de votare. Având în vedere faptul că mulți cetățeni vor alege varianta

electronică, vor rămâne mai puține voturi de numărat manual în fiecare secție la finalul zilei, așadar rezultatele alegerilor vor putea fi publicate mai rapid.

Factori critici în asociere cu cazurile de utilizare

Factorii critici care ar putea influența sau afecta în mod negativ adoptarea unui sistem de vot electronic bazat pe tehnologia blockchain pot fi împărțiți în următoarele categorii:

Factori critici privind cerințele tehnice

- Posibilele vulnerabilități de securitate de-a lungul întregului proces de vot, inclusiv potențiale probleme precum compromiterea dispozitivelor prin care utilizatorii accesează sistemul;
- Asigurarea scalabilității la scară națională și a disponibilității continue a sistemului pentru a putea face față la un număr mare de tranzacții într-un interval scurt de timp;
- Capacitatea de procesare și stocare suficientă;
- Absența standardizării limbajelor de programare;
- Imaturitatea generală a tehnologiei blockchain și posibilitatea apariției unor inovații tehnice ulterior dezvoltării sistemului;
- Capacitatea tehnică necesară pentru asigurarea interoperabilității sistemului de vot electronic pe blockchain cu alte aplicații și servicii publice online existente sau care urmează a fi dezvoltate.

Factori critici de cost

- Costurile inițiale de dezvoltare și implementare ridicate;
- Costurile legate de mentenanța pe termen mediu și lung a sistemului;
- Costurile cauzate de consumul mare de energie electrică pentru susținerea sistemului;
- Costurile utilizării votului electronic în paralel cu cel tradițional pentru o perioadă nelimitată de timp, pentru a se ține cont de accesul scăzut la resurse informatice în România și la nivelul scăzut de competențe digitale în rândul populației;
- Planificarea alocării unor bugete semnificative pe termen lung pentru a asigura succesul și buna funcționare a sistemului din partea mai multor instituții implicate în proiect;
- Costurile asociate cu recrutarea și/sau instruirea personalului instituțiilor responsabile cu organizarea și supravegherea procesului de vot.

Factori critici privind calitatea

- Ușurința de utilizare a sistemului pentru utilizatorii nespecializați;
- Menținerea încrederii utilizatorilor în sistem;
- Îndeplinirea criteriilor de calitate indicate de Consiliul European⁷ pentru sistemele de vot electronic.

Factori critici privind ușurința execuției

- Existența unui număr suficient de specialiști în dezvoltarea de infrastructuri de date complexe și cu cerințe crescute de securitate și integritate și de interfețe de utilizator care să răspundă tuturor cerințelor funcționale;
- Existența unui număr suficient de persoane din instituțiile implicate în proiect care să aibă o înțelegere suficient de bună a modului de funcționare a sistemului pentru a-l putea utiliza cu succes.

Factori critici sub aspect economic (efecte colaterale negative, costuri de oportunitate)

- Asigurarea finanțării pentru dezvoltarea sistemului tehnic (hardware/software);
- Asigurarea finanțării pentru mentenanța pe termen lung a sistemului tehnic (hardware/software);
- Asigurarea finanțării pentru instruirea personalului specializat din instituțiile interesate;
- Asigurarea finanțării pentru promovarea inițiativei și educarea publicului larg în legătură cu aceasta pentru a ajunge la un număr suficient de mare de utilizatori care să facă fezabilă funcționarea sistemului.

Factori critici sub aspect legal

- Lipsa unor reglementări și cadre legale adecvate pentru acomodarea dezvoltării, testării și implementării (atât în regim de proiect pilot cât și la scară largă) a sistemului de vot electronic;
- Asumarea tuturor implicațiilor introducerii acestui sistem, inclusiv a riscurilor și posibilității unui eșec;
- Probleme legate de respectarea reglementărilor privind confidențialitatea și protecția datelor personale ale utilizatorilor (ex. GDPR).

⁷ <https://www.roaep.ro/legislatie/wp-content/uploads/2017/08/Traducere-Recomandare.pdf>

Provocări tehnice în implementarea intervenției

- **Limitări de performanță & scalabilitate.** Una dintre problemele care apar cel mai des în cadrul sistemelor tehnice care folosesc tehnologia blockchain este performanța și viteza de procesare a operațiunilor (tranzacțiilor). Aceste caracteristici sunt strâns legate de tipul de blockchain ales și de mecanismele de consens ale acestuia, care pot face diferența în ceea ce privește viteza de procesare. În cazul unui sistem național de vot, sistemul ar trebui construit în așa fel încât să poată susține un număr foarte mare de tranzacții (voturi) care ar avea loc într-un interval scurt. Înregistrarea, validarea și confirmarea unui vot ar trebui să se poată finaliza în cel mult 10 secunde de la apăsarea butonului de trimitere, pentru a minimiza riscul ca votantul să părăsească sistemul înainte ca votul său să fie înregistrat. Prin urmare, proiectul pilot ar trebui să implementeze o arhitectură tehnică scalabilă care să poată fi extinsă la o scară largă în viitor fără să fie afectată performanța și viteza de procesare.
- **Securitate.** Un sistem de vot electronic va trebui să fie securizat corespunzător împotriva tuturor tipurilor de atacuri cibernetice sau încercări de manipulări de date semnalate de specialiști în trecut și descoperite pe parcursul elaborării proiectului. Deși tehnologia blockchain va contribui în mod semnificativ la securitatea sistemului, ea nu va putea răspunde în mod adecvat la toate riscurile de securitate la care un astfel de sistem ar fi expus, deoarece această tehnologie nu poate proteja toate informațiile care circulă pe internet și nu poate face ca serverele și infrastructura să fie complet rezistente la amenințări avansate persistente⁸. De aceea, securitatea sistemului se va număra printre cele mai complicate aspecte ale intervenției și va necesita contribuții și implicare din partea unui număr cât mai mare de specialiști cu experiență cât mai vastă.
- **Asigurarea secretului votului.** Unul dintre principiile fundamentale ale procesului electoral este respectarea secretului votului și imposibilitatea ca opțiunea de vot a alegătorului să poată fi depistată sau asociată cu identitatea acestuia după ce votul este transmis.
- **Consumul de energie.** Tehnologia blockchain incorporează procese care utilizează cantități mari de energie (protocoale, mecanisme de consens, comunicare peer-to-peer, criptare asimetrică, etc). Tipul de blockchain care va fi ales pentru acest proiect va trebui să fie eficient din punct de vedere energetic, fără a face însă compromisuri în ceea ce privește alte caracteristici tehnice care fac tehnologia să fie valoroasă în acest caz de utilizare.
- Alocarea și asumarea de roluri tehnice a tuturor actorilor instituționali implicați în proiect.
- Integrarea cu alte sisteme naționale (eg. identitatea digitală).

⁸ https://europeandigital.org/files/19/Internet_Voting_Challenges_and_Solutions_ROM.pdf

Procese curente care ar putea fi afectate de dezvoltarea proiectului

Dezvoltarea și implementarea unui proiect pilot de vot electronic bazat pe tehnologia blockchain în cadrul alegerilor parlamentare din 2028 nu va afecta alte procese la nivelul administrației, deoarece proiectul se va derula în paralel cu sistemul obișnuit de alegeri. Cetățenii care participă ca votanți în acest proiect nu vor mai putea vota în mod tradițional, însă voturile lor exprimate prin intermediul sistemului electronic vor fi înregistrate și considerate valide.

Obiectivele funcționale

Funcționalități dorite a fi regăsite în cadrul soluției tehnice/tehnologiei

- *Auditabilitate* – Procesele de audit ar trebui să fie independente de infrastructura tehnică și interfețele software și să fie bazat pe dovezi matematice incontestabile.
- *Anonimitate* – Pentru a menține identitatea votantului secretă, procesul de decriptare ar trebui să implementeze mecanisme criptografice care să prevină corelarea informației decriptate cu cea care rămâne criptată, mai exact să prevină corelarea identității votantului cu opțiunile sale de vot.
- *Verificabilitate publică și individuală* – Verificabilitatea înseamnă existența unor procese pentru auditarea alegerilor pentru a garanta corectitudinea acestora. Aceasta ar trebui să poată fi făcută atât de către instituțiile guvernamentale relevante și auditori independenți, cât și de către fiecare votant în parte, care să-și poată verifica votul și faptul că a fost înregistrat corect.
- *Disponibilitate* – sistemul de vot ar trebui să fie disponibil și funcțional pe toată durata scrutinului de vot, fără niciun fel de întrerupere.
- *Recuperare* – în cazul unor pierderi de date sau întreruperi în transmiterea acestora, sistemul de vot electronic ar trebui să aibă capacitatea de a recupera datele într-un timp cât mai scurt și fără a risca compromiterea acestora.
- *Accesibilitate* – Sistemul de vot electronic ar trebui proiectat în așa fel încât să fie cât mai intuitiv și ușor de înțeles și folosit pentru toți potențialii utilizatori, de la personalul instituțiilor publice cu roluri active și până la toate categoriile de votanți care ar putea să adopte sistemul.

Obiectivele de performanță

Caracteristicile de performanță tehnică ale soluției

- **Scalabilitate.** Se vor căuta soluții tehnice de ultimă oră pentru asigurarea scalabilității infrastructurii blockchain. Unul dintre modurile prin care un sistem blockchain poate fi scalat ar fi prin paralelizarea datelor, cunoscută și ca mecanism de *sharding*. Sharding -

Într-o rețea tradițională blockchain, tranzacțiile și blocurile sunt validate de toate noduri participante. O abordare a scalării ar fi fragmentarea blockchain-ului, care este numit sharding. Fragmentarea este o tehnică care este utilizată pe scară largă în bazele de date. Date sunt împărțite orizontal în bucăți, fiecare numită un shard (ciob), pentru a oferi un nivel ridicat de performanță. Acesta este însă doar un exemplu de îmbunătățire a scalabilității unei rețele de blockchain; este necesară o investigație detaliată pentru identificarea celei mai bune, mai sigure și mai eficiente abordări pentru cazul votului electronic.

- **Securitate.** Sistemul tehnic va trebui să parcurgă un proces complex de dezvoltare și evaluare a măsurilor de securitate de la toate nivelurile și punctele de acces, care să includă evaluarea și certificarea sistemului, elaborarea unei strategii de securitate cibernetică pe termen mediu și lung, teste de sistem concursuri de identificare a problemelor și erorilor, instruire a personalului cu privire la factorii de securitate.
- **Alegerea tipului de blockchain** utilizat pentru a garanta un echilibru între securitate, performanță și scalabilitate viitoare. În acest sens, ar trebui să se țină cont de factori precum:
 - Mecanismul de consens - Tehnica sau mecanismul prin care o tranzacție este propagată, validată și finalizată într-o rețea blockchain este denumită protocol sau algoritm consens. Și acest mecanism de consens este, de asemenea, responsabil pentru realizarea unui echilibru fin între gradul de descentralizare, scalabilitate și securitate pe care îl deține o rețea blockchain. Prin urmare, alegerea mecanismului de consens este direct legată de modul în care funcționează rețeaua blockchain.
 - Latența rețelei - Într-o arhitectură distribuită, acesta este cel mai important factor care afectează performanța generală a rețelei. Atunci când o tranzacție urmează să fie validată, aceasta trebuie difuzată către toate nodurile și răspunsul acestora trebuie colectat pentru consens majoritar. Așadar, a avea o lățime de bandă dedicată rețelei ajută la minimizarea întârzierilor rețelei și la îmbunătățirea capacității generale.
 - Infrastructura nodurilor - Nodurile de blockchain cuprind un motor de execuție și o bază de date care este găzduită local sau în cloud. În absența resurselor de infrastructură dedicate (adică CPU, memorie, hard disk), performanța nodului este cel mai probabil să fie afectată. Astfel, este imperativ ca dimensionarea infrastructurii și alocarea adecvată IOPS (operațiuni de intrare pe secundă) să fie asigurate.
 - Numărul de noduri - Pe măsură ce numărul de noduri crește, cu atât crește și timpul necesar propagării unei tranzacții și obținerea consensului și asta degradează performanța generală. Ar trebui introduse mecanisme de reducere a cheltuielilor de comunicare și de a permite nodurilor să se bazeze pe istoricul validării unui nod lider și / sau alte noduri.

- Dimensiunea tranzacției - Întrucât tranzacțiile sunt transmise prin rețea către toate nodurile, sarcinile utile mai mari necesită mai mult timp pentru replicare între noduri. Deci, una dintre cele mai bune practici este stocarea încărcăturilor utile mari și a documentelor într-un spațiu de stocare offchain și înregistrarea referințelor acestora pe blockchain.
- Capacitatea de stocare pe noduri și de adăugare de noi noduri în rețea - De obicei, rețelele blockchain acceptă depozitele de date pereche cheie-valoare pentru a menține tranzacția și starea registrului integrat. Există o cantitate semnificativă de operațiuni citire-scriere, iar eficiența bazei de date subiacente este un factor cheie în influențarea performanței întregii rețele. Fiecare nod participant la rețeaua blockchain, în formula inițială, trebuie să fie o replică integrală a celorlalte noduri, și să conțină atât registrul imutabil de date cât și datele stocate în baza de date în vederea asigurării disponibilității și reconstrucției informației. Ulterior, se poate testa și varianta în care unele dintre nodurile din rețea să fie de dimensiuni mai mici și să conțină doar informații parțiale relevante pentru nodul respectiv (în funcție de modul de distribuție a rețelei – ex. pe criterii geografice sau demografice). Fiecare nod trebuie însă să conțină/integreze cel puțin următoarele componente informatice, chiar dacă nu sunt replici complete ale nodurilor full: registrul distribuit, baza de date, interfața API și componentele de securitate.
- Coada de tranzacții - O rețea blockchain cuprinde mai multe noduri și oferă în mod colectiv o disponibilitate ridicată, dar capacitatea de gestionare a tranzacțiilor fiecărui nod individual determină câte tranzacții vor fi acceptate din aplicațiile client pentru procesare ulterioară. Și acest lucru are un efect direct asupra randamentului general al rețelei.

Elementele de noutate

Ce factori negativi doriți să eliminați în totalitate?

- Aspectele logistice și geografice care nu le permit unor cetățeni să participe la procesul de vot

Ce factori negativi doriți să diminueați?

- Lipsa încrederii în instituțiile și autoritățile statului
- Absenteismul din viața publică și politică, lipsa de interes
- Incidența fraudei electorale

Ce elemente doriți să le aduceți peste standardele actuale?

- Rata de participare la procesele de vot public

- Securitatea și posibilitatea de verificare a integrității fiecărui vot

Ce elemente noi doriți să creați și ce rezolvă acestea?

- Democrație directă, implicare crescută în viața publică și în luarea deciziilor

Criteriile de selecție

Comitetul Miniștrilor din cadrul Consiliului Europei a adoptat în 14 iunie 2017 o Recomandare – Rec(2017)5 – în care listează standardele pentru votul electronic de care orice Stat Membru al Uniunii Europene ar trebui să țină cont.

Aceste standarde ar trebui să fie atent studiate și integrate în orice soluție de vot electronic pe care un Stat Membru al UE îl implementează în următoarea perioadă. Din punct de vedere tehnic, din standardele de mai jos se pot extrage cerințe funcționale și tehnice inclusiv pentru proiectul pilot de vot electronic bazat pe tehnologia blockchain pe care România l-ar putea desfășura în 2028.

STANDARDE PENTRU VOTUL ELECTRONIC RECOMANDATE DE CONSILIUL EUROPEI (2017)⁹

I. Sufragiul universal

1. Interfața electorală a unui sistem de vot electronic trebuie să fie ușor de înțeles și de folosit de către toți alegătorii.
2. Sistemul de vot electronic trebuie conceput, în măsura în care este posibil, astfel încât să permită persoanelor cu handicap și nevoi speciale să voteze independent.
3. Cu excepția cazului în care metodele de vot electronic de la distanță sunt universal accesibile, acestea ar trebui să constituie doar o modalitate suplimentară și opțională de exercitare a dreptului de vot.
4. Înainte de a opta pentru exercitarea dreptului de vot prin intermediul unui sistem electronic de votare la distanță, alegătorii trebuie să conștientizeze faptul că alegerile la care își exercită dreptul de vot prin mijloace electronice sunt alegeri sau referendumuri reale.

II. Sufragiul egal

5. Toate informațiile oficiale privind votarea trebuie prezentate în mod egal, în cadrul și prin toate canalele de vot.
6. În cazul în care se utilizează atât metode de vot electronice, cât și non-electronice în cadrul aceluiași scrutin, trebuie să existe o metodă sigură și fiabilă de a agrega toate voturile și de a calcula rezultatul.
7. Trebuie să se asigure o identificare unică a alegătorilor, într-un mod care să permită distincția clară și sigură a persoanei.

⁹ https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f

8. Sistemul de vot electronic trebuie să acorde accesul unui utilizator doar după autentificarea acestuia ca persoană cu drept de vot.
9. Sistemul de vot electronic va permite exercitarea, stocarea în urna electronică și includerea în rezultatul final al alegerilor doar a numărului corespunzător de voturi la care are dreptul un alegător.

III. Sufragiul liber

10. Intenția de vot a alegătorului nu va fi afectată de sistemul de votare sau de orice altă influență nejustificată.
11. Sistemul de vot electronic va prezenta alegătorului un buletin autentic și informații autentice.
12. Modul în care alegătorii sunt ghidați prin procesul de votare electronică nu trebuie să-i determine să voteze pripit sau fără confirmare.
13. Sistemul de vot electronic trebuie să-i ofere alegătorului posibilitatea de a participa la alegeri sau la referendum, fără ca acesta să-și exprime preferința pentru una dintre opțiuni.
14. Sistemul de vot electronic va acorda asistență alegătorului dacă el sau ea transmite un vot electronic nevalabil.
15. Alegătorul trebuie să poată verifica dacă intenția sa este reprezentată cu precizie, iar votul sigilata intrat în urna electronică fără a fi modificat. Orice influență nejustificată care a modificat votul trebuie să fie detectabilă.
16. Alegătorul primește confirmarea din partea sistemului că votul a fost exprimat cu succes și că întreaga procedură de vot a fost încheiată.
17. Sistemul de vot electronic oferă dovezi solide că fiecare vot autentic este inclus în mod corect în rezultatele alegerilor respective. Dovezile trebuie să poată fi verificate prin mijloace independente de sistemul de vot electronic.
18. Sistemul trebuie să furnizeze dovezi solide că numai voturile alegătorilor eligibili au fost incluse în rezultatul final. Dovezile trebuie să poată fi verificate prin mijloace independente de sistemul de vot electronic.

IV. Sufragiul secret

19. Votarea electronică este organizată astfel încât secretul votului să fie respectat în toate etapele procedurii de votare.
20. Sistemul de vot electronic elaborează și stochează, cât timp este necesar, numai datele cu caracter personal necesare desfășurării alegerilor electronice.
21. Sistemul de vot electronic și orice actor autorizat trebuie să protejeze datele de autentificare, astfel încât părțile neautorizate să nu poată utiliza, intercepta, modifica sau obține cunoștințe despre aceste date.
22. Registrele alegătorilor stocate sau comunicate de sistemul de vot electronic sunt accesibile numai părților autorizate.
23. Un sistem de vot electronic nu oferă alegătorului dovezi privind conținutul votului exprimat, pentru a fi utilizat de către terți.

24. Sistemul de vot electronic nu permite divulgarea numărului de voturi exprimate decât după închiderea urnei electronice de vot. Aceste informații nu vor fi divulgate publicului decât după încheierea perioadei de votare.
25. Votarea electronică asigură respectarea secretului alegerilor anterioare înregistrate și șterse de către alegător, înainte de a-și exprima votul final.
26. Procesul de votare electronică, în special etapa de numărare, trebuie să fie organizat astfel încât să nu fie posibilă reconstituirea unei legături între votul deschis și alegător. Voturile sunt și rămân anonime.

V. Cerințe de reglementare și organizare

27. Statele membre care introduc votul electronic fac acest lucru într-o manieră treptată, progresivă.
28. Înainte de a introduce votul electronic, statele membre fac modificările necesare în legislația relevantă.
29. Legislația relevantă reglementează responsabilitățile pentru funcționarea sistemelor de vot electronic și asigură controlul organismelor electorale asupra acestora.
30. Orice observator trebuie să poată lua parte la numărarea voturilor. Organismul de management electoral este responsabil pentru procesul de numărare.

VI. Transparență și observare

31. Statele membre sunt transparente în toate aspectele legate de votul electronic.
32. Publicul, în special alegătorii, va fi informat, cu mult timp înainte de începerea votării, în limbaj clar și simplu, despre:-orice măsuri pe care un alegător ar trebui să le ia pentru a vota;-utilizarea și funcționarea corectă a unui sistem de vot electronic;-calendarul votului electronic, incluzând toate etapele.
33. Componentele sistemului de vot electronic trebuie să poată fi dezvăluite în scopuri de verificare și certificare.
34. Orice observator, în măsura permisă de lege, va putea să observe și să comenteze alegerile electronice, inclusiv stabilirea rezultatelor.
35. Vor fi utilizate standarde deschise, pentru a permite interoperabilitatea diferitelor componente sau servicii tehnice, eventual derivate dintr-o varietate de surse.

VII. Responsabilitatea

36. Statele membre vor elabora cerințe tehnice, de evaluare și certificare și se vor asigura că acestea reflectă pe deplin principiile juridice și democratice relevante. Statele membre vor actualiza permanent aceste cerințe.
37. Înainte de introducerea unui sistem de vot electronic și la intervale corespunzătoare după aceea, în special după modificarea semnificativă a sistemului, un organism independent și competent va evalua conformitatea sistemului de vot electronic și a oricărei componente a tehnologiei informației și comunicațiilor (TIC) cu cerințele tehnice. Aceasta poate fi o formă de certificare formală sau o altă formă adecvată de control.

38. Certificatul sau orice alt document corespunzător emis trebuie să identifice în mod clar obiectul evaluării și să includă garanții pentru a preveni modificarea sa în mod secret sau în mod accidental.
39. Sistemul de vot electronic poate fi supus auditului. Sistemul de audit trebuie să fie deschis și cuprinzător și să raporteze în mod activ posibilele probleme și amenințări.

VIII. Fiabilitatea și securitatea sistemului

40. Organismul de management electoral este responsabil cu respectarea tuturor cerințelor, chiar și în caz de erori și atacuri. Organismul de management electoral răspunde de disponibilitatea, fiabilitatea, utilitatea și securitatea sistemului de vot electronic.
41. Numai persoanele autorizate de organismul de management electoral au acces la infrastructura centrală, serverele și datele electorale. Numirea persoanelor autorizate să opereze în sistemul de vot electronic trebuie să fie clar reglementată.
42. Înainte ca orice alegeri electronice să aibă loc, organismul de management electoral se va asigura că sistemul de vot electronic este autentic și funcționează corect.
43. Trebuie să se instituie o procedură pentru instalarea regulată a versiunilor actualizate și corectarea tuturor software-urilor relevante.
44. Dacă sunt stocate sau comunicate în afara mediului controlat, voturile sunt criptate.
45. Voturile și informațiile alegătorilor se păstrează sigilate până la începerea procesului de numărare.
46. Organismul de management electoral va opera în siguranță toate materialele criptografice.
47. În cazurile în care apar incidente care ar putea amenința integritatea sistemului, persoanele responsabile cu exploatarea echipamentului informează imediat organismul de management electoral.
48. Trebuie păstrată autenticitatea, disponibilitatea și integritatea registrelor electorale și a listelor de candidați. Sursa datelor trebuie autenticată. Dispozițiile privind protecția datelor trebuie respectate.
49. Sistemul de vot electronic identifică voturile care sunt afectate de o iregularitate.

Descrierea în detaliu a cazului de referință

Mai multe state sau sub-unități administrativ-teritoriale au introdus votul electronic bazat pe tehnologia blockchain în ultimii ani, cele mai multe fiind până acum implementate într-un cadru restrâns (proiecte-pilot) pentru testarea tehnologiei și a aplicabilității și scalabilității acesteia în acest context. Rezultatele acestor proiecte sunt variate: unele au avut succes și ar putea fi extinse gradual la un număr mai mare de votanți, în timp ce altele au eșuat din cauza unor vulnerabilități de securitate sau probleme de funcționare și performanță. Printre țările care au utilizat sau testat până acum un astfel de sistem (fără să includă neapărat și tehnologia blockchain în arhitectura sa) se numără:

Estonia

Estonia este singura țară din lume care oferă tuturor cetățenilor săi posibilitatea de a vota online la alegerile locale, naționale și europene, prin intermediul unui sistem pilotat în 2005 și extins cu succes la nivel național¹⁰, dezvoltat de o companie locală de software¹¹. Sistemul de vot online al Estoniei nu este bazat pe tehnologia blockchain, deși țara este cunoscută pentru faptul că utilizează această tehnologie¹² pentru a securiza și proteja date guvernamentale din mai multe sisteme-cheie ale statului (ex. sănătate, cadastru, registrul comerțului, monitorul oficial etc). Pentru a vota online în sistemul *i-Voting*, cetățenii estonieni folosesc un card fizic ce conține identitatea lor electronică sau versiunea mobilă a acestui card de identitate, care folosește un tip special de cartelă SIM. Datele personale ale cetățenilor sunt eliminate și desprinse de buletinul de vot în momentul în care votul este înregistrat și trimis către numărare, pentru a asigura anonimitatea. Una dintre măsurile gândite pentru a preveni fraudă electorală este posibilitatea de a vota de mai multe ori înainte de data și ora limită, fiecare nou vot anulându-l pe cel precedent.

Elveția

În 2018, Orașul Zug a derulat un proiect pilot de creare de identități digitale „Zug ID” înregistrate în blockchain, pentru locuitorii orașului¹³. Printre alte aplicații, cetățenii au putut folosi această identitate securizată prin blockchain ca să voteze pe diverse teme legate de administrarea orașului lor.

Tot Elveția le permite și cetățenilor din străinătate și unor rezidenți să voteze online în alegerile locale în anumite cantoane sau în referendumuri¹⁴.

SUA - Virginia de Vest

Cetățenii statului american au avut la dispoziție o aplicație mobilă, cu blockchain în spate, ca să poată vota la alegerile din 2018¹⁵. În mod particular, soldații aflați în misiuni au fost încurajați să-și exercite dreptul de vot prin sistemul electronic.

Sistemul a fost pre-testat în două districte ale statului și trecut și prin patru procese de audit independente. Pentru înregistrare, votantul trebuie să încarce fotografia unui act de identificare cu poză, și un selfie curent, după care trece printr-un proces de autentificare multifactorială.

Australia – New South Wales

¹⁰ https://en.wikipedia.org/wiki/Electronic_voting_in_Estonia

¹¹ <https://digiexpo.e-estonia.com/Solutions/helmes-e-election-system/>

¹² <https://e-estonia.com/wp-content/uploads/2020mar-faq-ksi-blockchain-1-1.pdf>

¹³ www.swissinfo.ch/eng/crypto-valley_-_switzerland-s-first-municipal-blockchain-vote-hailed-a-success/44230928

¹⁴

https://www.ifes.org/sites/default/files/considerations_on_internet_voting_an_overview_for_electoral_decision-makers.pdf

¹⁵ <https://www.bloomberg.com/news/articles/2018-09-11/blockchain-based-voting-is-coming-to-west-virginia>

Statul australian New South Wales le permite cetățenilor cu dizabilități sau celor care locuiesc în zone izolate sau în afara statului să voteze online¹⁶, însă nu există încă planuri de a extinde acest sistem.

Opțiuni de îmbunătățire

Experiența acumulată de alte țări, în particular cazul de succes al Estoniei, demonstrează că implementarea unui sistem de vot electronic la nivel național este fezabilă și benefică. Totuși deocamdată nu există cazuri de implementare care să folosească tehnologia blockchain pe scară largă pentru votul electronic, prin urmare abordarea unei implementări de vot electronic la nivel național folosind blockchain trebuie să fie fazată, pornind cu un proiect pilot, cu utilizare restrânsă controlată, urmată eventual de extindere și generalizare.

Alegereile tehnologice sunt esențiale pentru a asigura capacitatea de scalare și performanța sistemului.

Analiza comparativă

Comparație dintre sisteme de vot existente bazate pe blockchain¹⁷

Online Voting Platforms	Framework	Language	Cryptographic Algorithm	Consensus Protocol	Main Features (Online Blockchain Voting System)							
					Audit	Anonymity	Verifiability by Voter	Integrity	Accessibility	Scalability	Accuracy/Correctness	Affordability
Follow My Vote	Bitcoin	C++/Python	ECC	PoW	✓	✓	✓	✓	✓	✗	✓	✓
Voatz	Hyperledger Fabric	Go/JavaScript	AES/GCM	PBFT	✓	✓	✓	✓	✓	✗	✓	✓
Polyas	Private/local Blockchains	NP	ECC	PET	✓	✓	✓	✓	✓	✗	✓	NA
Luxoft	Hyperledger Fabric	Go/JavaScript	ECC/ElGamal	PBFT	✓	✓	✓	✓	✓	✗	✓	✓
Polys	Ethereum	Solidity	Shamir's Secret Sharing	PoW	✓	✓	✓	✓	✓	✗	✓	✓
Agora	Bitcoin	Python	ElGamal	BFT-r	✓	✓	✓	✓	✓	✗	✓	✓

Comparație între cele mai cunoscute platforme blockchain din perspectiva scalabilității¹⁸

Framework	Year Release	Generation Time	Hash Rate	Transactions Per Sec	Cryptographic Algorithm	Mining Difficulty	Power Consumption	Reward/Block	Scalability
Bitcoin	2008	9.7 min	899.624 Th/s	4.6 max 7	ECDSA	High (around 165,496,835,118)	Very High	25 BTC	Very Low
Ethereum	2015	10 to 19 s	168.59 Th/s	15	ECDSA	High (around 10,382,102)	High	5 ether	Low
Hyperledger Fabric	2015	10 ms	NA	3500	ECC	No mining required	Very Low	No built-in cryptocurrency	Good
Litecoin	2011	2.5 min	1.307 Th/s	56	Script	Low 55,067	Moderate	25 LTC	Moderate
Ripple	2012	3.5 s	NA	1500	RPCA	No mining required	Very Low	Base Fee	Good
Dogecoin	2013	1 min	1.4 Th/s	33	Script	Low 21,462	Low	10,000 Doge	Low
Peercoin	2012	10 min	693.098 Th/s	8	Hybrid	Moderate (476,560,083)	Low	67.12 PPC	Low

¹⁶

https://www.ifes.org/sites/default/files/considerations_on_internet_voting_an_overview_for_electoral_decision-makers.pdf

¹⁷ : Jafar, U.; Aziz, M.J.A.; Shukur, Z. Blockchain for Electronic Voting System—Review and Open Research Challenges. Sensors 2021, 21, 5874. <https://doi.org/10.3390/s21175874>

¹⁸ Ibid.

Constrângeri privind implementarea

Indiferent de tehnologia folosită, sistemele de vot sunt foarte dificil de schimbat în orice stat, iar guvernele s-ar putea expune unui risc major prin implementarea unui sistem de vot electronic online pe scară largă, chiar dacă acesta va rula în paralel cu cel tradițional pentru o perioadă nelimitată de timp (ca o alternativă, în același mod în care funcționează votul prin corespondență în prezent).

Mai mult, deși tehnologia blockchain are o serie de caracteristici care ar face-o potrivită pentru susținerea unui astfel de sistem, mulți experți argumentează că ea nu a ajuns încă la o maturitate deplină din punct de vedere al performanței, eficienței sau securității. O dovadă în acest sens o reprezintă apariția frecventă pe piața comercială de tehnologie a unor sisteme blockchain îmbunătățite care promit că pot avea rezultate mult mai bune decât versiunile precedente, aceste salturi tehnologice demonstrând volatilitatea și imaturitatea acestei piețe și ilustrând riscul ca sistemul dezvoltat în cadrul acestui proiect să piardă teren în fața altora similare, dar mai performante în doar câțiva ani.

Resurse tehnice pentru implementare

Resursele tehnice necesare pentru implementarea unui sistem de vot electronic bazat pe blockchain în regim de proiect pilot în anul 2028 se împart în două categorii: resurse hardware și resurse software.

Componentele minime pe care acest sistem va trebui să le includă sunt următoarele:

- Resurse de stocare și procesare (hardware) – cloud sau on-premise:
 - Servere pentru baze de date tradiționale;
 - Servere cu rol de noduri blockchain;
 - Infrastructură middleware (componente care asigură conectarea bazelor de date cu motorul/motoarele blockchain utilizate și sincronizarea datelor între acestea).
- Interfețe software distincte pentru următoarele categorii de utilizatori:
 - Administratori (personal al instituției/instituțiilor cu rol central în dezvoltarea și gestionarea sistemului – ex. STS și AEP);
 - Instituții secundare (instituții cu rol secundar în desfășurarea proiectului pilot, al căror personal va avea diverse roluri în cadrul ecosistemului tehnic, cum ar fi verificare/audit/monitorizare/numărare voturi/comunicare rezultate – ex. MAI, ADR, BEC);
 - Cetățeni cu drept de vot.

Resurse umane pentru implementare

Planificarea, dezvoltarea și implementarea unui sistem de vot electronic bazat pe blockchain în regim de proiect pilot în anul 2028 și evaluarea rezultatelor acestui pilot în

vederea posibilității de a extinde sistemul de vot electronic la nivel național sunt activități care vor necesita implicarea unui număr mare de specialiști și reprezentanți ai instituțiilor publice relevante.

Numărul și categoriile de specialiști pe care un astfel de proiect îl necesită pot fi specificate cu mai multă acuratețe după o analiză foarte detaliată a proiectului, însă se pot menționa deja o serie de domenii și subiecte în care sunt necesare aptitudini avansate pentru dezvoltarea proiectului:

- Arhitecturi software
- Infrastructuri hardware
- Analiză de business
- Tehnologia blockchain/DLT
- Securitate cibernetică
- Criptografie
- Design UX/UI, design grafic, design web/mobile
- Dezvoltare aplicații web, mobile
- Mentenanță sisteme informatice – hardware & software
- Sisteme electorale
- Tehnologie și inovație în sectorul public
- Educație și comunicare publică
- Managementul schimbării
- Audit sisteme tehnice
- Analiză de impact.

Resurse financiare pentru implementare

Implementarea proiectului pilot pentru introducerea unui sistem de vot electronic bazat pe blockchain va implica o serie de costuri semnificative pentru care instituția/grupul de instituții responsabile cu implementarea vor trebui să identifice surse de finanțare stabile și sustenabile. Proiectarea costurilor poate fi făcută separat pentru proiectul pilot și pentru posibila extindere a acestuia la scară largă, însă cele două dimensiuni ale proiectului trebuie bine corelate astfel încât pilotul să reprezinte o resursă utilă din punct de vedere al estimării costurilor unui proiect la nivel național.

Categoriile de costuri asociate cu proiectul pilot sunt următoarele:

- Costuri de analiză de business/cercetare/elaborare proiect tehnic

- Costuri de dezvoltare și licențe software
- Costuri de infrastructură hardware
- Costuri de integrare cu sisteme existente
- Costuri pentru resurse umane
- Costuri de testare
- Costuri de mentenanță
- Costuri de monitorizare/evaluare.

Resurse logistice pentru implementare

Din punct de vedere logistic, pentru dezvoltarea și implementarea proiectului va fi nevoie de resurse precum dispozitive de lucru adecvate din punct de vedere al performanței (PC, laptop) pentru toți actorii implicați în faza de dezvoltare a proiectului, dar și de resurse și materiale educaționale și informative pentru utilizatorii finali ai soluției (personal al instituțiilor, cetățeni care participă la pilot ca votanți).

Riscuri și planuri de contingență

Riscuri de finanțare

- Reducerea/eliminarea finanțării pentru implementarea unui proiect pilot în cadrul alegerilor europarlamentare din 2028 sau ulterior, în implementarea pe scară largă în toate tipurile de alegeri – risc mediu.

Riscuri legislative

- Incompatibilitatea votului electronic de la distanță cu legislația din România – risc ridicat.

Riscuri ale costurilor de întreținere

- Reducerea/eliminarea finanțării pentru mentenanța pe termen lung a sistemului de vot electronic – risc mediu.

Riscuri de ocupare

- Lipsa de specialiști care să dezvolte, testeze, administreze și întrețină sistemul de vot electronic – risc mediu.
- Lipsa personalului instruit în modul de operare a sistemului în cadrul instituțiilor relevante – risc mediu.

- Un număr insuficient de membri ai publicului larg care să fie dispuși să participe în proiectul pilot – risc scăzut.

Riscuri operaționale

- Întârzieri față de planul de execuție pentru dezvoltarea componentelor software sau hardware – risc ridicat.
- Probleme de disponibilitate a specialiștilor implicați în proiect sau lipsa unui număr suficient de specialiști (manageri de proiect, specialiști hardware/software, alte resurse umane importante) – risc mediu.
- Întreruperi în serviciile de electricitate sau internet care să pericliteze buna funcționare a sistemului – risc scăzut.

Riscuri de planificare

- Estimarea necorespunzătoare a duratei de lucru pentru diferite faze ale proiectului – risc ridicat.

Riscuri de schimbare a opțiunilor politice (riscuri decizionale)

- Opre/inconsistență a finanțării pe termen lung a proiectului – risc ridicat.
- Absența unui climat politic favorabil pentru dezvoltarea/extinderea/mentenanța proiectului – risc ridicat.

Riscuri legate de procedurile de achiziții publice

- Dificultăți și neclarități în elaborarea documentației necesare pentru demararea achizițiilor publice (caietelor de sarcini), în special datorită numărului mare de părți interesate și de componente ale sistemului – risc mediu.
- Lipsa furnizorilor suficient de experimentați/specializați pe cerințele unui sistem de vot electronic bazat pe tehnologia blockchain – risc mediu.
- Întârzieri cauzate de potențialele contestații la atribuirea unor contracte de achiziții publice care ar putea prelungi durata de dezvoltare a sistemului astfel încât proiectul pilot să nu se poată desfășura în condiții optime conform planului, în cadrul alegerilor europarlamentare din 2028 – risc mediu.

Riscuri reputaționale (influența opiniei publice)

- Orice problemă de funcționare a sistemului, în cadrul proiectului-pilot, ar putea genera o respingere a acestuia din partea opiniei publice, chiar dacă problemele identificate ar putea fi corectate până la implementarea pe scară largă – risc ridicat.

Riscuri ale schimbărilor tehnologice

- Deși a apărut în urmă cu mai mult de un deceniu, tehnologia blockchain încă e în plină dezvoltare, atât din punct de vedere tehnic și al performanței, cât și din punct de vedere al aplicabilității și fezabilității în diverse cazuri de utilizare. Prin urmare, unul dintre riscurile asociate tehnologiei blockchain este acela ca un sistem dezvoltat în următorii 3-5 ani să ajungă să fie perimat și să nu mai facă față cerințelor și așteptărilor de performanță, eficiență și scalabilitate la foarte puțin timp de la lansare – risc mediu-ridicat.
 - Sistemul de vot electronic ar trebui construit în așa fel încât să poată fi actualizat și îmbunătățit cu efort tehnic, operațional și financiar minim, inclusiv să ofere posibilitatea de schimbare a soluției blockchain utilizate.

Riscuri ale volumului de activitate estimat

- O rată de utilizare/adopte scăzută a sistemului care să îl facă inefficient din punct de vedere financiar și operațional – risc ridicat.
 - În cazul în care autoritățile naționale decid că este oportună extinderea sistemului de vot electronic în urma rezultatelor pilotului, va fi necesară impunerea unor praguri minime de utilizare care vor trebui atinse odată cu primele utilizări pe scară largă ale sistemului pentru ca autoritățile să poată decide dacă acesta rămâne sau nu funcțional pe termen lung și un plan de contingență pentru scoaterea din uz a sistemului în cazul în care nu se dovedește a fi sustenabil.

Interacțiunea cu alte sisteme tehnice

- Sistemul informatic de monitorizare a prezenței la vot și de prevenire a votului ilegal (SIMPV) – sistem în care a fost deja implementată tehnologia blockchain, în vederea creșterii rezilienței sistemului electoral românesc, precum și a încrederii alegătorilor și competitorilor electorali în integritatea datelor și informațiilor înregistrate.
- Sistemul informatic de centralizare a datelor din procesele-verbale privind consemnarea rezultatelor votării (SICPV) - sistem în care a fost deja implementată tehnologia blockchain, în vederea creșterii rezilienței sistemului electoral românesc, precum și a încrederii alegătorilor și competitorilor electorali în integritatea datelor și [informațiilor înregistrate](#).
- Sistemul Național de Interoperabilitate – lansat în noiembrie 2021, posibilitate de extindere pentru mai multe instituții/servicii publice în următorii ani – printre acestea s-

ar putea număra și sisteme/registre publice care au legătură cu procesul de vot, așadar ar putea exista nevoia de interacțiune între sisteme.

- Platforma Software Centralizată pentru Identificare Digitală (PSCID) – conform Autorității pentru Digitalizarea României, PSCID va reprezenta un punct unic de intrare pentru acces la toate platformele de servicii publice – planificat pentru finalizare în 2023.

Diagrama pentru implementare

Stadiile de implementare ale sistemului de vot electronic, de la conceptualizarea inițială și până la implementarea proiectului pilot în 2028 vor fi definite folosind conceptul de [Technology Readiness Level \(TRL\) utilizat la nivelul Comisiei Europene](#).

Activitate			Rezultat	An implementare										
				1	1,5	2	2,5	3	3,5	4	4,5	5-7	8	10
Pregătirea proiectului pilot și a procedurilor de evaluare/analiză	2 ani: Proiectare, dezvoltare, implementare back-end și front-end		Sistem prototip verificat (TRL4 [Eroare! Fără sursă de referință., Eroare! Fără sursă de referință.])											
	0,5 ani: Formare personal și testare beta	0,5 ani: Formare personal, training pe sistemul dezvoltat	Tehnologie validată în mediu relevant (TRL5)											
		0,5 ani: Testare beta de către utilizatori	Tehnologie demonstrată în mediu relevant (TRL6)											
	1 an: „Smoke testing”, ucenic non-producție		Sistem model și prototip demonstrate în mediu operațional (TRL7)											
	0,5 ani: Analiză comparativă rezultate sistem nou/sisteme existente de referință		Sistem complet și validat (TRL8)											
	1 an: Optimizare/eliminarea defecte raportate de utilizatori		Sistem validat în mediul operațional (TRL9)											

Activitate		Rezultat	An implementare										
			1	1,5	2	2,5	3	3,5	4	4,5	5-7	8	10
Operaționalizarea sistemului de vot electronic de la distanță bazat pe blockchain pentru desfășurarea proiectului pilot în cadrul alegerilor parlamentare din 2028	Desfășurarea proiectului pilot în cadrul alegerilor parlamentare din 2028	Cetățenii invitați să participe în proiectul pilot au posibilitatea de a-și exercita votul online, de la distanță, prin intermediul noului sistem.											
	Analizarea și evaluarea rezultatelor pilotului	Concluzii despre posibila continuare a dezvoltării pentru adopția pe scară largă											

Metodologia de management a proiectului și modelul de dezvoltare

Proiectul introducerii unui sistem de vot electronic bazat pe tehnologia blockchain în România este format din mai multe categorii de activități, iar fiecare dintre aceste părți poate fi considerată un proiect în sine din punct de vedere al disciplinei managementului de proiect: software, hardware, logistică, aliniere legislativă, campanii de educație și informare. Fiecare categorie de activități va trebui să fie gestionată de una sau mai multe instituții diferite, care vor aplica metode de management și dezvoltare cel mai probabil diferite pentru a ajunge la rezultatele dorite, însă această variantă este preferabilă aplicării unei metodologii rigide de-a lungul întregului proiect care să fie impusă tuturor instituțiilor și entităților implicate, fapt care ar putea duce la blocaje din cauza lipsei de experiență sau de personal specializat în aplicarea metodologiei respective. Evaluarea metodologiilor de management și a rezultatelor acestora în diferitele componente ale proiectului pilot poate fi efectuată odată cu evaluarea generală a pilotului, iar eventualele modificări vor putea fi aplicate când (și dacă) proiectul de vot electronic va fi extins pe scară largă ulterior.

Cu toate acestea, este însă nevoie și ca o instituție cheie să preia conducerea întregului proiect pilot pentru a urmări toate aceste subproiecte ale celorlalte instituții, astfel încât proiectul pilot să poată fi pregătit corespunzător din toate punctele de vedere și să se poată desfășura în condiții optime în anul 2028. Ținând cont de contextul național și de experiența instituțională, cea mai potrivită instituție care să supravegheze întregul proiect ar fi Serviciul de Telecomunicații Speciale (STS), instituție care are deja experiență în implementarea tehnologiei blockchain în timpul proceselor electorale (tehnologia a fost utilizată ca instrument care să asigure transparența și integritatea datelor la alegerile parlamentare din 2020)¹⁹.

¹⁹ <https://www.sts.ro/ro/anunturi/tehnologia-blockchain-garanteaza-integritatea-sistemelor-informatic-pentru-alegerile-parlamentare>.

Precondiții și factori critici pentru succes

Pentru ca proiectul să poată avea succes, este nevoie ca următoarele precondiții să fie îndeplinite:

- Legislație care să permită implementarea unui sistem electronic de vot bazat pe tehnologia blockchain.
- O colaborare continuă între instituțiile implicate în proiect, indiferent de posibilele schimbări care ar putea avea loc la nivel politic.
- Efectuarea unei analize ex-ante extrem de detaliate în legătură cu proiectul, care să ia în considerare toate direcțiile potențiale de impact ale acestuia, atât la nivel tehnic, cât și la nivel politic, social, economic. Planul de dezvoltare și implementare care va reieși din analiză va trebui să detalieze cu exactitate obiective generale și intermediare, resurse umane, tehnice și financiare necesare pentru fiecare fază a proiectului, calendar de implementare, plan de lansare etc.

Indicatori pentru monitorizare și evaluare

Indicatori de ieșire:

- Sistemele informatice create pentru implementarea proiectului pilot, pe baza cărora se poate construi în continuare pentru ca sistemul de vot electronic să fie extins și pus la dispoziția tuturor cetățenilor români de pe teritoriul țării și din străinătate.
- Procesul de evaluare a proiectului pilot le va permite autorităților statului să facă observații și să tragă concluzii importante nu numai despre atingerea obiectivelor proiectului în sine, ci și despre calitatea și eficiența colaborării dintre mai multe instituții-cheie ale statului, cu implicații pentru alte proiecte și planuri viitoare de colaborare (fie aspecte pozitive ale experienței, fie constatări importante cu privire la aspectele care au nevoie de îmbunătățiri majore). În baza acestor observații făcute prin intermediul procesului de evaluare a proiectului pilot, autoritățile vor putea decide și asupra continuării sau abandonării implementării votului electronic bazat pe blockchain.

Indicatori de rezultat:

- Un proiect pilot pentru implementarea unui sistem de vot electronic bazat pe tehnologia blockchain care se desfășoară cu succes, fără incidente sau probleme majore, ar putea determina extinderea pe scară largă a acestui sistem, oferind un acces mai bun cetățenilor din țară și din străinătate la procesul de vot de la distanță. Prin urmare, dacă procesul continuă, rezultatele ar putea include o creștere a participării la vot în alegerile post-2028.

Indicatori de impact:

- O participare mai mare la vot datorită implementării cu succes a unui sistem de vot electronic de la distanță bazat pe tehnologia blockchain ar crea efecte pozitive pe termen lung și ar crește

interesul cetățenilor în viața publică și în teme și inițiative civice și ar crește coeziunea socială.

- Un sistem de vot electronic bazat pe blockchain care funcționează conform standardelor impuse de contextul național și internațional ar poziționa România ca lider în domeniile guvernării digitale, inovației și tehnologiei, iar țara ar putea reprezenta un exemplu și pentru alte state care sunt interesate de implementarea unui sistem de vot electronic.

Referințe bibliografice

1. <https://www.oecd.org/social/society-at-a-glance-19991290.htm>.
2. <https://www.edupedu.ro/analiza-doar-25-dintre-tinerii-de-pe-listele-electorale-au-votat-la-parlamentare-cea-mai-scazuta-prezenta-de-la-alegerile-din-ultimii-4-ani/>.
3. <https://republica.ro/tinerii-de-18-24-de-ani-o-dezagire-in-2016-dar-o-speranta-in-2020>.
4. <https://rm.coe.int/168071bc84>.
5. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f.
6. <https://www.coindesk.com/tech/2020/11/16/new-mit-paper-roundly-rejects-blockchain-voting-as-solution-to-election-woes/>.
7. <https://www.roaep.ro/legislatie/wp-content/uploads/2017/08/Traducere-Recomandare.pdf>.
8. https://europeandigital.org/files/19/Internet_Voting_Challenges_and_Solutions_ROM.pdf.
9. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f.
10. https://en.wikipedia.org/wiki/Electronic_voting_in_Estonia.
11. <https://digiexpo.e-estonia.com/Solutions/helmes-e-election-system/>.
12. <https://e-estonia.com/wp-content/uploads/2020mar-faq-ksi-blockchain-1-1.pdf>.
13. www.swissinfo.ch/eng/crypto-valley-switzerland-s-first-municipal-blockchain-vote-hailed-a-success/44230928.
14. https://www.ifes.org/sites/default/files/considerations_on_internet_voting_an_overview_for_electoral_decision-makers.pdf.
15. <https://www.bloomberg.com/news/articles/2018-09-11/blockchain-based-voting-is-coming-to-west-virginia>.
16. https://www.ifes.org/sites/default/files/considerations_on_internet_voting_an_overview_for_electoral_decision-makers.pdf.
17. <https://doi.org/10.3390/s21175874> Jafar, U.; Aziz, M.J.A.; Shukur, Z. Blockchain for Electronic Voting System—Review and Open Research Challenges. Sensors 2021, 21, 5874.
18. <https://www.sts.ro/ro/anunturi/tehnologia-blockchain-garanteaza-integritatea-sistemelor-informatic-pentru-alegerile-parlamentare>



Proiect:

Proiect selectat în cadrul Programului Operațional Capacitate Administrativă cofinanțat de Uniunea Europeană, din Fondul Social European

Axa Prioritară 1: Administrație publică și sistem judiciar eficiente

Obiectivul specific 1.1: Dezvoltarea și introducerea de sisteme și standarde comune în administrația publică ce optimizează procesele decizionale orientate către cetățeni și mediul de afaceri, în concordanță cu SCAP.

Titlul proiectului: „Cadru strategic pentru adoptarea și utilizarea de tehnologii inovative în administrația publică 2021-2027 – soluții pentru eficientizarea activității”

COD: SIPOCA 704

Beneficiar: AUTORITATEA PENTRU DIGITALIZAREA ROMÂNIEI

Partener: UNIVERSITATEA TEHNICĂ DIN CLUJ - NAPOCA

Fundamentarea cazului de utilizare și studiu de evaluare ex-ante pentru Monitorizarea execuției bugetare cu accent pe achizițiile publice

Cuprins

Acronime și abrevieri	3
Referințe	4
Scopul intervenției	5
Părțile interesate.....	7
Beneficiile estimate.....	9
Factori critici în asociere cu cazurile de utilizare	9
Provocări tehnice în implementarea intervenției.....	10
Procese curente care ar putea fi afectate de dezvoltarea proiectului	10
Obiectivele funcționale	11
Obiectivele de performanță.....	12
Elementele de noutate	15
Criteriile de selecție	16
Descrierea în detaliu a cazului de referință	18
Opțiuni de îmbunătățire	18
Analiza comparativă.....	19
Constrângeri privind implementarea.....	21
Resurse tehnice pentru implementare	21
Resurse umane pentru implementare.....	22
Resurse financiare pentru implementare.....	25
Resurse logistice pentru implementare.....	29
Riscuri și planuri de contingență.....	29
Interacțiunea cu alte sisteme tehnice	30
Diagrama pentru implementare	30
Metodologia de management a proiectului și modelul de dezvoltare	31
Precondiții și factori critici pentru succes	32
Indicatori pentru monitorizare și evaluare	33
Referințe bibliografice.....	33

Acronime și abrevieri

Abreviere sau acronim	Expresia completă	Explicație
WEF	World Economic Forum	Forumul Economic Mondial este o organizație internațională neguvernamentală și de lobby cu sediul în Cologny, cantonul Geneva, Elveția.
HHS	U.S. Department of Health & Human Services	
GSA	General Services Administration	
IDB	Inter-American Development Bank	
OCDE	Organizația pentru Cooperare și Dezvoltare Economică	
DIDs	Decentralized identifiers	Tip nou de identificador care permite o identitate digitală descentralizată și verificabilă.
EBSI	European Blockchain Services Infrastructure	Infrastructura europeană pentru servicii blockchain, promovată de Comisia Europeană.
IdM	Identity Management	Cadru de politici și tehnologii pentru a se asigura că utilizatorii potriviți (într-o întreprindere) au acces adecvat la resursele tehnologice.
WOT	web-of-trust	Este un concept utilizat în PGP, GnuPG și alte sisteme compatibile cu OpenPGP pentru a stabili autenticitatea legăturii dintre o cheie publică și proprietarul acesteia.
EVM	Ethereum Virtual Machine	
PGP	Pretty Good Privacy	Program de criptare care oferă confidențialitate criptografică și autentificare pentru comunicarea datelor.
POW	Proof-of-Work	O formă de dovadă criptografică în care o parte demonstrează altora munca pentru a fi remunerat.

Referințe

O serie de proiecte guvernamentale cu scopul de a spori eficiența și transparența în domeniul exercițiului bugetar (în special pentru achizițiile publice) sunt cu potențial și par destul de promițătoare pentru a fi extinse. Totuși, efectele lor asupra eliminării corupției sunt mai puțin clare, în special pentru formele sofisticate, cum ar fi conflictul de interese. Din 2017, mai multe guverne au apelat la tehnologia blockchain pentru a-și îmbunătăți sistemele de achiziții publice și aparatele bugetare în format electronic.

Japonia¹ dorește să utilizeze tehnologia de stocare a datelor din spatele bitcoin și a monedelor virtuale similare pentru a actualiza modul în care persoanele fizice și companiile interacționează electronic cu guvernul, cu scopul de a consolida securitatea informațiilor, reducând în același timp costurile administrative. Ministerul Afacerilor Interne și Comunicațiilor testează un sistem bazat pe blockchain pentru procesarea licitațiilor guvernamentale.

Statele Unite vizează reducerea costurilor și raportul costuri-beneficii prin automatizarea analizei prețurilor (HHS)² și revizuirea contractelor (GSA)³.

Mexic (State of Jalisco)⁴ urmărește să sporească transparența și să reducă corupția. În august 2021, a fost executat primul caz real al unei licitații desfășurate pe o rețea blockchain din Mexic. Tot atunci a fost prezentat și modelul de guvernare care guvernează această rețea, care promite să fie un aliat al achizițiilor publice în ceea ce privește transparența.

Coreea de Sud (Seoul)⁵ caută să îmbunătățească evaluarea sumelor licate. Districtul intenționează să extindă treptat sistemul de evaluare a propunerilor folosind blockchain. Este planificată extinderea și completarea obiectivului de aplicare la toate proiectele de evaluare a propunerilor din cadrul aparatului administrativ bugetar central în acest an și extinderea și diseminarea acestuia către alte administrații locale.

Guvernul columbian⁶ recunoaște că achizițiile publice și bugetarea participativă reprezintă unele dintre cele mai slabe verigi în eforturile anticorupție ale țării la nivel național, regional și local. Cu toate acestea, încercările recente de reformă, inclusiv 2011 Legea anticorupție și noua lege federală anticorupție, au contribuit prea puțin pentru a reduce cazurile

¹ <https://asia.nikkei.com/Politics-Economy/Policy-Politics/Japan-looks-to-blockchains-for-more-secure-e-government-systems>

² <https://govmatters.tv/hhs-obtains-first-blockchain-ato-in-federal-government/>

³ <https://fcw.com/blogs/lectern/2017/10/comment-kelman-gsa-blockchain.aspx>

⁴ <https://www.eleconomista.com.mx/tecnologia/Gobierno-federal-realiza-el-primer-caso-real-de-licitacion-con-blockchain-en-agosto-20180727-0035.html>

⁵ https://newsis.com/view/?id=NISX20190116_0000531364&cID=10801&pID=14000

⁶ WEF_Blockchain_Government_Transparency_Report(weforum.org)
https://www3.weforum.org/docs/WEF_Blockchain_Government_Transparency_Report.pdf

de corupție în acest domeniu. Astfel, sectorul public columbian a decis să adopte abordări inovatoare în materie de combatere a corupției, care, printre alte inițiative, includeți un proiect comun între Biroul inspectorului general columbian, IDB și WEF pentru dezvoltarea unui răspuns bazat pe tehnologia blockchain la corupția achizițiilor publice.

Scopul intervenției

Definirea problemei

Potrivit unor organizații internaționale de top, cum ar fi OCDE și *Transparency International*, **achizițiile publice, contracte sau licitații guvernamentale** sunt unele dintre activitățile din sectorul public care sunt cele mai vulnerabile în fața corupției. Guvernele cheltuiesc împreună aproximativ 9,5 trilioane de dolari privind contractele de achiziții publice la nivel mondial prin intermediul proceselor adesea marcate de complexitate, opacitate și un grad ridicat de eroare umană. În întreaga lume, OCDE și *Oficiul Națiunilor Unite pentru Droguri și Criminalitate* estimează că 10-30% din valoarea totală a unui contract de achiziții publice este de obicei pierdută este deturnată în buzunarele guvernelor afectate de corupție. Motivele principale sunt:

- a) În fiecare an, guvernele cheltuiesc între 10% și 30% din PIB-ul național privind achizițiile publice conform exercițiului bugetar anual. Procente însemnate din bugetul alocat sunt alocate clientelar, în funcție de interesul partidului aflat de la guvernare pentru a câștiga capital electoral și susținerea filialelor din teritoriu;
- b) Proiectele publice-private implică o atenție deosebită și repetată interacțiunea dintre funcționarii guvernamentali și sectorul privat. Combinarea activității sectorului public cu cea privată, care are la bază motivații de profit, sunt supuse unui risc ridicat de corupție;
- c) Procesul de achiziție este adesea complex și birocratic, fapt care favorizează creșterea oportunităților și motivația pentru se găsi scurtături administrative pentru rectificări bugetare dedicate pentru a spori artificial bugetul unui anumit Minister sau pentru un proiect specific;
- d) Transparența scăzută în evaluarea nevoilor alocărilor bugetare corecte, ale specificațiilor contractatelor de licitație și selecția furnizorilor, ceea ce lasă distribuirea unor sume mari de bani la discreția funcționarilor din domeniul achizițiilor publice.
- e) Oamenii rareori raportează activități de corupție în public procesul de achiziție chiar și atunci când devin conștienți de ele. Acest lucru este adesea atribuit unui sentiment de indiferență față de pierderile financiare guvernamentale, absența unei raportări eficace și a unei modalități de urmărirea a integrității acestui proces.

O mare parte din activitățile specific unui exercițiu bugetar sunt netransparente și, prin urmare, deosebit de vulnerabil la practicile corupte. De exemplu, acorduri de achiziție directă și negociate contractual nu sunt, în general, atribuite pe baza unui set de criterii predeterminate, obiective, care le fac pe acestea procese de atribuire mult mai dificil de monitorizat sau de auditat în comparație cu procedurile competitive precum licitația deschisă. În mod similar, lipsa

ghidurilor de piață ușor de obținut și imprevizibilitatea multor proiecte majore, de exemplu lucrări de construcții, evaluări ale necesităților instituțiilor în viitor și ajustări post-atribuire sunt în mare parte la discreția funcționarilor guvernamentali. Corupția în achizițiile publice erodează încrederea în guvern și instituții, promovează practici comerciale neloiale, are ca rezultat distorsiunile pieței, slăbește apetitul investitorilor străini și scade accesul și calitatea publicului atât de necesar la bunuri și servicii⁷.

În cazul contractelor guvernamentale mari, achizițiile publice constă de obicei, în patru etape: planificare, licitație, evaluarea ofertelor și atribuirea contractului, etapa post-atribuire (implementarea și monitorizarea). Contractele mai mici sau cele foarte complexe pot fi acordate printr-un acord de achiziție direct sau respectiv negociat direct. Fiecare etapă a fiecărui tip de proces de achiziții publice prezintă propriile provocări și riscuri pentru corupție, inclusiv mita, influența nejustificată asupra guvernului evaluări, coluziune în sectorul privat, trucarea ofertelor, constrângere; extorsiune, depuneri frauduloase și evaluări ale ofertelor.

Obiectivele generale

Execuția bugetară constă în două operațiuni principale: **angajamente și plăți**. În ceea ce privește angajarea cheltuielilor, se ia o decizie de a utiliza o anumită sumă de la o linie bugetară specifică în scopul finanțării unei anumite activități. Procedura execuției bugetare este formată din următoarele faze:

1. repartizarea pe trimestre a veniturilor și cheltuielilor bugetare;
2. execuția de casă bugetară;
3. realizarea veniturilor bugetare;
4. **efectuarea cheltuielilor bugetare (achiziții).**

Totodată, coordonarea activității privind execuția bugetară de ansamblu, urmărind și corelarea operațiunilor de alocare a sumelor din buget, pentru efectuarea de cheltuieli, cu cele de încasare a veniturilor bugetare se asigură printr-un departament specializat, care funcționează în Ministerul Finanțelor Publice.

Obiectivele generale urmărite prin adoptarea unei soluții bazate pe tehnologia blockchain pentru monitorizarea execuției bugetare și a achizițiilor publice sunt următoarele:

- Creșterea transparenței și responsabilității instituțiilor guvernamentale și, prin urmare, reducerea cazurilor de corupție în administrația publică locală și centrală;
- Digitalizarea serviciilor și proceselor guvernamentale pentru a face instituțiile publice mai eficiente, reducând costurile și îmbunătățind calitatea interacțiunii dintre cetățeni și administrația locală, de stat sau națională;
- Generarea unui prototip și a recomandărilor de politici publice privind utilizarea tehnologiei Blockchain în cadrul achizițiilor publice.
- Accelerarea digitalizării serviciilor publice;

⁷ https://www.transparency.org/files/content/corruptionqas/Topic_Guide_Codes_of_Conduct.pdf

- Dezvoltarea/implementarea de noi sisteme informatice într-un mod unitar, rapid și profesionist;
- Asigurarea mentenanței evolutive și preventive a sistemelor deja dezvoltate;
- Asigurarea interoperabilității bazelor de date ale instituțiilor publice locale și centrale;
- Îmbunătățirea fluxurilor operative, în vederea transformării digitale, pentru instituții publice locale și centrale;
- Îmbunătățirea accesului la informațiile și serviciile oferite de către autoritățile administrației publice printr-o deservire rapidă și eficientă;
- Creșterea calităților serviciilor publice oferite de către instituțiile publice locale și centrale.

Obiectivele specifice

- Construirea unui centru integrat de bugetare publică electronică într-un proiect pilot.
- Verificarea facilă și auditarea exercițiului bugetar anual și alocării bugetare pentru un eșantion de instituții parte din proiect.
- Verificarea, auditarea și urmărirea transparentă a achizițiilor publice efectuate de instituțiile participante pentru un eșantion de instituții parte din proiect.
- Alocarea și cheltuirea bugetului alocat de instituțiile participante într-o manieră transparentă și audiabilă.
- Generarea de dovezi cu privire la beneficiile blockchain și a contractelor inteligente pentru a îmbunătăți transparența în ceea ce privește licitațiile pentru achiziții publice care privesc instituțiile participante în proiectul pilot

Obiectivele operaționale

Obiectivele operaționale urmărite prin adoptarea unei soluții bazate pe tehnologia blockchain pentru auditarea și asigurarea integrității sistemului de bugetare participativă, alocare bugetară și achiziții publice:

- Asigurarea unei infrastructuri tehnologice și organizaționale la nivelul administrației centrale și locale.
- Asigurarea unei infrastructuri tehnologice și organizaționale la nivel de minister.
- Asigurarea unei infrastructuri tehnologice și organizaționale pentru publicul larg.
- Asigurarea interoperabilității cu între instituțiile publice.

Părțile interesate

Obiectivele operaționale urmărite prin adoptarea unei soluții bazate pe tehnologia blockchain pentru auditarea și asigurarea integrității sistemului de bugetare participativă, alocare

bugetară și achiziții publice pot fi clasificate în două mari categorii: beneficiarii, respectiv utilizatorii soluției dezvoltate.

- Proiectarea și implementarea de tip multi-stakeholder: Dezvoltarea și rezultatele soluțiilor vor fi îmbunătățite dacă părțile interesate relevante contribuie la proiectare sau implementare. Printre aceștia se numără funcționarii publici din instituțiile de achiziții publice și agențiile de ofertare, cetățenii afectați în mod direct, vânzători, avocați, funcționarii guvernamentali relevanți, inginerii în tehnologie și alții. Poate fi recomandabil să se construiască o "matrice a părților interesate" sau o hartă a universului contribuitorilor relevanți.
- În special, alinierea și implicarea părților interesate trans sectoriale, inclusiv a liderilor din industrie și din guvern, sunt esențiale pentru succesul proiectului. Rezistența la schimbare și interesele ilegite pot reprezenta o provocare pentru dezvoltarea proiectului; acolo unde este posibil, implicarea timpurie și frecventă și comunicarea clară a obiectivelor proiectului pot contribui la cultivarea buy-in-ului între acești actori.
- Cercetări privind principalele condiții de corupție în domeniul achizițiilor publice: Cercetarea surselor și modelelor de corupție vor oferi informații valoroase cu privire la conceperea soluțiilor. Alerte și funcționalități automate ar putea fi integrate într-un sistem pentru a detecta activitatea suspectă acolo unde apare cel mai frecvent.
- Instruire și ghiduri de utilizare: Ghidurile de utilizare sau manualele pot fi dezvoltate pentru a ghida diferitele tipuri de participanți (ofertanți, furnizori, cetățeni și alte monitoare) pentru a interacționa cu succes cu platforma de achiziții. Poate fi benefic să se desfășoare ateliere publice sau să se practice workshopuri pentru a învăța diferite părți interesate cum să folosească sistemul și să crească adopția. Sponsorul proiectului ar trebui să ia în considerare îndeaproape potențialele obstacole de participare pentru ofertant, furnizori și public, cu accent pe costuri, conștientizare, accesibilitate și utilizare.
- Strategia de comunicare publică: Ar trebui elaborată o strategie de gestionare a percepției și așteptărilor publicului legate de noul sistem de achiziții publice electronice. Poate cel mai important, ar trebui să fie clar că noua soluție nu este un "glonț de argint" pentru a pune capăt corupției. Rezultatele și obiectivele sistemului ar trebui să fie comunicate în mod clar, realiste și să le permită cetățenilor să înțeleagă atât potențialul, cât și limitările acestuia. De asemenea, poate fi oportun să se adapteze comunicarea pentru diferite categorii de public: este posibil ca anumite grupuri să aibă deja o înțelegere de bază a tehnologiei blockchain sau a procedurilor de achiziții publice, în timp ce altele nu.
- Primării - în funcție de abordarea preferată a monitorizării cetățenilor, mai multe strategii pot implica și educa publicul cu privire la oportunitatea de a ajuta la auditarea licitațiilor de achiziții publice. Birourile administrației locale pot găzdui în direct ședințe ale primăriei sau discuții publice sau pot oferi pamflete educaționale și materiale electronice. Răspândirea gradului de conștientizare a oportunității de a participa este esențială. De asemenea, poate fi util să se vizeze grupuri specifice de părți interesate.

Beneficiile estimate

Guvernarea digitală este paradigma ultimilor ani în administrația publică. Conceptul de e-guvernare a fost un catalizator al digitalizării și modernizării. Guvernarea digitală face un pas înainte și se concentrează pe furnizarea de servicii centrate pe utilizator, agile și inovatoare. Aceste servicii și modele de furnizare a serviciilor ar trebui să utilizeze tehnologia blockchain și mijloace de informare digitală pentru cetățeni. Blockchain este cu siguranță una dintre cele mai inovatoare tehnologii digitale care trebuie luate în considerare în cadrul elaborării politicilor guvernamentale și a furnizării de servicii. Principalele beneficii ale aplicării tehnologiei blockchain în e-bugetare ar fi:

- Reducerea costurilor economice, a timpului și a complexității schimburilor de informații interguvernamentale și publice care sporesc funcția administrativă
- Reducerea birocrăției, a puterii discreționare și a corupției, indusă de utilizarea registre distribuite și contracte inteligente programabile.
- Creșterea automatizării, transparenței, auditabilității și responsabilității informațiilor în registre guvernamentale în beneficiul cetățenilor.
- Creșterea încrederii cetățenilor și a mediului privat în procesele guvernamentale și ținerea evidenței determinată de utilizarea algoritmilor care nu mai sunt sub controlul exclusiv al guvernului.

Factori critici în asociere cu cazurile de utilizare

Factori critici privind cerințele tehnice:

- Necesitatea existenței unei rețele de servere, distribuite geografic;
- Probleme de scalabilitate;
- Capacitatea hardware mare necesară pentru a susține aplicații pe blockchain cu volum mare de tranzacții;
- Capacitatea de stocare mare, necesară pentru participarea la blockchain pe termen lung;
- Capacitate de rețea și procesare suplimentară pentru interfațarea aplicațiilor blockchain cu aplicațiile existente;
- Absența standardizării limbajelor de programare;
- Imaturitatea tehnologiei.

Factori critici de cost

- Costuri legate de mentenanță pe termen lung, pentru asigurarea disponibilității blocurilor mai vechi;
- Consum de energie mare necesar pentru efectuarea calculelor criptografice;
- Cost ridicat de implementare (costuri legate de echipamentele hardware și software);

- Costul schimbării infrastructurii actuale, costul de timp din cauza tranzacțiilor lente și costul de gestionare a datelor de dimensiuni mari
- Costuri legate de formarea și recrutarea personalului specializat.

Factori critici privind calitatea

- Acces la blocuri, conform arhitecturii și protocolului;
- Probleme de latență;
- Risc de atac cibernetic.

Factori critici privind ușurința execuției

- Lipsa de expertiză și cunoștințe tehnice. Este necesară pregătirea personalului pentru dezvoltare de aplicații back-end, front-end, respectiv a utilizatorilor.
- Menținerea fluxului de personal calificat.

Factori critici sub aspect economic (efecte colaterale negative, costuri de oportunitate)

- Asigurarea de fonduri pentru mentenanță hardware/software;
- Asigurarea de fonduri pentru instruirea personalului/utilizatorilor.

Factori critici sub aspect legal

- Lipsa unor reglementări și cadre legale adecvate în blockchain;
- Nu există o autoritate responsabilă pentru rezolvarea disputelor;
- Structurile juridice nu protejează în mod satisfăcător utilizatorii de cauza problemelor care pot să apară pe platforma blockchain.

Provocări tehnice în implementarea intervenției

- **Limitări de performanță & scalabilitate.** Una dintre problemele care apar cel mai des în cadrul sistemelor tehnice care folosesc tehnologia blockchain este performanța și viteza de procesare a operațiunilor (tranzacțiilor). Aceste caracteristici sunt strâns legate de tipul de blockchain ales și de mecanismele de consens ale acestuia, care pot face diferența în ceea ce privește viteza de procesare.
- **Interoperabilitatea tehnică cu alte sisteme naționale și ale instituțiilor.** Execuția bugetară implică activități complexe care trebuie bine corelate în privința schimbului de informații și de documente, inclusiv în relație cu sistemele naționale relevante cum este de exemplu platforma națională SEAP (Sistemul Electronic de Achiziții Publice)

Procese curente care ar putea fi afectate de dezvoltarea proiectului

Mai multe procese din contextul execuției bugetare și din ciclul de viață al activităților de achiziție publică sunt profund afectate pozitiv de o abordare care urmărește digitalizarea completă utilizând tehnologia blockchain.

Ne referim în primul rând la

- Auditul ex-post a procedurilor de achiziție publică și a achizițiilor directe pe baza logurilor detaliate de activitate (cine ce când a luat o decizie, a introdus sau a modificat o informație)
- Raportarea și investigarea privind realizarea achizițiilor directe, inclusiv procesul de planificare cu toate fazele sale (de la identificarea și justificarea necesității de achiziție, la aprobarea și avizarea acesteia, la planificarea și alocarea valorii estimate), și a procesului de identificare a furnizorului
- Analiza și investigarea informațiilor privind atribuirea contractelor, asigurarea disponibilității complete a informațiilor privind atribuirile și asigurarea faptului că nici o informație nu poate fi șteasă sau modificată
- Evaluarea cantitativă a unor criterii de calificare în cazul procedurilor competitive se poate realiza și automat, în funcție de caz, folosind Smart Contracts dacă informațiile privind ofertele au fost stocate pe blockchain (de exemplu verificarea cifrei de afaceri sau a codurilor CAEN autorizate, etc)
- Derularea proceselor de consultare a pieței, care acum sunt în general slab documentate și puțin transparente, poate fi susținută de blockchain, răspunsurile furnizorilor din piață fiind stocate si disponibile pentru auditare ulterioară.

Obiectivele funcționale

Acest capitol listează obiectivele minime funcționale pentru o soluție de achiziții de succes bazată pe tehnologia blockchain și care evidențiază cele mai importante caracteristici și componente prioritare. De asemenea, listează caracteristici cu prioritate mai mică care ar sprijini implementarea îmbunătățită, împreună cu cerințele pentru echipa de dezvoltare software pentru a documenta și descrie anumite aspecte ale soluției, cum ar fi vectorii de atac și vulnerabilitățile.

- Interfața cu utilizatorul și accesibilitatea datelor pentru ca cetățenii să vizualizeze sau să monitorizeze procesele de licitație trecute sau prezente care se desfășoară prin intermediul sistemului de achiziții publice electronice bazat pe tehnologia blockchain (inclusiv toate ofertele licitate).
- Interfață cu utilizatorul sau funcționalitate pentru ca cetățenii să vizualizeze toate ofertele concurente dintr-o ofertă de licitație curentă sau anterioară care trece prin sistem pentru a evalua dacă a fost selectată cea mai competitivă ofertă.
- Funcționalitatea cetățenilor de a ridica alerte sau de a comenta comportamentul suspect atunci când monitorizează procesele actuale de licitație.

- Rezistența bazelor de date la manipulare (de exemplu, a ofertelor, a ofertelor de participare la licitație) și a evidenței licitațiilor inviolabile; include cenzurarea ofertelor și a ofertelor de participare la licitație.
- Confidențialitatea ofertelor de ofertă pentru TOATE părțile până la încheierea perioadei de licitație pentru o procedură.
- Datele și fazele de deschidere/închidere automată și temporizată a licitației pentru comentariile publice.
- Auditabilitatea deciziilor de contractare directă, a modificărilor ofertelor de ofertă și a criteriilor de referință ale prețurilor.

Obiectivele de performanță

Caracteristicile de performanță tehnică ale soluției propuse derivă din beneficiile rezultate din adoptarea unei soluții bazate pe blockchain și sunt următoarele:

- **Asigurarea imutabilității și integrității datelor dintr-un sistem informatic**
 - Soluția trebuie să asigure imutabilitatea și integritatea datelor care vor fi stocate în registru și să permită reconstrucția acestora în cazul în care datele au fost modificate de surse externe neautorizate (acces direct la baza de date sau atac cibernetic).
 - Soluția trebuie să permită stocarea criptată a datelor în registrul imutabil de blocuri și tranzacții.
- **Partajarea securizată a datelor**
 - Partajarea securizată de date, cu posibilitatea de a oferi drept de proprietate pe date oricărui utilizator de sistem care are posibilitatea de a înregistra o tranzacție.
 - Acordare de acces implicit la date altor utilizatori, în baza unor cereri de acces specifice.
 - Expunerea de API-uri pentru a permite altor sisteme să înregistreze tranzacții, să integreze soluția de back-up în timp real și să ofere uneltele necesare care preiau automat datele din sistemul de stocare cărui i se aplica soluția de back-up.
 - Interogarea registrului imutabil de tranzacții în blocurile de date, prin interfețe grafice și API.
 - Posibilitatea de a defini structuri de date personalizate care pot acomoda datele protejate indiferent de structura acestora.
 - Definirea de alerte în cazul modificărilor de date în anumite structuri predefinite.
 - Posibilitatea de a configura politicile de sincronizare datele stocate în sistemul de back-up în așa fel încât, la cerere, anumite structuri să nu fie stocate decât pe anumite noduri în funcție de scop, nevoie și grad de securitate.
- **Mecanismele de stocare de date într-un mediu distribuit, securizat și transparent**

- Mecanism care preia în vederea protejării orice tip de date din baze de date tradiționale într-un sistem de stocare distribuit, transparente și imuabil.
- Stocarea datelor protejate integral în motorul de bază de date și a meta datelor (referințe, amprente digitale etc) într-un registrul imutabil.
- Salvarea datelor și în registrul imutabil, nu doar în baza de date, atât în forma clară cât și în formă criptată.
- Replicarea datelor stocate pe toate nodurile distribuite din rețea, atât datele din registrul imutabil cât și datele din baza de date.
- Stocarea versiunilor anterioare a unei înregistrări modificate în sistemul de gestiune a bazei de date a soluției software.
- **Distribuția datelor pe noduri în rețea**
 - Crearea de mai multe noduri într-o rețea distribuită, cu posibilitatea de a adăuga/configura și alte noduri ulterior livrării inițiale.
 - Fiecare nod participant la rețeaua peer-to-peer, în formula inițială, trebuie să fie o replică integrală a celorlalte noduri, și să conțină atât registrul imutabil de date cât și datele stocate în baza de date în vederea asigurării disponibilității și reconstrucției informației.
 - Posibilitatea de a adăuga noduri în rețeaua distribuită, noduri care stochează datele în motoare de baze de date diferite. Posibilitatea de a avea 2 noduri, fiecare cu alt sistem de stocare, va deservi mai eficient datele protejate unei soluții software în funcție de scop. (Ex: Un nod cu baze de date NoSQL va deservi mai bine datele unui sistem de căutare de date, pe când un nod cu o baza de date SQL se va preta mult mai bine unui sistem de analiza de date și raportare).
 - Fiecare nod trebuie să conțină/integreze cel puțin următoarele componente: registrul distribuit, baza de date, interfața API și componentele de securitate.
- **Reconstrucția în timp real datelor alterate**
 - Verificarea integrității datelor salvate, la fiecare operațiune de extragere (citire) a datelor din sistem.
 - Reconstrucția unei înregistrări salvate inițial, odată ce aceasta a fost identificată ca modificată pe rute neconforme (direct în baza de date sau atac informatic). Reconstrucția datelor trebuie făcută în baza nodurilor în care informația nu a fost modificată.
 - Reconstrucția și integritatea datelor trebuie să fie disponibile și pentru informațiile stocate criptat în sistem.
- **Proprietatea datelor**
 - Stocarea datelor în sistem cu indicatorul de proprietate, fiecare utilizator fiind unicul proprietar al informațiilor înregistrate.
 - Selectarea vizibilității datelor introduse în sistem: datele putând fi salvate cu indicatorul public (accesibil tuturor) sau cu indicatorul protejat (accesibil altor

utilizatori doar în baza unei cereri de acces care sa se aprobe de către proprietarul datelor).

- Mecanismul de proprietate a datelor trebuie să poată fi invocat și la criptarea datelor, în așa fel încât datele configurate a fi salvate criptat sa fie anonimizate folosind cheia secretă a utilizatorului.
- Utilizatorii au interfețe API pentru a verifica gradul de vizibilitate, pentru a cere și a obține permisiunea de acces la date.

Categoria metricului de performanță	Definiție	KPI
Gradul de transparență	Capacitatea cetățenilor, a întreprinderilor, a funcționarilor publici și a societății civile de a obține informații materiale despre procesul de selecție a furnizorilor în cadrul licitației de achiziții publice. Aceasta include atât transparența materială, cât și cea procedurală.	- Actualitatea informațiilor publicate - Relevanța și calitatea informațiilor publicate - Cantitatea de informații publicate - Ușurința de căutare și gradul de utilizare pentru public
Gradul de responsabilitate	Capacitatea cetățenilor, a întreprinderilor, a societății civile și a altor părți interesate de a verifica, echilibra și supraveghea procesul de achiziții publice. Aceasta include atât responsabilitatea orizontală (internă/guvernamentală), cât și pe cea verticală (neguvernamentală).	- Accesibilitatea platformei - Cantitatea de trafic de pe site-ul web terță parte - Numărul de observații ale utilizatorilor finali (de exemplu, reclamații) prezentate
Prevenție și echitate	Prevenție: Reducerea oportunităților pentru corupție. Aceasta include factori care minimizează procesul decizional monopolizat și discreționar. Corectitudine: Un proces de achiziții bazat pe calificările furnizorilor, merit și concurență onestă	- Valoarea ofertei câștigătoare - Numărul de furnizori implicați - Numărul de oferte depuse - Numărul de interacțiuni public-privat în persoană

Cost, grad de utilizare, funcționalitate, securitate și alte măsuri de performanță	Gradul de utilizare, eficacitatea și eficiența platformei de achiziții blockchain în general.	- Timpul necesar pentru procesul de licitație (de la publicarea proiectului de ofertă de participare la declararea ofertantului câștigător) - Costurilor - Securitatea platformei - Satisfacție față de infrastructura tehnică - Bariere de reglementare - Ușurința de formare și utilizare
--	---	--

Elementele de noutate

Factorii negativi care se pot diminua și elimina în totalitate sunt următorii:

- Majoritatea soluțiilor bazate pe tehnologia inovatoare sunt fabricate la comandă și ar putea necesita investiții inițiale mari.
- Structurile de date moștenite de întreprindere au de obicei un punct central de vulnerabilitate și un atac poate compromite întregul sistem.
- Politicile privind datele trebuie să respecte atât reglementările specifice industriei, cât și legislația generală privind protecția vieții private (de exemplu, GDPR).
- Instituțiile pot întâmpina dificultăți în partajarea datelor pe plan intern și extern, din cauza limitărilor tehnice sau a preocupărilor legate de riscurile potențiale.

Lista de elemente tehnice adiționale cu valoare adăugată pentru acest proiect este următoarea:

- Propunem construirea un mediu blockchain sigur și stabil, economisind costurile operaționale și de întreținere și accelerarea dezvoltării sistemului, eliminând în același timp decalajul de expertiză blockchain.
- Infrastructură agnostică - Conversia unui set complex date dezagregate într-un singur sistem de baze de date stabil fără a solicita proprietarilor de date modificarea sistemelor curente sau partajarea bazei de date către terți neautorizați.

Acces la citire: Fără permisiune (cu confidențialitate a ofertei sisteme, dacă este cazul)

- Toate informațiile privind tranzacțiile și licitația sunt publice (Blockchain Explorer), permiterea înregistrărilor publice să capete un caracter permanente și de a fi monitorizate în timp real.

- Toate ofertele de licitație pot fi vizualizate public începând cu anunțarea licitației în, ele ne fiind niciodată criptate în baza de date și fiind puse la dispoziție pentru acces public imediat.
- Toate ofertele furnizorului sunt publice, dar criptate pentru toate părțile din momentul depunerii până după încheierea perioadei de licitare în care pot fi decriptate. După ce ofertantul încheie fiecare rundă de evaluare a ofertelor, informația devine publică și toate informațiile despre ofertă se dezvăluie în timpul acelei runde de evaluare.
- Deciziile de ofertare și evaluările ofertantului sunt întotdeauna vizibile public și vor rămâne permanent înregistrate de îndată ce deciziile sunt încheiate. Publicul poate comenta deciziile și evaluările în perioadele pre-specificate în procesul de achiziții publice.

Acces la scriere: Fără permisiune (cu excepția participarea cu permisiune a furnizorului)

- Accesul la scrierea publică permite cetățenilor, jurnaliștilor și alte părți care monitorizează procesul de licitație, să comenteze în cadrul sistemului și să ridice alerte cu privire la comportament suspect și potențial corupt de către ofertant sau părți la licitație. Publicul poate face comentarii și reclamații în cadrul sistemului în timpul perioadei prestabilite pentru comentarii publice.
- Trimiterea ofertei furnizorului este parțial "permisă" în platformă. Oricine poate trimite oferte, dar numai oferte din preînregistrări oficiale conturi - care primesc o frază de acces secretă la înregistrare - sunt revizuite. Toate aceste oferte sunt documentate, iar ofertantul nu este în măsură să șteargă sau "cenzura" ei.
- Capacitatea unei instituții de a organiza o licitație în cadrul soluției blockchain este, de asemenea cu "permisiune": ofertanții care lansează și conduc licitațiile din sistem trebuie să fie aprobate în prealabil de către agenția de ofertare.

Criteriile de selecție

Criteriile de selecție care stau la baza deciziei alegerii platformei blockchain cea mai potrivită pentru a fi folosită în implementarea unei soluții adecvate:

- **Interfață de utilizator clară și utilizare facilă:** Ușurința de utilizare pentru toate părțile relevante ar trebui să fie o prioritate de top pentru a maximiza participarea. Interfața cu utilizatorul și proiectarea experienței utilizatorului ar trebui să includă testarea de către publicul larg, cu un accent puternic pe accesibilitatea cognitivă și tehnică.
- **Evaluarea compromisurilor tehnice:** În faza de cercetare și proiectare a soluției, compromisurile și preferințele ar trebui evaluate și determinate pe baza ofertanților necesari anumite blocajele tehnice care pot apărea în timpul fazei de tranziție. În timpul tranziției, noul sistem de achiziții publice electronice se poate integra cu orice sistem existent de achiziții publice electronice și poate funcționa în paralel pentru a găzdui utilizatorii care nu sunt încă pregătiți pentru noul sistem și pentru a reduce riscurile în cazul unei defecțiuni sau al unei defecțiuni a noului

sistem. Toate documentele relevante pot fi publicate atât în sistemele de revizuire publică, cât și în gestionarea redundantă a datelor.

- În plus, **noua soluție ar trebui să susțină un set limitat de licitații**, începând cu achiziții mici de bunuri comune sau standardizate. Trecerea completă la noul sistem poate avea loc atunci când soluția gestionează cu succes achizițiile complexe de achiziții, servicii și lucrări publice. Concentrarea în primul rând asupra achiziționării de bunuri similare ar sprijini, de asemenea, măsurarea performanței printr-o mai bună comparabilitate între rezultatele vechi și cele noi.
- **Analiza vectorilor de atac cibernetic și a vulnerabilităților:** Orice implementare la nivel de producție a unui sistem de achiziții publice electronice bazat pe blockchain ar trebui să cerceteze, să evalueze și să prezică cu atenție întreaga gamă de vulnerabilități. Dacă este posibil, aceste vulnerabilități ar trebui abordate înainte de implementare. Este important ca întreaga infrastructură a sistemului să fie evaluată pentru vulnerabilități, inclusiv interfețe de programare a aplicațiilor (API), browsere și funcționalități de stocare a datelor. Poate fi benefic să se evite utilizarea API-urilor din cauza centralizării și vulnerabilității lor la atacuri care ar putea compromite sistemul. Orice funcționalități dependente de intermediari, oameni sau funcții centralizate ar trebui evaluate pentru potențiale disfuncționalități, defecțiuni umane sau intervenții nejustificate.
- **Audit și revizuire a securității:** Este recomandabil să se efectueze un audit de securitate și o revizuire terță parte pentru orice nou sistem de achiziții electronice bazat pe tehnologia blockchain pentru a înțelege mai bine riscurile și a identifica erorile și vulnerabilitățile software-ului. Pentru orice implementare la nivel de producție, un audit de securitate profesionist și independent este probabil esențial pentru a reduce riscurile.
- **Selectarea unei rețele blockchain:** odată ce se determină accesul la citire, scriere și participare la consens, poate fi selectat protocolul blockchain care susține noua soluție de achiziții publice. Este important de selectat un protocol cu o securitate foarte mare a rețelei. Rețeaua ar trebui să aibă, de asemenea, un ecosistem de dezvoltare tehnică și de sprijin. De asemenea, este benefic dacă contribuitorii lucrează continuu la îmbunătățirea rețelei - de la remedierea problemelor software la implementarea upgrade-urilor și îmbunătățirea scalabilității. Rețeaua blockchain Ethereum are în prezent cea mai mare rată de hash a rețelei, un parametru cheie de securitate și cel mai mare ecosistem de validare a nodurilor și a contribuitorilor tehnici ai oricărei rețele blockchain inteligente care poate fi contractată; cu toate acestea, rețelele alternative cu securitate ridicată și ecosisteme tehnice robuste pot fi, de asemenea, adecvate. Mainnet-ul unei rețele este, de asemenea, puternic preferat, toate celelalte egale, din cauza securității sale mai mari a rețelei în raport cu o rețea de testare sau a mediilor "testnet", care de obicei au mai puține noduri validatoare și, prin urmare, sunt mai vulnerabile la atacurile contradictorii care pot compromite înregistrările și tranzacțiile din rețea. Testnets pot fi, de asemenea, închise sau resetate, punând în pericol o aplicație și înregistrările sale.

Descrierea în detaliu a cazului de referință

Pandemia de COVID-19 din 2020 este un exemplu de urgență publică care poate necesita contractarea directă pentru a achiziționa rapid bunurile și serviciile necesare. OCP a publicat recent recomandări pentru achiziții de urgență pentru COVID-19. Țări precum Columbia, au publicat rapoarte publice în conformitate cu aceste recomandări. În plus, Transparency International a publicat orientări din 13 capitole din America Latină care prezintă elementele minime pe care guvernele trebuie să le ia în considerare pentru a sprijini integritatea în contractarea publică în timpul situațiilor de urgență, cum ar fi pandemia de COVID-19. Capitolele îndeamnă în continuare la următoarele stenograme cele mai bune practici pentru achizițiile publice, în special în perioade de urgență sanitară:

- Activarea agențiilor naționale anti-monopol pentru a evita coluziunea între actorii economici sau practicile care duc la speculații de prețuri.
- Activarea auditurilor în timp real pentru procesele de achiziții publice, tocmai din cauza naturii excepționale a situației și a amplitudinii situației de urgență.
- Furnizați toate informațiile relevante privind achizițiile publice pe o singură platformă sau identificați o platformă pe care pot fi stocate aceste informații.
- Asigurarea responsabilității adecvate în timpul răspunsului în caz de urgență.

Opțiuni de îmbunătățire

Pentru a rezolva provocările legate de scalabilitate, soluția ar putea fi necesară pentru a utiliza una dintre următoarele arhitecturi:

- O implementare blockchain privat.
- O implementare "hibridă" cu două rețele blockchain la nivel de protocol: o rețea blockchain cu permisiune poate permite o rată de transfer mai mare a tranzacțiilor în timp ce un protocol fără permisiune este utilizat pentru păstrarea înregistrărilor falsificate.
- O nouă implementare la nivel de protocol de ultimă generație, cu debit avansat (de exemplu, Ethereum 2.0 pentru Ethereum rețea fără permisiune).
- O soluție de scalabilitate "strat 2" pe lângă un protocol blockchain fără permisiune, cum ar fi "canalele de stat" pentru Ethereum. Cercetarea pentru majoritatea implementărilor la nivel de protocol de generație următoare și a rețelelor "de nivel 2" este încă în curs de desfășurare și nu este pregătită pentru implementări la nivel de producție.

Pentru a răspunde provocărilor legate de stocarea datelor, fișierele de date pot fi stocate într-un sistem specializat descentralizat de stocare a fișierelor conectat cu rețeaua blockchain. Un exemplu este IPFS, un sistem de stocare distribuită a fișierelor de top compatibil cu rețeaua blockchain Ethereum. Se poate folosi o soluție care utilizează IPFS pentru a stoca, într-o manieră descentralizată, informațiile de licitație transmise de ofertant, o copie criptată a fiecărei oferte de ofertă depusă de la furnizori și o copie decriptată a fiecărei oferte de ofertă eligibilă după încheierea perioadei de licitație.

De asemenea, **este recomandabil să se stocheze fișiere de date "de rezervă" într-un sistem centralizat**. Dacă este posibil, acest sistem ar trebui să aibă elemente de rezistență la manipulare frauduloasă sau de inviolabilă. Stocarea fișierelor de rezervă reduce riscurile asociate cu rețelele blockchain care ar putea apărea în viitor. De exemplu, este posibil ca participarea la rețea să scadă dramatic în timp și să reducă securitatea înregistrărilor în acest sistem. În acest caz, ar putea fi fezabil ca înregistrările anterioare să fie afectate. Atunci când este necesar (adică în timpul fazei de evaluare a ofertelor), documentele, cum ar fi ofertele de ofertă, ar trebui să fie stocate într-o stare criptată.

Analiza comparativă

Blockchain public, fără permisiune	Blockchain public, cu permisiune	Hibrid: blockchain public, fără permisiune și cu permisiune	Consideratii
Anonimat			
Finanțarea conturilor furnizorului pentru taxele de tranzacție necesare (pentru a trimite cerere de oferta)	Problemă rezolvată	Problema poate fi abordată, în funcție de proiectare și implementare	Tehnicile moderne de criptografie (zero-knowledge-proofs pot aborda probabil problema
Trimiterea cererilor de oferta din conturile furnizorului	Problema poate fi abordată, în funcție de proiectare și implementare	Problema poate fi abordată, în funcție de proiectare și implementare	Primitivele criptografice, cum ar fi schemele de angajament sau construcțiile, cum ar fi zero-knowledge-proofs, pot aborda problema
Utilizarea criptomonedelor în comisioanele de tranzacție			
Potențiale blocaje juridice sau de reglementare	Problemă rezolvată	Problema poate fi abordată, în funcție de proiectare și implementare	

Eventuala necesitate de a instrui furnizorii și ofertanții cu privire la utilizarea criptomonedelor	Problemă rezolvată	Problema poate fi abordată, în funcție de proiectare și implementare	
Spam-ul și drenarea atacurilor			
Eliminarea comentariilor legitime cu numeroase comentarii frauduloase sau cu valoare scăzută	Problemă potențial sporită	Problemă potențial sporită	
Defăimarea permanentă a vânzătorilor onești (în comentarii)	Problema depinde de algoritmul de consens și de normele de guvernare a rețelei	Problema depinde de algoritmul de consens și de normele de guvernare a rețelei	Capacitatea de a afecta comentariile poate introduce mai multă corupție și trebuie să fie bine concepută
Întreruperi de sistem din cauza atacurilor de drenare a conturilor de finanțare a comisioanelor de tranzacție menite să finanțeze ofertele furnizorilor și comentariile publice	Problemă rezolvată	Problemă rezolvată	
Altele			
Scalabilitate redusă a tranzacțiilor	Problemă rezolvată	Problemă rezolvată (pentru tranzacțiile din blockchain-ul cu permisiune)	Problema depinde de numărul de noduri și de algoritmul de consens. Inovarea tehnologică poate aborda problema în viitor (de exemplu, "stratul 2" sau protocoalele de generație următoare, cum ar fi Ethereum 2.0)
Dificultate în implementarea deciziilor de guvernare la nivel de protocol sau a	Problemă rezolvată	Problemă rezolvată (pentru tranzacțiile din blockchain-ul cu permisiune)	

remedierilor de securitate			
Nota	Introduce o mai evidență mai slabă și securitatea și integritatea proceselor	Poate oferi o evidență puternică și securitate și integritate a proceselor, în funcție de implementare	Desemnarea nodurilor de înaltă încredere în sistemul de consens cu permisiune poate ajuta la menținerea integrității înregistrărilor și a proceselor

Constrângeri privind implementarea

1. **O înțelegere a constrângerilor și motivațiilor utilizatorilor:** factorii de decizie politică ar trebui să ia în considerare constrângerile pe care cetățenii le-ar putea avea legate de monitorizarea achizițiilor publice electronice. Publicul trebuie să aibă o conectivitate adecvată la internet, alfabetizare digitală și acces la computere sau smartphone-uri pentru a participa la sistem. Factorii de decizie politică ar trebui, de asemenea, să identifice motivațiile pentru ca cetățenii să participe la monitorizarea licitațiilor și, după caz, să încerce să activeze aceste motivații.
2. **Stimulente și motivații pentru furnizori și ofertanți:** În general, poate fi dificil pentru jurisdicții să stimuleze sau să oblige utilizarea de noi programe informatice de achiziții electronice atât pentru furnizori, cât și pentru ofertanți, dacă acest lucru nu este necesar din punct de vedere legal. Înainte de implementarea tehnologiei ar trebui să se țină seama de provocările legate de stimularea furnizorilor sau ofertanților să participe la sistem.
3. **Scalabilitatea blockchain:** În viitor, dacă soluția software încearcă să se extindă la mai multe jurisdicții cu volume mai mari de tranzacții, debitul de rețea într-o rețea blockchain publică, fără permisiune, cum ar fi Ethereum, ar putea fi prohibitiv.
4. **Stocarea fișierelor și a documentelor:** Stocarea datelor în rețele blockchain publice, fără permisiune, cum ar fi Ethereum, este în mod inerent costisitoare, deoarece datele sunt stocate și reproduse permanent pe miile de noduri din rețea.

Resurse tehnice pentru implementare

Structură tabulară

NUME	CLASIFICARE	TIP	ROL
auth01	Node	Fizic	BCDB Auth 1
auth02	Node	Fizic	BCDB Auth 2
auth03	Node	Fizic	BCDB Auth 3
data01	Node	Fizic	BCDB Data 1
data02	Node	Fizic	BCDB Data 2
data03	Node	Fizic	BCDB Data 3
http01	entrypoint	Fizic	Acces servicii web
http02	entrypoint	Fizic	Acces servicii web
firewall01	firewall	Fizic	Load Balancer / VPN / Firewall
firewall02	firewall	Fizic	Load Balancer / VPN / Firewall

Detalii tehnice

HOSTNAME	auth01, auth02, auth03
ROLE	Nod de autorizare din rețeaua BCDB
PROCESOR	4 core-uri
HDD Size	Min 500 GB, recomandat tip SSD
RAM SIZE	16 GB

HOSTNAME	data01, data02, data03
ROLE	Nod de date din rețeaua BCDB
PROCESOR	4 core-uri
HDD Size	Min 500 GB, recomandat tip SSD
RAM SIZE	16 GB

HOSTNAME	firewall01, firewall02
ROLE	Se ocupă de firewall, de balansare de sarcina și de vpn
HARDWARE	FortiGate 100F

HOSTNAME	http01 si http02
ROLE	Gateway (servere HTTP) pentru access
PROCESOR	2 core-uri
HDD Size	Min 200 GB, recomandat tip SSD
RAM SIZE	8 GB

Resurse umane pentru implementare

Expert	Responsabilitățile expertului
Manager de proiect	- Coordonarea eficientă a tuturor activităților proiectului în vederea atingerii obiectivelor stabilite la cele mai înalte standarde de calitate. - Pregătirea și organizarea planurilor de activitate în cadrul proiectului și asigurarea resurselor necesare pentru atingerea obiectivelor proiectului.

	• Asigurarea comunicării cu Autoritatea Contractantă și respectarea obligațiilor contractuale. • Întocmește, împreună cu Autoritatea Contractantă, planul de execuție a unui proiect. • Monitorizează activitățile în vederea contabilizării modului de execuție și determinării eventualelor întârzieri. • Coordonează activitățile din cadrul proiectului supervizând direct echipele tehnice și echipe partenere (daca e cazul). • Monitorizează în timp progresul atins față de obiectivele propuse și redactează rapoarte lunare către Autoritatea Contractantă și parteneri (daca e cazul) cu respectarea datelor prevăzute în contracte. • Asigură circulația informației în cadrul proiectului organizând periodic întâlniri cu echipa Autorității Contractante. • Asigură rezolvarea problemelor apărute în realizarea proiectului și informează la timp Autoritatea Contractantă despre problemele apărute. • Face propuneri de îmbunătățire pentru a maximiza eficiența atingerii obiectivelor propuse. • Întreține taskurile și activitățile într-un sistem de Project Management.
Expert blockchain	• Cercetează, evaluează și propune implementarea soluțiilor blockchain în proiecte software noi sau existente. • Cercetează evoluțiile tehnologice și comerciale în domeniul blockchain, identifică oportunități strategice și face propuneri relevante pentru proiectele interne. • Propune soluții tehnologice pentru integrare și adopția tehnologiei blockchain în proiectele software noi sau existente. • Supervizează, coordonează și oferă suport de-a lungul întregului ciclu de dezvoltare a proiectelor cu componente blockchain (colectarea cerințelor, design, scriere cod, testare, deployment, documentație etc.). • Participă la elaborarea și documentarea cerințelor funcționale și arhitecturii tehnice soluțiilor blockchain ale proiectelor, aprobă forma finală și intervine cu actualizări unde este cazul. • Lucrează direct cu dezvoltatorii blockchain externi/interni, verifică și aprobă livrabilele. • Testează funcționalități și raportează defecte de dezvoltare pentru a asigura calitatea livrabilelor. • Urmărește evoluția și performanța soluțiilor blockchain și propune modificări/optimizări acolo unde este necesară. • Raportează progresul și rezultatele soluțiilor blockchain către superiori și către echipele tehnice relevante la nivel intern.

	• Elaborează proceduri pentru mentenanța și remedierea defectelor soluțiilor de blockchain.
Frontend Developer	• Dezvoltare produse software și întocmire documentație aferentă procesului de dezvoltare. • Dezvoltă și întreține aplicații software și baze de date. • Scrie programe software (cod sursă) conform caietelor de sarcini / specificații și a documentelor tehnice. • Scrie testele unitare pentru codul sursă creat. • Remediază bug-uri și erori din codul sursă al produselor software. • Optimizează cod sursă. • Revizuieste cod sursă. • Proiectează scheme logice și diagrame pentru structurarea cerințelor proiectului în secvențe logice. • Elaborează module de cod în limbaje de programare folosind medii de dezvoltare integrate. • Configurează aplicațiile necesare, testează aplicațiile și modifică programele. • Proiectează și modifică structura bazelor de date prin codarea descrierii datelor folosind sisteme de gestiune a bazelor de date. • Colectează, structurează și analizează informațiile. • Întocmește rapoarte tehnice. • Asigură accesul celorlalți membri ai echipei la informațiile colectate; • Asigură buna funcționare a programelor dezvoltate prin respectarea procedurilor legate de protecția împotriva atacurilor informatice.
Backend Developer	• Dezvoltare produse software și întocmire documentație aferentă procesului de dezvoltare. • Dezvoltă și întreține aplicații software și baze de date. • Scrie programe software (cod sursă) conform caietelor de sarcini / specificații și a documentelor tehnice. • Scrie testele unitare pentru codul sursă create. • Remediază bug-uri și erori din codul sursă al produselor software. • Optimizează cod sursă. • Revizuieste cod sursă. • Proiectează scheme logice și diagrame pentru structurarea cerințelor proiectului în secvențe logice. • Elaborează module de cod în limbaje de programare folosind medii de dezvoltare integrate. • Configurează aplicațiile necesare, testează aplicațiile și modifică programele. • Proiectează și modifică structura bazelor de date prin codarea descrierii datelor folosind sisteme de gestiune a bazelor de date.

	• Colectează, structurează și analizează informațiile. • Întocmește rapoarte tehnice. • Asigură accesul celorlalți membri ai echipei la informațiile colectate. • Asigură buna funcționare a programelor dezvoltate prin respectarea procedurilor legate de protecția împotriva atacurilor informatice.
--	--

Resurse financiare pentru implementare

În timpul fazei de proiectare, ar putea fi efectuată o analiză cost-beneficiu care să evalueze valoarea utilizării tehnologiei blockchain și diferitele sale configurații de permisiune în comparație cu procesele status quo sau soluțiile alternative de achiziții. Întreaga arhitectură software ar trebui evaluată. O astfel de analiză ar trebui să ia în considerare o varietate de costuri și beneficii economice, procedurale și sociale care pot fi suportate.

- Investiția în soluția software customizată de achiziții publice
- Investiția în licența de bază de date conectată cu un motor de blockchain
- Investiția în infrastructură și hardware
- Investiția în mentenanță și suport.

Componenta	Tip licențiere	Unitate	Cantitate	Preț unitate EUR	Total EUR
Soluția software	Dezvoltare custom	ora	10.000	100	1.000.000

Notă: Prețul, respectiv numărul de ore necesar dezvoltării formei finale a produsului, se bazează numai pe implementarea tuturor proceselor de colectare și analiză de risc ale instituției, respectiv pe extinderea aplicației cu funcționalități esențiale analizate pe durata derulării prezentului contract, nu și pentru alte eventuale procese nediscutate sau soluții software pe care Beneficiarul le-ar putea dori implementate.

Componenta	Tip licențiere	Unitate	Cantitate	Preț unitate EUR	Total EUR
Blockchain Database	Licență	Nod/An	12 noduri/5 ani • 7 noduri date • 5 noduri autorizare	42.000/nod/an	2.520.000

Notă: Prețurile exprimate sunt construite în baza unei analize generale de piață și pot fi luate în considerare cu titlu informativ și estimat. Aceste prețuri pot fi subiectul unor discounturi și se pot modifica în baza unor cerințe extra din partea Beneficiarului.

	On-Prem/Privat	Cloud Public
Nuclee CPU	150	308
RAM (GB)	3160	6340

Stocare (TB)	160	385
--------------	-----	-----

Infrastructura locală (on-prem) trebuie să susțină 30% din resursele rețelei Blockchain Database, iar restul de 70% vor fi găzduite pe infrastructura de cloud public. Resursele rămase pe cloud privat trebuie să poată acomoda orice nou proiect sau migrare de resurse din infrastructura curentă care trebuie să ruleze pe o infrastructură privată on-prem.

Cloud public

Descriere	Tip resursă	OS	Nuclee CPU	RAM	Stocare	Cantitate
BCDB Nodes	Virtual Machine	Ubuntu 18.04	10	40	12100	9
HTTP Server	Virtual Machine	Ubuntu 18.04	2	8	150	2
Prometheus/Grafana Monitoring	Virtual Machine	Ubuntu 18.04	2	16	1000	1

Cloud privat

Descriere	Tip resursă	OS	Nuclee CPU	RAM	Stocare	Cantitate
BCDB Nodes	Virtual Machine	Ubuntu 18.04	8	32	12000	4
HTTP Server	Virtual Machine	Ubuntu 18.04	2	8	150	1

Componente hardware local (On-prem/Privat)

Componentele hardware recomandate și scopul fiecăreia sunt detaliate în tabelul de mai jos. Componentele au fost selectate și configurate pentru a lucra cu Microsoft Azure stack.

ID	Denumire Componentă	Tip	Scop
1	HPE DL380 Gen10	Server	Monitoring Services
2	HPE DL380 Gen10	Server	Compute Nodes
3	HPE MSA 2062 Storage LFF or SFF with 4x 16Gbps FCE connectors and 80 TB	SAN Storage	SAN replicated storage for Infrastructure VM storage
4	HPE SN3600B 32Gb 24/8 Fibre Channel Switch 8 or more active ports license	SAN Switch	SAN switch for storage traffic between computers and Storage Servers

5	HPE FlexFabric 5710 24XGT 6QSFP+ 960Gbps	24x 10Gbps Switch	Internal connectivity, storage data flow, VLAN segmentation and LACP channeling - Independent Resilience
6	Fortigate 600E/601E	Security Gateway	Firewall (NGFW), Secure Web Gateway (SWG), Secure SD-WAN (Transport between zones) IPS, VPN, Content Processor, Load Balancer - HA System

Infrastructura a fost construită în așa fel încât să permită procesarea paralelă, iar dacă una dintr e încăperi (locații) este nefuncțională, să poată fi înlocuită de cealaltă.

Puterea de procesare a fost supra-alocată, iar în fiecare încăpere a fost configurat un server care rămâne inactiv până când un anumit prag este atins.

Nr. crt.	Denumire produs	Furnizor	Cod produs	U.M.	Cant.	PU €	TOTAL
Echipamente							
1	Infrastructura hiperconvergentă HPE certificată Microsoft Azure Stack și cuprinde: 2 clustere formate din 8 servere HP DL 380 G10, - câte 4 servere aflate în fiecare dintre cele 2 data-room-uri, care satisfac o nevoie de procesare totală de 150 de core-uri de procesor, 5 TB memorie RAM, 180 TB spațiu de stocare, cu scopul de a găzdui, fără servicii Microsoft Azure Stack - garanție 5 ani, servicii suport 24/7, cu păstrarea discurilor defecte	HPE	0	set	1	234.747,74 EUR	234.747,74 EUR
2	Fortigate 600E care cuprinde: - Servicii de suport 24x7 FortiCare pe 3 ani - Servicii FortiGuard IPS pe 3 ani - Servicii FortiGuard Web Filtering pe 3 ani - Servicii SD-WAN Overlay Controller VPN pe 3 ani - Licența SD-WAN Orchestrator Entitlement pentru 3 ani	Veracomp / Fortinet	FG-600E	buc	4	31.656,02 EUR	126.624,07 EUR

3	Licențe Ms Server 2019 DataCenter OLP cu SA	ALEF	WinSvrDCCore 2019 SNGL OLP 2Lic NL CoreLic Qlfd	buc	1	133.235,20 EUR	133.235,20 EUR
4	Servicii instalare clustere HCI (2 data-centre), care includ: • Instalare si configurare fizică servere și switch-uri, cablare • Upgrade firmware servere și componente, configurare modul de management (4 servere) • Upgrade firmware switch-uri, configurare management (2 switch-uri) • Configurare redundanță switch-uri • Configurare politici de acces și securitate switch-uri • Instalare OS Windows Server 2019, drivere, roles & features, updates • Configurare opțiuni rețea: teaming, virtual switches, virtual ethernet adapters • Configurare cluster Storage Spaces Direct, definire volume • Configurare cluster Hyper-V nou • Configurare volume de tip CSV pe clusterul nou • Testare funcționalități soluție HCI (servere, Storage Spaces Direct, virtualizare) • Configurare replicare pentru Disaster recovery: Hyper-V Replica / Storage Replica • Configurare politici replicare date- Configurare politici de failover și failback- • Testare replicare, failover și failback- • Documentație și handover • Suport post implementare (tip garanție): 3 luni	Ecko Systems	Servicii instalare	buc	2	9.136,13 EUR	18.272,26 EUR
							512.879,28 EUR
Servicii							
1	Servicii asociate manoperei			set	1	1.115,38EUR	965,22 EUR
							965,22 EUR
						TOTAL OFERTA, EXCLUSIV TVA	513.844,49 EUR
						TVA 19%	97.630,45 EUR
						Total oferta inclusiv TVA	611.474,95 EUR

Resurse logistice pentru implementare

Utilizarea spațiilor de testare guvernamentale: acolo unde sunt disponibile, pot fi explorate "spații de testare" în materie de inovare pentru a urmări achizițiile publice electronice și experimentele tehnologice anticorupție într-un mod care nu trebuie să respecte reglementările care restricționează reglementările.

Riscuri și planuri de contingență

Principalele bariere care pot îngreuna sau opri implementarea actualei strategii sunt:

- Insuficiența înțelegere din partea decidenților privind impactul tehnologiei blockchain, a aplicabilității sale în sectorul public și trendurile la nivel european și internațional.
- Confuzia între blockchain ca tehnologie și criptomonede, în contextul unei piețe în expansiune a acestora. Aceasta este una dintre cele mai toxice asocieri, mai ales pentru instituții din zona financiar monetară și poate dăuna mult eforturilor de implementare a tehnologiei blockchain în zona serviciilor publice.
- Lipsa de capital politic, instabilitatea politica sau deturnarea narativului politic. Tehnologia blockchain necesită o înțelegere fină a complexităților sale, care este mult mai greu atins într-o perioadă de turbulențe politice. Un asemenea context ar putea focaliza atenția decidenților pe probleme mult mai ușor de translatat în mesaje către cetățeni.
- Insuficienta implicare a sectorului privat și a experților IT din sectorul privat. Instituțiile publice au încă un deficit de personal calificat, cu precădere în implementarea de soluții inovatoare precum tehnologia blockchain. Pentru a putea implementa cu succes această strategie este nevoie de utilizarea unor instrumente precum parteneriatul public-privat sau mecanismul parteneriatul pentru inovare.
- Resurse financiare – pentru ca ecosistemul să poată evolua corespunzător, este nevoie ca o mare parte dintre părțile interesate să aibă capacitatea financiară de a se angaja în proiecte majore.
- Capacitatea limitată de planificare și elaborare de proiecte, implementare, evaluare, care ar putea duce la blocaje în diferite stadii ale unor inițiative, în special dacă acestea implică mai mulți actori.
- Lipsa resursei umane specializate, atât în sectorul public cât și în cel privat.
- Capacitate administrativă – neclaritățile încă nerezolvate în legătură cu modul de organizare a instituțiilor naționale de digitalizare și a modului în care acestea

colaborează între ele și cu părți externe, ceea ce poate duce la existența unor proiecte ale căror coordonatori sunt greu de identificat, la dublarea sau suprapunerea unor eforturi între instituții sau la pierderea vizibilității asupra unor inițiative.

- Bariera legislativă - unele inițiative se pot bloca din cauza legislației neactualizate și neadaptate la noile realități tehnologice care nu permite dezvoltarea anumitor soluții sau forme de colaborare dintre entități sau cauzează neclaritate/incertitudine în aspecte importante ale unor proiecte.

Interacțiunea cu alte sisteme tehnice

Sistem agnoistic: Datorită și faptului că există mai mulți producători de motoare de blockchain, iar nevoile clienților/beneficiarilor se pot raporta și la acest lucru, soluția propusă se prezintă ca o platforma independenta de aceasta componenta. Asta înseamnă ca poate funcționa și cu HyperLedger Fabric (motor de blockchain), și cu Tendermint și cu oricare motor de blockchain își dorește beneficiarul aplicației. Soluția tehnica va fi distribuită beneficiarului cu o combinație de motor blockchain și motor baza de date la solicitarea acestuia, fiind la latitudinea dezvoltatorului sa creeze o diversitate cat mai mare de distribuții pentru a acoperi nevoile tuturor beneficiarilor.

Interoperabilitate: While most organizations are already engaged in a digitalization process, they do not all use the same software applications and databases. This usually means that it is difficult for them to share data automatically without significantly modifying existing software configurations. Blockchain technology can help build an ecosystem where data can be shared among several entities efficiently, securely, and transparently with the major benefit that that system participants will not be required to make major changes to their infrastructure, and will be able to continue to work with the same software applications and the same databases.

Diagrama pentru implementare

Activitate			Rezultat	An implementare										
				1	1,5	2	2,5	3	3,5	4	4,5	5-7	8	10
Pregătirea proiectului pilot și a procedurilor de evaluare/analiză	2 ani: Proiectare, dezvoltare, implementare back-end și front-end		Sistem prototip verificat (TRL4 [31, 32])											
	0,5 ani: Formare personal și testare beta	0,5 ani: Formare personal, training pe sistemul dezvoltat	Tehnologie validată în mediu relevant (TRL5)											

	0,5 ani: Testare beta de către utilizatori	Tehnologie demonstrată în mediu relevant (TRL6)																	
	1 an: „Smoke testing”, ucenic non-producție	Sistem model și prototip demonstrate în mediu operațional (TRL7)																	
	0,5 ani: Analiză comparativă rezultate sistem nou/sisteme existente de referință	Sistem complet și validat (TRL8)																	
	1 an: Optimizare/eliminare defecte raportate de utilizatori	Sistem validat în mediul operațional (TRL9)																	
Operaționalizarea sistemului de vot electronic de la distanță bazat pe blockchain pentru desfășurarea proiectului pilot în alegerile europarlamentare 2028	Desfășurarea proiectului pilot în cadrul alegerilor parlamentare din 2028	Cetățenii invitați să participe în proiectul pilot au posibilitatea de a- și exercita votul online, de la distanță, prin intermediul noului sistem.																	
	Analizarea și evaluarea rezultatelor pilotului	Concluzii despre posibila continuare a dezvoltării pentru adopția pe scară largă																	

Metodologia de management a proiectului și modelul de dezvoltare

- Identificarea problemelor și corelarea soluțiilor:** Înainte de a decide să implementeze tehnologia blockchain, instituțiile ar trebui să identifice problemele specifice din cadrul achizițiilor publice pe care încearcă să le abordeze și fezabilitatea tehnologiei blockchain pentru a contribui la rezolvarea acestor probleme.
- Un cadru puternic de operațiuni pentru dezvoltatori:** un cadru puternic de operațiuni pentru dezvoltatori ar aduce beneficii proiectului. Aceasta include politici bine definite de control al versiunilor și de control al calității.
- Raportare și evaluare periodică:** Echipa de dezvoltare sau de management a proiectului ar trebui să țină părțile interesate evaluate cu privire la progresele și provocările platformei prin actualizări periodice pe parcursul dezvoltării și implementării acesteia.

Echipa de proiect ar trebui, de asemenea, să evalueze performanța licitației odată implementată.

1. **Transparența proiectării soluțiilor:** Poate fi benefic să se asigure transparența în modul în care este concepută și programată soluția software, pentru a oferi înțelegere și încredere participanților și publicului. Codul software în sine ar putea fi, de asemenea, open-source, care poate permite monitoarelor cetățenești să evalueze corectitudinea software-ului sau să identifice orice prejudecăți sau vulnerabilități codificate. Tehnologia și datele cu sursă deschisă ar permite, de asemenea, ca soluția software să servească drept "bun public" digital și să fie adoptată, îmbunătățită și scalată de alte jurisdicții.

Precondiții și factori critici pentru succes

Componentele de politică și guvernare trebuie să fie însoțite de punerea în aplicare a tehnologiei blockchain pentru a-și maximiza potențialul de a îmbunătăți transparența și responsabilitatea în cadrul proceselor de achiziții publice. Această secțiune oferă o listă de factori critici pentru succes pe care guvernele ar trebui să le ia în considerare cu fermitate în ceea ce privește consolidarea integrității în domeniul achizițiilor publice electronice.

Întregul potențial anticorupție al oricărei noi platforme de achiziții publice electronice nu poate fi realizat în absența unui **cadru juridic clar, bazat pe cele mai bune practici internaționale și pe implicarea și supravegherea eficace a părților interesate**. În timp ce particularitățile fiecărei țări și ale contextului industrial fac imposibile propuneri de politici detaliate, există o serie de soluții de politici publice care pot completa și amplifica capacitatea anticorupție a unui sistem de achiziții publice electronice, indiferent dacă este bazat sau nu pe tehnologia blockchain.

1. **Eliminarea barierelor juridice:** Guvernul ar trebui să revizuiască legile care limitează utilizarea platformelor de achiziții publice electronice, cum ar fi cele care necesită interacțiuni în persoană între ofertant și furnizor sau care mandatează depunerea de oferte pe suport de hârtie.
2. **Mandatarea utilizării:** Guvernul ar trebui să mandateze utilizarea unei noi platforme de achiziții publice electronice, dacă este posibil, pentru a obliga schimbarea proceselor de achiziții în persoană și pentru a consolida toate tranzacțiile într-o singură bază de date sau sistem de înregistrare.
3. **Accesul facil la informații:** Toate aceste informații trebuie să fie gratuite și accesibile publicului. Taxele de acces și înregistrare nu ar trebui să existe, iar conținutul site-ului ar trebui să poată fi căutat și descărcat. Site-urile de achiziții electronice existente, cum ar fi contractele publice deschise în Slovacia și Monitorul licitațiilor din Georgia, oferă planuri pentru o astfel de platformă. Ambele site-uri web, dezvoltate de capitolele naționale ale Transparency International, exemplifică puterea datelor privind achizițiile publice, permițând utilizatorilor să caute semne cheie de corupție, cum ar fi câștigătorii frauduloși, licitațiile cu un singur ofertant și detaliile contractului de achiziții publice.

4. **Eliminarea restricțiilor arbitrare privind eligibilitatea contractelor:** Ca o considerație de bază, guvernele ar trebui să reducă la minimum restricțiile arbitrare sau inutile privind eligibilitatea contractelor. Aceasta include interdicții generale împotriva companiilor străine sau din afara statului și specificațiile contractuale excesiv de restrictive care blochează frecvent participarea tuturor, cu excepția unui singur furnizor.
5. **Sprijinirea furnizorilor mici și mijlocii:** Acolo unde este posibil, condițiile de licitație nu ar trebui să favorizeze producătorii și vânzătorii la scară mai mare. Desfășurarea licitațiilor la nivel de oraș sau județ, mai degrabă decât la nivel de țară. De asemenea, poate fi posibil să se sprijine furnizorii mai mici prin eforturi precum precalificarea licitației sau scutirea de la anumite cerințe privind anumite documente.

Indicatori pentru monitorizare și evaluare

Indicatori tehnici și de proces

- Toate activitățile realizate de către persoanele implicate în procesele de achiziție publică să fie stocate în blockchain pentru a se putea realiza auditul și investigarea completă (cine, ce, când)
- Toate informațiile privind ofertele, atribuirile, contractele să fie stocate în blockchain și disponibile pentru audit
- Sistemele naționale relevante (SEAP) să fie complet integrate cu sistemul de stocare bazat pe blockchain

Indicatori de impact

- Auditurile, raportările și investigațiile să se realizeze pe baza informațiilor stocate în blockchain
- Publicarea rezultatelor procedurilor, inclusiv sub formă de seturi de date deschise procesabile informatic să se realizeze pe baza informațiilor stocate în blockchain

Referințe bibliografice

1. https://ec.europa.eu/isa2/news/emerging-technologies-public-procurement-study-results_en/
2. Disruptive Technologies in Public Procurement, Banca Mondială
<https://documents.worldbank.org/en/publication/documents-reports/documentdetail/522181612428427520/disruptive-technologies-in-public-procurement>

3. <https://asia.nikkei.com/Politics-Economy/Policy-Politics/Japan-looks-to-blockchains-for-more-secure-e-government-systems>
4. <https://govmatters.tv/hhs-obtains-first-blockchain-ato-in-federal-government/>
5. <https://fcw.com/blogs/lectern/2017/10/comment-kelman-gsa-blockchain.aspx>
6. <https://www.eleconomista.com.mx/tecnologia/Gobierno-federal-realizara-el-primer-caso-real-de-licitacion-con-blockchain-en-agosto-20180727-0035.html>
7. https://newsis.com/view/?id=NISX20190116_0000531364&cID=10801&pID=14000
8. WEF_Blockchain_Government_Transparency_Report(weforum.org)
https://www3.weforum.org/docs/WEF_Blockchain_Government_Transparency_Report.pdf
9. https://www.transparency.org/files/content/corruptionqas/Topic_Guide_Codes_of_Conduct.pdf



Proiect:

Proiect selectat în cadrul Programului Operațional Capacitate Administrativă cofinanțat de Uniunea Europeană, din Fondul Social European

Axa Prioritară 1: Administrație publică și sistem judiciar eficiente

Obiectivul specific 1.1: Dezvoltarea și introducerea de sisteme și standarde comune în administrația publică ce optimizează procesele decizionale orientate către cetățeni și mediul de afaceri, în concordanță cu SCAP.

Titlul proiectului: „ Cadru strategic pentru adoptarea și utilizarea de tehnologii inovative în administrația publică 2021-2027 – soluții pentru eficientizarea activității”

COD: SIPOCA 704

Beneficiar: AUTORITATEA PENTRU DIGITALIZAREA ROMÂNIEI

Partener: UNIVERSITATEA TEHNICĂ DIN CLUJ - NAPOCA

Fundamentarea cazului de utilizare și studiu de evaluare ex-ante pentru Trasabilitatea tranzacțiilor comerciale (cu accent pe factura electronică – e-invoice și smart contracts)

Cuprins

Acronime și abrevieri	3
Scopul intervenției	4
Părțile interesate.....	7
Beneficiile estimate.....	9
Factori critici în asociere cu cazurile de utilizare	10
Provocări tehnice în implementarea intervenției.....	13
Procese curente care ar putea fi afectate de dezvoltarea proiectului	14
Obiectivele funcționale	14
Obiectivele de performanță.....	16
Elementele de noutate	16
Criteriile de selecție	17
Descrierea în detaliu a cazului de referință	18
Opțiuni de îmbunătățire	18
Analiza comparativă.....	18
Constrângeri privind implementarea.....	19
Resurse tehnice pentru implementare.....	19
Resurse umane pentru implementare.....	20
Resurse financiare pentru implementare	20
Resurse logistice pentru implementare.....	21
Riscuri și planuri de contingență.....	21
Interacțiunea cu alte sisteme tehnice	23
Diagrama pentru implementare	23
Metodologia de management a proiectului și modelul de dezvoltare	24
Precondiții și factori critici pentru succes	24
Indicatori pentru monitorizare și evaluare	24
Referințe bibliografice	24

Acronime și abrevieri

Abreviere sau acronim	Expresia completă	Explicație
ADR	Autoritatea pentru Digitalizarea României.	
AI	Inteligență Artificială	Provine de la termenul în engleză Artificial intelligence
ANAF	Agencia Națională de Administrație Fiscală	
B2G	Business to Government.	
B2B	Business to Business	
B2I / B2C	Business to Individual / Business to Consumer.	
CFE	chitanțe fiscale electronice.	
CNIF	Centrul Național pentru Informații Financiare.	
CUI	Cod Unic de Înregistrare.	
DeFi	Descentralizarea sistemului financiar	Provine din termenul englez Decentralized Finance
DGI	Direcția Generală a Impozitelor	
DTE	Documente Fiscale Electronice	
IT	Information technology.	
PEPPOL	Pan-European Public Procurement Online	Achiziții publice paneuropene online
OSN	Orbit Showtime Network	Rețeaua Orbit Showtime
UE	Uniunea Europeană.	
CTC	Continuous Transaction Controls	Formă de raportare sau validare bazată pe facturi sau pe componente ale facturilor.
SAF-T	fișierul standard de audit	Provine din engleză <i>Standard Audit File for Tax</i> .

Scopul intervenției

Definirea problemei

Un element esențial în asigurarea sustenabilității statului și a capacității de operare a instituțiilor publice este capacitatea de control și auditare a activității economice taxabile derulate pe teritoriul țării de către operatorii economici înregistrați, respectiv asigurarea capacității de colectare a taxelor și minimizarea fraudei economice.

În fiecare țară, evoluția formelor de raportare a activității operatorilor economici a fost strâns corelată cu dezvoltarea capacităților de trasabilitate și control exercitată de autoritatea centrală asupra proceselor economice. Acolo unde sistemul instituțional este încă slab dezvoltat, în multe țări în curs de dezvoltare, nivelul economiei informale rămâne foarte ridicat (de exemplu la valori de 70-80% în multe țări din Africa sub-sahariană), iar capacitatea de colectare a statului foarte redusă.

Evoluția tehnologiei, combinată cu dezvoltarea politicilor publice și a standardelor, permite țărilor dezvoltate, în particular a statelor membre din UE, un avans rapid de la forma tradițională de raportare fiscală până în 25 a lunii următoare, la raportarea electronică bazată pe fișierul standardizat de audit (ȘAF-T), și deja în tot mai multe țări la urmărirea în timp real a tranzacțiilor economice prin raportarea automată a facturilor în formatul electronic standard european EN 16931, publicat în noiembrie 2017 și transpus în standard român sub numărul SR EN 16931.

Următoarea etapă, în curs de implementare în mai multe state, este asigurarea controlului continuu al tranzacțiilor (CTC) care îmbină raportarea tranzacțiilor prin facturi electronice (sau un subset de date ale acestora) cu validarea existenței și corectitudinii tranzacției prin confirmarea destinatarului facturii (cumpărătorul), prin intermediul unui proces electronic auditabil.

Digitalizarea completă a întregului proces comercial între cumpărător și vânzător, incluzând raportarea către autoritatea fiscală, precum și mecanismul de validare, deschide posibilități suplimentare la care în trecut nici părțile implicate în tranzacție, nici instituțiile statului, nu aveau acces.

Aceste noi posibilități apar în relația dintre companii și stat, dar și în relația comercială B2B și B2C. Astfel, în relația dintre companii și autoritatea fiscală a statului, va putea fi urmărită în timp real balanța dintre facturile emise și facturile primite, cel puțin cele care sunt emise între părți care aparțin aceleiași jurisdicții fiscale, ceea ce determina ca sumele aferente taxei pe valoarea adăugată să poată fi monitorizate în timp real, pentru a evidenția sumele datorate de către operatorii economici către stat, respectiv sumele asupra cărora companiile au dreptul să primească rambursare. Aceasta monitorizare facilitează în mod fundamental creșterea colectării taxei pe valoare adăugată, respectiv rambursările atunci când este cazul. Automatizarea procesului de rambursare este o posibilitate de asemenea.

Prin monitorizarea și analiza continuă în timp real se reduce foarte mult riscul de fraudă de tip carusel, mecanism prin care o companie fictivă intermediar colectează TVA pe care nu îl mai remite statului.

Comisia Europeană a anunțat în 2021 intenția de a stabili un mecanism de urmărire și raportare în timp real a facturilor intracomunitare, prin conectarea sistemelor naționale pentru facturare electronică și centralizarea raportării pentru a putea bloca fraudă de tip carusel care începe cu o plată între un operator economic dintr-un stat membru către un intermediar fictiv din alt stat membru.

În relația comercială dintre companii (tranzacțiile B2B), introducerea controlului continuu al tranzacțiilor, incluzând validarea corectitudinii și validității facturilor de către cumpărător, permite extinderea pe scară largă a serviciilor de factoring și finanțare a facturilor de către terțe părți (operatori de factoring), cărora părțile implicate în tranzacție le permit accesul la informațiile relevante, astfel încât vânzătorul să poată beneficia de plata anticipată remisă de către operatorul de serviciu, iar cumpărătorul să realizeze plata facturii către operatorul de factoring.

Evoluțiile din perioada următoare la nivel european vor cuprinde acoperirea de către standardul european pentru facturare electronică a facturilor simplificate și a bonurilor ("receipt"), ceea ce va extinde posibilitățile de raportare și trasabilitate a tranzacțiilor B2C. Comitetul European de Standardizare (CEN) a lansat în ancheta către țările membre propunerea de model semantic aferent, elaborate de către Comitetul Tehnic 434 (prEN 16931-8, Electronic invoicing - Part 8: Semantic data model of the elements of an e-receipt or a simplified electronic invoice)

Dezvoltarea și lansarea în cursul anului 2021 a sistemului național pentru facturare electronică, proiect implementat de CNIF, aliniază România la obligațiile rezultate din Directiva Europeană 55/2014 privind facturarea electronică în achizițiile publice și deschide posibilitatea extinderii utilizării facturării electronice în relațiile B2B, pe lângă cele B2G impuse de directivă, respectiv permite implementarea mecanismelor de raportare directă a facturilor emise care conțin TVA și în perspectivă implementarea mecanismelor de validare aferente controlului continuu al tranzacțiilor (CTC).

În condițiile în care va crește numărul de operațiuni informatice de raportare, validare, notificare, iar stocarea și arhivarea facturilor poate fi mult ușurată prin adoptarea formatului standard european, introducerea tehnologiilor blockchain în relație cu urmărirea tranzacțiilor comerciale și a facturilor electronice se evidențiază ca oportunitate demnă de analiză.

Vom detalia și analiza în continuare modul în care acest lucru se poate realiza. Utilizările tehnologiei blockchain în relație cu facturarea electronică sunt încă în stadiul incipient, de experiment, sau de teoretizare. În lipsa unei standardizări a platformelor de transmisie, stocare și validare a facturilor și a implementării unor abordări arhitecturale diverse în țările care au adoptat facturarea electronică, discuțiile privind utilizarea blockchain în relația cu facturile nu implică neapărat o implementare tehnică controlată de către o autoritate centrală de stat. De exemplu, o abordare posibilă este stocarea facturilor ca atare într-un blockchain decentralizat, la care au acces diverse sisteme informatice care pot realiza verificări sau adaugă informație, cum ar fi de exemplu asocierea unui indicator care arată că factura a fost plătită. Pentru participanții la tranzacție este foarte relevantă posibilitatea de a verifica execuția tranzacției financiare, adică realizarea efectivă a plății, în relație cu o cerere de plată, transmisă sub forma

de factură, sau emiterea unei dovezi de plată ca bon („e-receipt”) care poate fi ulterior verificată de ambele părți implicate.

Un pionier în acest sens este China, care în 18 martie 2019 a realizat primul experiment de combinare a tehnologiei blockchain cu facturile electronice, în relația B2C. În acea zi China a introdus un sistem nou de taxare pentru pasagerii metroului din orașul Shenzhen, bazat pe plăți electronice. Pasagerii au primit facturi generate automat în urma finalizării călătoriei cu metroul, marcate prin citirea unui cod QR cu telefonul mobil, și stocate într-un ledger interogabil de către fiecare utilizator autentificat prin aplicația WeChat. Această abordare a permis renunțarea la tipărirea de bilete sau la fabricarea și încărcarea cu bani sub forma de credit a cardurilor speciale de transport, rezultant economii substanțiale.

În ceea ce privește smart contract, acestea au devenit utilizate în diversele aplicații de tip DeFi, Ethereum fiind cea mai mare piață de aplicații în domeniul blockchain. Printr-un contract inteligent se dorește implementarea unui sistem economic echilibrat, care să fie mai accesibil, fără să mai existe părți intermediare în punerea în aplicare a acestui sistem. **Contractele inteligente (Smart Contracts)** pot avea utilizări multiple în domeniul urmăririi tranzacțiilor, raportării și colectării impozitelor, validării facturilor electronice și optimizării proceselor de plată.

Vom analiza în continuare o serie de cazuri de utilizare posibile, prin care entitățile implicate pot obține avantaje, atât autoritățile statului cât și operatorii economici.

Obiectivele generale

Analiza oportunității și fezabilității implementării de soluții bazate pe tehnologia blockchain și pe contracte inteligente în urmărirea tranzacțiilor comerciale din România, în particular prin facturare electronică. Se dorește astfel facilitarea între contribuabili și reducerea evaziunii fiscale, crearea unor legături între cumpărător și vânzător, care să ofere o tranzacție directă, fără să mai existe o terță persoană, acest lucru ajută la oferirea produsului direct și într-un interval de timp foarte rapid, pe baza așa numitelor contracte inteligente.

Obiectivele specifice

Analiza utilizării tehnologiilor blockchain pentru:

- Raportarea tranzacțiilor comerciale evidențiate prin facturi electronice.
- Stocarea și arhivarea facturilor electronice și a contractelor inteligente.
- Asigurarea procesului de validare în relația dintre vânzător și cumpărător.

Analiza utilizării contractelor inteligente pentru:

- Rambursări de TVA către operatorii economici.

- Eliberarea garanțiilor în cazul contractelor realizate în urma procedurilor de achiziție publică.
- Aplicarea de reduceri în cazul plăților anticipate a facturilor.

Obiectivele operaționale

- Definirea modului concret de utilizare a tehnologiilor blockchain pentru a susține operațiunile de raportare, stocare și validare.
- Evidențierea abordărilor alternative ale stocării datelor referitoare la facturile electronice în blockchain și identificarea unei variante optime.
- Descrierea modului în care contractele inteligente ar putea fi implementate în contextul cadrului de reglementare actual din România.

Care sunt granițele de utilizare/aplicabilitate avute în vedere?

Ne concentrăm asupra utilizării tehnologiilor blockchain în sisteme implementate și gestionate de către statul român. Abordările pot fi ulterior extinse la sisteme operate de către mediul privat.

Părțile interesate

Cine sunt beneficiarii soluției tehnice/tehnologiei care ar urma să fie dezvoltată?

Beneficiile adoptării tehnologiei blockchain în urmărirea tranzacțiilor și a facturilor electronice se răsfrâng asupra următorilor actori:

- Statul român, prin Agenția Națională de Administrare Fiscală (ANAF), ca entitate care urmărește și auditează tranzacțiile comerciale și colectarea taxelor, în particular a taxei pe valoare adăugată.
- Statul român, prin Centrul Național pentru Informații Financiare (CNIF), ca entitate care realizează implementarea tehnică și gestiunea sistemului informatic pentru colectarea și raportarea facturilor electronice.
- Instituțiile publice care au calitatea de autoritate contractantă în contextul achizițiilor publice și primesc și procesează facturi electronice emise de către furnizori în urma derulării contractelor de achiziție publică.
- Operatorii economici care emit facturi purtătoare de TVA, și care primesc facturi la rândul lor de la alți operatori economici.
- Cetățenii, persoanele fizice, care realizează plăți către operatori economici și alte entități, în urma cărora primesc dovezi ale realizării plății. Nu ne vom concentra asupra acestui tip de beneficiar al sistemului deoarece trasabilitatea completă a tranzacțiilor în relația B2C sau G2C este încă la început, nefiind pe deplin realizată de către nici un stat,

și având în fața provocări semnificative de reglementare și implementare. Notăm însă ca evoluția va fi rapidă în anii următori, în contextul unui interes tot mai mare manifestat de guverne și de Comisia Europeană.

În contextul acestui document, vom avea în vedere în principal interesul statului român ca beneficiar direct al implementării unei soluții de trasabilitate utilizând tehnologia blockchain.

Cine sunt utilizatorii soluției tehnice/tehnologiei?

Considerăm că soluția tehnologică care implică utilizarea blockchain este direct integrată cu sistemele de raportare, stocare și transport de tip EDI (Electronic data interchange), prin urmare în mod indirect utilizatorii acestora sunt utilizatorii soluției analizate.

Aceștia sunt:

- Statul român, prin ANAF, cu rolul de colectare și analiza a informațiilor aferente tranzacțiilor descrise prin facturile electronice, și respectiv rol asumat de validator al acțiunii de emitere a facturilor de către vânzător.
- Operatorii economici, ca vânzător într-o relație comercială de tip B2G sau B2B, care emit facturi electronice și le raportează în sistemul central.
- Cumpărătorii persoane juridice, fie operatori economici la rândul lor, fie autorități contractante, care primesc și procesează facturi electronice

Nu vom trata în contextul acestei analize cumpărătorii persoane fizice deoarece trasabilitatea relației B2C nu are încă un orizont imediat de digitalizare, însă în mare parte considerentele aferente cumpărătorilor persoane juridice se aplică și acestora.

Cum sunt beneficiarii și utilizatorii soluției tehnice/tehnologiei implicați în luarea deciziei asupra soluției propuse? Concretizați și dați detalii.

Ca beneficiar principal și utilizator esențial, statul român prin instituțiile specializate în colectarea taxelor și auditarea rapoartelor privind activitatea economică a operatorilor economici este decidentul esențial. Statul român de asemenea este cel mai în măsură să își asume, singur sau într-o formula de parteneriat cu alte organizații, gestiunea implementării și mentenanței unei soluții informatice care utilizează blockchain în contextul discutat.

Putem avea în vedere scenarii în care implementarea și mentenanța nu este asigurată de către autoritățile statului în exclusivitate, ci pe baza unui parteneriat public privat cu operatori privați de servicii informatice. Acest scenariu poate fi benefic pentru stat prin reducerea costurilor implicate în implementare și gestiunea sistemului, și a posibilităților de dezvoltare de servicii cu valoare adăugată în piață, însă trebuie avută în vedere asigurarea unui nivel de protecție a accesului operatorilor privați neautorizați la date sensibile care ar putea fi eventual exploatate în dauna unor operatori economici privați. Aceste date sensibile pot fi legate de natura bunurilor și serviciilor comercializate, cantități și preturi, cu excepția cazului în care operatorii economici implicați în tranzacții își dau în mod explicit acordul, pe baza unei

formule contractuale a cărei aplicare poate fi controlată, ca anumite informații să poată fi utilizate de operatori de servicii privați pentru oferirea unor servicii cu valoare adăugată, cum ar fi de exemplu servicii de factoring sau finanțare a facturilor.

Vom reveni asupra analizei naturii informațiilor care este stocată în blockchain și accesabilă de către diverse entități implicate, acesta fiind un element esențial în proiectarea soluției.

Beneficiile estimate

Natura oportunității de a dezvolta soluția tehnică/tehnologia

Statul român poate obține avantaje considerabile prin asigurarea capacității de auditare, inclusiv ca probă legală, a informației raportate prin facturile electronice înregistrate, și respectiv a acțiunilor realizate de către părțile implicate în tranzacție (vânzător, respectiv cumpărător).

Aceste informații și acțiuni includ:

- Conținutul facturii electronice, în forma completă sau subset al acestei informații (vom discuta în continuare variantele de abordare).
- Corecturile aduse facturilor electronice emise, prin facturi rectificative (având în vedere ca o factură electronică raportată nu mai poate fi retrasă și înlocuită, chiar dacă de la transmiterea ei inițială nu au existat operațiuni fiscale ca urmare a emiterii).
- Identitatea celui care raportează factura, trimițând-o în sistem, precum și momentul (data, ora) la care o realizează.
- Momentul înregistrării și procesării facturii de către autoritatea națională responsabilă (ANAF).

Sistemul național pentru facturare electronică are la această dată (decembrie 2021) în principal funcția de colectare și procesare a facturilor raportate de către operatorii economici, în mod voluntar deocamdată și cu caracter de obligativitate pentru anumiți operatori economici începând cu 1 iulie 2022, conform reglementării date de ORDONANȚA DE URGENȚĂ nr. 130 din 17 decembrie 2021 privind unele măsuri fiscal-bugetare, prorogarea unor termene, precum și pentru modificarea și completarea unor acte normative.

Este oportun însă să avem în vedere că atât cadrul de reglementare cât și sistemele informatice operate de stat, independent sau împreună cu alte entități, vor evolua în contextul cerințelor și tendințelor de la nivelul Uniunii Europene și de la nivel mondial spre o abordare în care toate facturile în relația B2G și B2B sunt obligatoriu raportate și validarea implică receptorul facturii (cumpărătorul) într-o formă care îi permite acestuia accesarea, procesarea, verificarea și transmiterea confirmării validității și conformității facturii, către sistemul central de raportare și/sau către sistemul emitentului, cu notificarea sistemului central de raportare.

În aceste condiții trebuie să avem în vedere informații și acțiuni adiționale listate precedente care vor putea fi stocate și verificate în blockchain, după cum urmează:

- Momentul (data, ora) la care factura este recepționată de către beneficiar (cumpărător) în vederea procesării.
- Momentul la care factura este confirmată de către cumpărător ca fiind acceptată ca validă și conformă.
- Momentul la care vânzătorul (emitentul facturii) este notificat cu privire la acceptul cumpărătorului.

Pentru toate părțile implicate, o informație foarte utilă o reprezintă indicația privind efectuarea plății unei facturi. Din păcate până în acest moment această posibilitate a fost împiedicată de nivelul ridicat de inerție și reticență a instituțiilor financiare (bănci comerciale, trezoreria statului) de a permite unor operatori terți posibilitatea de planificare și execuție a plăților prin interfețe informatice, deși există atât cadrul de reglementare favorabil (prin Directiva Europeană 2366/2015, cunoscută și ca directiva PSD2) cât și cunoștințele, capacitatea și soluțiile tehnologice.

În momentul în care serviciile de tip „bancă deschisă” („open banking”) vor fi accesibile și integrabile în sistemele utilizate de cei care transmit, respectiv primesc facturi electronice, vor fi disponibile informații suplimentare cu valoare adăugată mare pentru toate părțile implicate, inclusiv pentru autoritățile statului, care vor putea fi de asemenea stocate și verificate în blockchain.

Aceste informații specifice se refera la: Momentul la care cumpărătorul (receptorul facturii) a realizat plata către vânzător (emițătorul facturii), inclusiv cu posibilitatea evidențierii unor cazuri speciale, însă nu excepționale, cum ar fi: plăți parțiale, plăți greșite (de exemplu transferul unei sume mai mari sau plata dublă), plăți în valoare mai mare care includ penalități de întârziere dacă acestea au fost aplicate conform contractului dintre părți.

Care sunt beneficiile estimate?

Capacitatea de auditare a tuturor informațiilor enunțate mai sus conferă statului român posibilitatea de a răspunde rapid și concludent oricărei contestații venite din partea operatorilor economici. Astfel se reduc semnificativ riscurile și costurile aferente investigațiilor și litigiilor în care ar fi fost posibil să fie atrase autoritățile statului.

Utilizarea tehnologiei blockchain pentru stocarea facturilor ar elimina necesitatea semnării acestora cu un certificat de semnătură electronică al ANAF la momentul raportării, deoarece blockchainul în sine devine garantul autenticității și imutabilității facturilor. Pe lângă beneficiul obținut direct prin simplificarea procesului tehnologic, un avantaj adițional este eliminarea unei încărcări suplimentare a sistemului de stocare, considerând că certificatul în sine are în medie 3KB, care se adaugă mărimii facturii electronice care este în medie de 5-6KB.

Factori critici în asociere cu cazurile de utilizare

Avem în vedere în continuare următorii factori critici relevanți pentru implementarea și operarea unui suport de stocare și interogare a facturilor electronice (sau subset al acestora) și a informațiilor adiționale enumerate în secțiunea precedentă:

Factori critici privind cerințele tehnice

- **Scalabilitatea sistemului.** Estimările actuale indica faptul că numărul total al facturilor emise în România în fiecare lună de cei circa 500.000 operatori economici activi și instituții emițătoare de facturi (de exemplu operatorii publici de utilități) se ridică la 50 de milioane, majoritatea fiind purtătoare de TVA. Chiar dacă un număr mare de facturi de utilități sunt adresate consumatorilor casnici, așadar clienților persoane fizice, faptul că ele sunt purtătoare de TVA va implica, în momentul reglementării obligativității de raportare directă a facturilor electronice, că toate aceste facturi să fie transmise prin sistem către ANAF. O factură electronică realizată într-unul din cele două standarde tehnice XML reglementate prin standardul european pentru facturare electronică are o mărime medie de 5KB, fără a considera eventualele fișiere suplimentare atașate unelor facturi (standardul pentru facturare electronică permițând această practică). Simpla multiplicare ne indică faptul că un volum de 250GB de facturi în format electronic vor fi raportate lunar. Dacă ANAF vă menține practica de semnare a facturilor raportate cu certificatul propriu de semnătură digitală, pentru a asigura autenticitatea și imutabilitatea informațiilor, fiecărei facturi i se mai adaugă 2-4KB, ceea ce ar duce la un volum suplimentar lunar stocat de circa 400GB. Am argumentat în secțiunea precedentă că în condițiile utilizării tehnologiei blockchain pentru stocare, aplicarea certificatelor devine redundantă și prin urmare poate fi eliminată. Stocarea facturilor în blockchain va duce la o creștere rapidă în timp a informațiilor stocate, necesitând spații de stocare, costuri aferente și inducând posibile penalizări ale vitezei de interogare și obținere de informații din blockchain. Avem în vedere că vor fi de asemenea stocate alte informații suplimentare aferente fiecărei facturi, așa cum am detaliat în secțiunea precedentă.

- **Performanța sistemului,** în special rata de scriere în unitate de timp, va fi un element critic. Trebuie să avem în vedere că cele circa 50 de milioane de facturi emise lunar nu se raportează în mod uniform în timp de-a lungul unei luni. O analiză predictivă a distribuției raportării în cursul unei luni calendaristice ar fi necesar să fie realizată chiar în lipsa utilizării unui blockchain. Trebuie să avem în vedere că sistemul trebuie să facă față unor vârfuri de volum, datorate transmiterii unui număr foarte mare (milioane) de facturi de către operatorii de utilități, într-un interval de timp foarte strâns.

- **Accesibilitatea informațiilor.** Informațiile conținute în facturile electronice, precum și celelalte informații stocate (legate de starea facturilor sau de momentul efectuării unei acțiuni) trebuie să fie disponibile oricând celor care au dreptul să le acceseze (incluzând operatorii economici implicați), dar numai acestora.

- **Disponibilitatea sistemului.** Fiind un sistem critic la nivel național, de care vor depinde în mod direct toți operatorii economici, este esențial ca sistemul să fie permanent disponibil.

- **Securitatea sistemului.** Informația stocată este critică și din perspectiva confidențialității sau a riscurilor aferente divulgării în piață a unor informații care ar putea fi clasificate de către operatorii economici ca fiind secrete comerciale, sau informații care pot fi utilizate de concurența comercială în scopuri detrimentale vânzătorilor (de exemplu ce vinde, cui vinde, cât vinde, cu cât vinde un anumit operator economic).

Factori critici de cost

Elementele de cost relevante pentru implementarea și întreținerea sistemului sunt:

- Costul direct de implementare, în orice formă ar fi el suportat: implementare realizată integral de către personalul tehnic al statului român prin CNIF, parteneriat inter-instituțional sau public-privat, respectiv proiect implementat pe baza unui contract atribuit prin procedura de achiziție publică.
- Costul de pregătire al proiectului, incluzând analiza, specificarea, pregătirea și derularea procedurii de achiziție publică dacă este cazul sau organizarea și planificarea resurselor umane necesare, dacă proiectul se derulează exclusiv cu personal tehnic al statului, sau într-o formulă combinată public-privată.
- Costul de instruire al personalului, mai mic dacă se referă doar la capacitatea de întreținere, mai mare dacă se referă și la capacitatea de implementare.
- Costul necesar infrastructurii de stocare și a întreținerii acesteia. Nu este în mod necesar un cost suplimentar față de cel care ar fi implicat în cazul stocării facturilor, fără a utiliza blockchain.
- Costul operațiunilor de gestiune a blockchain-ului pe baza unei strategii de utilizare, stocare și arhivare. Pentru a gestiona problema scalabilității pe termen mediu și lung, poate fi considerată o strategie prin care ledger-ul se înlocuiește atunci când se ajunge la un număr mare critic de înregistrări, iar ledger-ul utilizat anterior rămâne disponibil pentru interogări într-un regim special. Aceasta abordare ar putea fi fezabilă din punctul de vedere al necesităților funcționale, deoarece în general ciclul de viață al unei facturi este relativ redus, doar în mod excepțional depășind 120 de zile, de cele mai multe ori 30-60 sau 90 de zile, implicând emiterea, raportarea, verificarea, acceptarea și plata facturii. Dat fiind că fiecare entitate implicată (vânzător și cumpărător) are obligația legală de a asigura arhivarea facturilor trimise, iar statul nu își asuma (cel puțin deocamdată) înlocuirea acestei obligativități cu un sistem național de arhivare disponibil pe termen lung părților implicate, o strategie care implică resetarea periodică a ledger-ului ar putea fi fezabilă.

Factori critici privind calitatea

Calitatea arhitecturii, atât la nivelul procesului, cât și la nivel tehnic, este un aspect esențial pentru succesul sistemului. Acesta pornește de la modul în care este definit și implementat ciclul de viață al facturii electronice între cei 3 participanți la proces: vânzător, cumpărător și autoritatea fiscală. Dat fiind că nu există un standard impus la acest moment

pentru modul în care este implementat procesul de validare (clearance), statele care au realizat deja astfel de implementări au ales diverse modele.

Factori critici privind ușurința execuției

Sistemul bazat pe blockchain este o componentă integrată cu alte sisteme, care asigură interfețele tehnice și vizuale prin care atât sistemele informatice terțe cât și utilizatorii umani interacționează.

Factorul critic legat de utilizabilitate este capacitatea de răspuns a sistemului în condițiile unui flux masiv de facturi trimise într-un interval scurt de timp. Rezolvarea acestei probleme necesită abordări tehnice specializate, de exemplu utilizarea unor cozi de așteptare și o comunicare informatică bidirecțională care să asigure că eventualele erori de transmisie pot fi remediate printr-o nouă încercare de trimitere a facturii.

Cu un risc mai redus, dar totuși de considerat, trebuie să asigurăm capacitatea crescută a răspunsului la interogări legate de statusul unor facturi.

Factori critici sub aspect economic (efecte colaterale negative, costuri de oportunitate)

Trebuie asigurată capacitatea financiară pentru:

- Implementarea sistemului
- Menținerea sistemului
- Instruirea personalului care va realiza mentenanța sistemului și eventual implementarea lui, dacă aceasta nu se va realiza ca urmare a unei proceduri de achiziție publică.

De asemenea trebuie avut în vedere și costul generat de consumul de energie, necesar derulării proceselor specifice blockchain (mecanisme de consens, criptare asimetrică etc). Acest consum poate fi ridicat și este mult influențat de tipul de blockchain care va fi ales.

Costurile cu infrastructura trebuie avute în vedere, atât pentru stocare (asigurarea volumului necesar și a performanței de scriere și citire pe și de pe mediul de stocare), cât și pentru operațiile specifice blockchain.

Factori critici sub aspect legal

Nu există impedimente legale privind stocarea de către autoritatea financiară a statului a informațiilor descrise în acest context.

Provocări tehnice în implementarea intervenției

Potrivit Standardului european privind facturarea electronică cerințele tehnice implementării unui sistem tehnologic ar trebui să respecte specificațiile tehnice existente elaborate în cadrul organizațiilor europene de standardizare precum CEN (CWA 16356-MUG și

CWA 16562-CEN BII) și ar trebui să ia în considerare alte specificații tehnice relevante elaborate în cadrul organizațiilor internaționale de standardizare precum ONU/CEFACT (CII v. 2.0) și ISO (factură financiară bazată pe metodologia ISO 20022).

Odată cu implementarea unui sistem de tip blockchain se va trece la o descentralizare a sistemului financiar (*DeFi - Decentralized Finance*), care implică existența unor rețele vaste, open-source, care permit oricui să creeze aplicații care oferă desfășurarea activității financiare fără implicarea instituțiilor centralizate. Acest tip de finanțări sunt construite pe baza unor contracte inteligente și sunt programate să ruleze pe baza unui cod dezvoltat care îi permite să fie disponibil pentru oricine face posibilă rețeaua peer-to-peer.

Provocările sunt semnificative, date de volumul mare de articole (facturi electronice) care trebuie primite, procesate și stocate. Aceste provocări sunt:

- Scalabilitatea componentei blockchain, care trebuie să facă față la stocarea a peste 50 de milioane de facturi sau extrase din facturi, în fiecare lună. Acest factor a fost detaliat mai sus.
- Performanța, prin viteza de răspuns, la un număr mare de cereri concurente. Și acest factor a fost detaliat mai sus.
- Securitatea, dat fiindcă se stochează informații sensibile.
- Consumul de energie, un element important pentru orice proiect bazat pe blockchain.
- Infrastructura necesară pentru stocare și pentru operațiunile specifice blockchain trebuie să fie optim dimensionată, într-un mod care să permită scalarea în timp dacă va fi nevoie.

Procese curente care ar putea fi afectate de dezvoltarea proiectului

Principalele procese afectate pozitiv de această implementare sunt:

- Raportarea fiscală a tranzacțiilor comerciale, prin transmiterea și analiza facturilor electronice.
- Răspunsul autorității financiare la reclamații și cereri de investigare.
- Validarea facturilor de către cumpărător.

Obiectivele funcționale

Funcționalități dorite a fi regăsite în cadrul soluției tehnice/tehnologiei

Abordarea pe care o propunem se concentrează pe stocarea și capacitatea de accesare controlată a informațiilor esențiale din ciclul de viață a unei facturi fiscale, transmisă ca factură electronică standard.

Argumentăm pentru a realiza stocarea în blockchain a unui subset de date, din cadrul facturii, nu a întregii facturi electronice. Acest subset, pe care îl putem numi ca „date esențiale

de identificare și raportare”, este suficient pentru a asigura atât trasabilitatea cât și auditul facturilor în vederea asigurării colectării complete a TVA-ului. În esență, acest subset este suficient pentru autoritatea fiscală centrală în relația cu urmărirea tranzacțiilor și raportarea lor, atâta timp cât datele complete rămân în continuare disponibile pentru auditare, conform cerințelor legale actuale.

Acest subset este reprezentat de următoarele informații:

- Identitatea părților implicate în tranzacție (vânzător, cumpărător, eventual partea care va fi plătită dacă diferă de vânzător). Identitatea poate fi specificată simplu prin CUI sau numărul de înregistrare în scopuri de TVA pentru eventualele facturi emise de entități nerezidente, dacă la un moment dat facturi emise de acestea vor fi raportate în sistem.
- Numărul și data emiterii facturii.
- Suma totală fără TVA.
- Suma reprezentând TVA-ul.
- Rezumat criptografic al facturii (explicația se regăsește în continuare).

Eventual se poate determina în urma unei analize suplimentare realizată la nivelul experților fiscali din ANAF dacă acest subset trebuie să includă explicit, în mod defalcăt, sumele fără TVA și respectiv TVA-ul pentru fiecare cotă de TVA aplicată în cazul în care factura conține articole la care se aplică cote diferite.

Acest subset propus spre stocare în blockchain poate fi formatat independent de formatul original al facturii electronice din care este extras, așadar nu trebuie să urmeze un format XML standardizat, ci poate fi un format determinat astfel încât să asigure procesabilitatea rapidă și interogarea eficientă a structurii de stocare.

Stocarea efectivă a facturilor electronice nu este, cel puțin deocamdată, un aspect pe care statul român să și-l asume în numele participanților la tranzacția economică, în condițiile în care cadrul legal îi obligă pe aceștia să păstreze facturile. În același timp, stocarea efectivă a facturilor electronice ar determina probleme de scalabilitate datorită numărului lor mare pe luna (peste 50 de milioane) și a mărimii lor (5-6 KB, fără certificatul de semnătură digitală care mai adaugă 2-4KB). Prin urmare, stocarea efectivă a facturilor în blockchain nu este recomandată. În schimb, o abordare care ar permite verificarea ulterioară a integrității facturii electronice transmise, chiar fără a utiliza aplicarea unui certificat, este prin generarea și stocarea unui rezumat criptografic (checksum, hash).

În cazul în care facturile electronice vor fi stocate centralizat, este preferabil să nu fie stocate în blockchain pentru a putea permite mai ușor arhivarea lor prin extragerea periodică din structura de stocare de producție a facturilor vechi (care au o vârstă mai mare decât cea care se va defini pentru asta), și arhivarea acestora, într-o structură de stocare care ulterior va fi interogată doar excepțional, atunci când este nevoie de o verificare a unei facturi vechi. În acest scenariu informațiile esențiale ar putea cuprinde și o referință spre structura de stocare, care să permită identificarea atât în cadrul structurilor de producție cât și în arhive.

Celelalte informații relevante a fi stocate în blockchain se referă la ciclul efectiv de viață al facturii și la procesul de validare a lor în relația dintre vânzător și cumpărător. Astfel, aceste date sunt:

- Data și ora la care factura a fost raportată (trimisă în sistemul central) de către vânzător.

- Data și ora la care cumpărătorul a fost notificat de sistemul central (sau de un sistem satelit, în funcție de modul de implementare viitor) că factura a fost transmisă și înregistrată.
- Data și ora la care cumpărătorul a primit factura pentru procesare, în urma unui proces automat realizat de sistemul informatic al cumpărătorului, sau al unei operațiuni realizată manual.
- Data și ora la care cumpărătorul a confirmat corectitudinea și validitatea facturii, sau dacă este cazul
- Data și ora la care cumpărătorul a refuzat factura pe motiv de incorectitudine și în acest caz va trebui să stocăm și
- Motivul refuzului facturii, descris de către destinatarul facturii.

Stocarea și interogarea acestor informații în blockchain va fi realizată prin sistemul național de facturare electronică. Dată fiind natura sensibilă a acestor informații și necesitatea unui control strict asupra sistemului, stocarea va trebui realizată într-un blockchain de tip permissioned, care nu este accesibil public. În același timp, ar fi oportun ca ledger-ul să fie distribuit, cu câteva noduri care să fie în custodia mai multor instituții centrale (cu titlu de exemplu, nodurile ar putea fi găzduite de CNIF, STS, MAI).

Adaugirile de informații și interogările se vor realiza prin intermedierea platformei naționale de facturare electronică. Ar fi oportun de analizat în continuare dacă anumite interogări ar putea fi realizate și de către aplicații terțe autorizate. De exemplu, verificarea dacă o anumită factură a fost confirmată de către cumpărător este o informație foarte utilă pentru operatorii de servicii de factoring sau finanțare a facturilor și permite operatorului economic vânzător să beneficieze mai ușor și mai ieftin de un serviciu valoros pentru el. Acesta este un exemplu de valoare adăugată adusă de această abordare tehnică.

Obiectivele de performanță

Caracteristicile de performanță tehnică ale soluției

Scalabilitatea, performanța și securitatea sunt obiectivele principale care guvernează analiza tehnică în vederea identificării soluției optime, atât ca arhitectură, cât și din perspectiva tipului de blockchain utilizat.

De asemenea, latenta rețelei, în strânsă dependență de numărul de noduri ale rețelei blockchain, dat fiind că pentru validarea unei tranzacții trebuie colectat consensul majoritar de la toate nodurile, ceea ce determină că numărul de noduri să fie cât mai mic posibil, totuși păstrându-se abordarea distribuită.

Elementele de noutate

Ce factori negativi doriți să eliminați în totalitate?

- Dificultatea probării realizării unei acțiuni a vânzătorului sau cumpărătorului în ciclul de viață al facturii electronice.
- Necesitatea aplicării certificatului de semnătură digitală al ANAF pe facturile raportate ca probă a raportării și garant al imutabilității conținutului.

Ce factori negativi doriți să diminueați?

- Necesitate stocării pe termen lung a unui număr mare de fișiere pe infrastructura autorității fiscale.

Ce elemente doriți să le aduceți peste standardele actuale?

- Stocarea și posibilitatea de verificare a fiecărei acțiuni importante din procesul de transmitere, raportare, primire și validare a facturilor fiscale în format electronic.

Ce elemente noi doriți să creați și ce rezolvă acestea?

- Posibilitatea stocării fără echivoc a confirmării date de cumpărător asupra validității și corectitudinii facturii.

Criteriile de selecție

Listă criterii

Deciziile esențiale sunt de natură tehnică și se referă la tehnologia blockchain utilizată.

Criteriile de selecție pentru aceasta sunt:

- Scalabilitatea – capacitatea de a stoca multe înregistrări, cel puțin 50 de milioane facturi (sau date esențiale ale facturilor) pe luna, plus încă cel puțin 3 informații esențiale pentru fiecare factură (data și ora raportării, data și ora accesării pentru procesare, data și ora confirmării validității și corectitudinii).
- Performanța – capacitatea de stocare și de interogare în unitate de timp.
- Securitatea
- Asigurarea accesului controlat la resurse doar pentru entitățile care au acest drept.
- Blockchainul să fie distribuit, cu mai multe noduri aflate în custodia unor operatori de încredere.
- Asigurarea interoperabilității cu EBSI (European Blockchain Services Infrastructure), ceea ce limitează implicit alegerea tehnologiei.

Nivel minim de performanță pe fiecare criteriu

- Scalabilitate – cel puțin 200 de milioane de înregistrări adăugate lunar.
- Performanța – să facă față, direct sau prin utilizarea unor cozi de așteptare, a unui număr ridicat de tranzacții transmise foarte rapid (doar Digi de exemplu emite 7 milioane de facturi pe lună și este posibil ca sistemul de generare să le transmită într-o singură sesiune compactă)

Ponderea criteriilor

În ordine, prioritatea criteriilor este:

- Securitatea
- Performanța
- Scalabilitatea
- Compatibilitatea cu EBSI.

Descrierea în detaliu a cazului de referință

Deocamdată nu cunoaștem cazuri de implementare relevante pentru producție. Am descris în introducere cazul de utilizare experimental în China, utilizat însă într-un scenariu tranzacțional de tip B2C, cu scopul urmăririi plății și eliberării dovezii de plată. Deși în perspectivă astfel de cazuri de utilizare pot fi avute în vedere pentru extinderea sistemului propus, ele nu reprezintă scopul acestei implementări.

Datorită avansului înregistrat de multe state în direcția reglementării și implementării sistemelor de urmărire și raportare a tranzacțiilor prin facturi electronice ne vom aștepta ca astfel de implementări să fie tot mai des avute în vedere în anii următori.

Opțiuni de îmbunătățire

În lipsa unei referințe comparabile, îmbunătățirile se pot referi doar la situația actuală a informatizării proceselor discutate în România și în alte state unde sunt utilizate platforme pentru transmitere, raportare, stocare, și validare, după caz. În România implementarea platformei naționale pentru facturare electronică va continua, crescând în complexitate, iar în alte țări abordarea tehnică și de proces este specifică, așadar aplicarea unei comparații nu aduce valoare adăugată.

Analiza comparativă

Obiectul alegerii și respectiv al analizei în vederea alegerii, este tehnologia blockchain utilizată. Candidații de bază sunt Ethereum și Hyperledger Fabric, această filtrare fiind deja realizată, argumentat, pentru compatibilitatea cu EBSI.

Dat fiindcă avem restricția necesară din perspectiva securității ca blockchain-ul să fie permissioned, candidatul rezultat care corespunde și acestui criteriu rămâne Hyperledger Fabric.

Constrângeri privind implementarea

Datorită caracterului de pionierat al implementării și în lipsa unor analize comparative realizate de alte state privind efectul economic al unei implementări bazate pe blockchain a proceselor de raportare fiscală, un element important de constrângere va fi determinat de necesitatea justificării economice a acestui tip de abordare. Pentru aceasta, trebuie să avem în vedere colectarea suplimentară de informații privind costurile litigiilor în care este atrasă autoritatea fiscală națională ca urmare a contestațiilor primite de la contribuabili privind corectitudinea calculului taxelor datorate. Chiar dacă mecanismul de raportare se schimbă prin introducerea raportării facturii electronice, natura contestațiilor se păstrează. Soluționarea acestora, prin probe edificatoare transmise de către ANAF contribuabilului sau prin instanță, induce costuri directe și indirecte (de oportunitate a implicării personalului în activități utile).

Alte constrângeri se refera la:

- Costurile necesare implementării și operării sistemului.
- Efortului și cunoștințelor necesare pentru specificarea, implementarea și întreținerea, iar în cazul implementării externalizate prin contract realizat în urma unei achiziții publice, a capacității de evaluare a ofertelor și de verificare a calității implementării.
- Alegerea tehnologică limitată datorită criteriilor aplicate.

Resurse tehnice pentru implementare

Resursele tehnice necesare implementării se referă la:

- Infrastructura hardware: Noduri blockchain. Numărul lor trebuie determinat, însă având în vedere caracterul permissioned al blockchainului vizat și nivelul ridicat de securitate al accesului necesar, numărul nodurilor va fi probabil restrâns (3-4 noduri gestionate de instituții care au capacitate tehnică să o facă).
- Componentele software pentru pre-procesarea cererilor de scriere în blockchain și a cererilor de citire a informațiilor. În funcție de arhitectura de proces care va fi stabilită, se vor defini operațiuni specifice componentei blockchain, care nu sunt utilizate de celelalte componente ale sistemului național pentru facturare electronică.

Resurse umane pentru implementare

Planificarea și implementarea acestui sistem necesită aptitudini diverse, care trebuie asigurate de o echipă tehnică bine instruită. Includem în continuare doar domeniile de competență specifice implementării componentei blockchain, fără a include dezvoltarea de interfețe vizuale, deoarece utilizatorii nu vor interacționa în mod direct prin browser sau alte tipuri de client software cu sistemul:

- Arhitectura software
- Infrastructura hardware
- Analiză de business și de proces
- Tehnologie blockchain/DLT
- Criptografie
- Securitate cibernetică.

Resurse financiare pentru implementare

Tipurile de costuri implicate se regăsesc în următoarele categorii:

- Costuri de coordonare
- Costuri de analiză de proces
- Costuri de specificare funcțională și non-funcțională
- Costuri de derulare a procedurilor de achiziție publică și de gestiune a contractului (în cazul în care se optează pentru această variantă)
- Costuri de training al personalului (în pondere mai mare dacă implementarea nu va fi contractată prin achiziție publică)
- Costuri de dezvoltare
- Costurile infrastructurii hardware – achiziție și operare
- Costuri de integrare cu sistemele existente
- Costuri de testare
- Costuri de evaluare și monitorizare
- Costuri de audit de securitate
- Costuri de mentenanță.

Costuri estimative pentru infrastructura hardware de stocare

Server: 10 bucăți, câte două per locație (cu echilibrare de sarcină).

Stocare online: 1TB/server, în configurație RAID cu disponibilitate ridicată.

Server cu discuri în RAID incluse: 70000 RON/server , 700000 RON/10 servere.

Costuri cu resursa umana: Cost salarial pentru specialist în medie 13,500 RON. Circa 24 luni-om necesare în total.

Resurse logistice pentru implementare

Pregătirea și implementarea acestui sistem necesită conlucrarea între mai multe instituții publice, ceea ce necesită o bună gestiune a comunicării și planificării proiectului în toate fazele sale.

Dacă se va implementa un blockchain permissioned cu mai multe noduri, gestionate de organizații diferite, trebuie asigurat cadrul formal de cooperare între aceste instituții, precum și mecanismul tehnic de interoperare.

Riscuri și planuri de contingență

- **Riscuri de finanțare.** Justificarea efectelor pozitive ale implementării sistemului trebuie realizată inclusiv prin evaluarea impactului financiar (de exemplu prin reducerea costurilor generate de litigii), pentru a avea șanse de aprobare a bugetelor de implementare inclusiv dacă aceasta trebuie realizată din fonduri bugetare, în lipsa asigurării unor finanțări externe (europene).
- **Riscuri legislative.** Nu sunt riscuri specifice implementării bazate pe blockchain.
- **Riscuri ale costurilor de întreținere.** Trebuie asigurată capacitatea umană și financiară a întreținerii sistemului. Risc redus, în condițiile existentei capacității tehnice și a asumării la nivelul Ministerului Finanțelor Publice, prin CNIF.
- **Riscuri de ocupare.** România are deocamdată un număr relativ redus de specialiști în blockchain care ar putea realiza implementarea, cu atât mai mult în sectorul public. Cei din sectorul public trebuie instruiți corespunzător, iar pentru mediul privat, în cazul în care se optează pentru implicarea companiilor prin contracte de achiziție publică, trebuie asigurată competitivitatea și accesibilitatea procedurilor de achiziție pentru a permite participarea companiilor care au competențe în domeniu.
- **Riscuri operaționale.** Disponibilitatea nodurilor blockchain reprezintă un factor critic, dat fiind că va fi un element de care va depinde capacitatea de raportare a facturilor electronice la nivelul întregii țări.
- **Riscuri de planificare.** În lipsa unei experiențe comparabile atât pentru specialiștii interni cât și pe plan internațional, estimarea efortului și planificarea calendarului de implementare este dificilă. Acesta este un risc ridicat. Ar trebui optat pentru planificarea cu o variantă pesimistă.
- **Riscuri de schimbare a opțiunilor politice (riscuri decizionale).** În lipsa unei strategii documentate pe termen mediu și lung, și asumate de către guvern, care să prevadă evoluția cadrului de reglementare care influențează utilizarea facturii electronice în

raportarea fiscală, și a introducerii graduale a obligativității de utilizare a sistemului de facturare electronică, respectiv a mecanismelor de notificare și de validare (clearance), avem un risc ridicat în privința specificației pentru colectarea și stocarea dovezilor de primire, respectiv de facturare. Ar trebui susținută necesitatea unei planificări documentate și asumate pe termen mediu și lung, chiar dacă va fi doar sub forma unui plan de acțiune inter-instituțional și nu a unei strategii formale.

- **Riscuri legate de procedurile de achiziții publice.** Riscurile aferente sunt multiple dar se pot mitiga printr-o pregătire corespunzătoare:
 - Specificații funcționale și nefuncționale insuficient de detaliate.
 - Criterii de calificare și selecție, respectiv factori de evaluare care să reducă competitivitatea calitativă a ofertelor și să limiteze competiția.
 - Lipsa unui suport tehnic adecvat de nivel expert în procesul de evaluare a ofertelor.
 - Neasigurarea unui proces strict de management a derulării contractului și a procesului de testare, evaluare, audit al rezultatului.

Se recomandă organizarea în prealabil, înaintea definitivării documentației de atribuire, a unui proces formal de consultare a pieței, incluzând discuții directe cu operatorii economici interesați să participe la procedură.

- **Riscuri reputaționale (influența opiniei publice).** Fiind vorba de un sistem critic, cu influență directă în abilitatea operatorilor economici de a transmite și recepționa facturi, indisponibilitatea sistemului, sau funcționarea lui defectuoasă (erori, întârzieri mari etc.) pot genera critici deschise din partea opiniei publice.
- **Riscuri ale schimbărilor tehnologice.** Utilizarea tehnologiei blockchain în proiecte critice la nivel național presupune un risc inherent nivelului relativ redus de maturitate a tehnologiei. Deși a fost folosit în alte sisteme importante pentru stat (de exemplu în Estonia), tehnologia rămâne în continuare relativ puțin probată.
- **Riscuri ale volumului de activitate estimat.** În perspectiva evoluției spre un sistem național prin care se raportează toate facturile purtătoare de TVA emise, volumul de date și numărul de tranzacții va fi ridicat. Urmărind tendințele la nivel mondial și mai ales european de a integra în aceeași abordare standardizată și documentele de tip bon electronic (e-receipt), chitanță și factură simplificată, este posibil ca în cazul integrării acestor tipuri de tranzacții dimensionarea inițială să se dovedească inadecvată. Totuși, acele cazuri trebuie analizate pentru a nu încărca sistemul într-un mod care nu este necesar, dat fiindcă acele tranzacții nu sunt purtătoare de risc de contestare și că nu necesită validarea cumpărătorului, aceasta fiind realizată implicit la momentul plății, în general anterior emiterii documentului.

Interacțiunea cu alte sisteme tehnice

Sistemul care face obiectul acestui document este integrat direct cu sistemul național pentru facturare electronică. El poate fi integrat, potențial, cu orice sistem de tip EDI care are aceleași funcționalități de bază, dar contextul descris în documentul de față descrie o relație directă, dependentă, cu sistemul național, care la rândul lui este conectat cu alte sisteme, atât cele operate de instituții cât și de furnizori privați.

Abordarea pe care o recomandăm este ca sistemul bazat pe blockchain să nu fie accesibil în mod direct din exterior din alte aplicații, ci toate interogările să treacă prin sistemul central de facturare electronică.

În funcție de scenariile care se vor defini și implementa, în special pentru procesele de notificare și validare (clearance) care încă nu sunt implementate în sistemul național pentru facturare electronică, se poate asigura o eventuală accesabilitate directă a unor funcționalități, ca servicii expuse de sistemul bazat pe blockchain.

Diagrama pentru implementare

Activitate	Rezultat	Perioada de implementare (în trimestre)							
		Q1	Q2	3	4	5	6	7	8
Analiză și specificare	Arhitectura de proces, arhitectura tehnică, specificațiile funcționale și non-funcționale, configurația infrastructurii hardware								
Formarea personalului	Acumulare de cunoștințe și activități de implementare pilot folosind frameworkuri blockchain (Hyperledger fabric si/sau altele)								
Pregătire logistică, consultarea pieței	Protocoale inter-instituționale pentru găzduirea nodurilor, evaluări comparative ale efortului și costului de implementare, bază pentru decizia „make or buy”								
Pregătirea logistică internă sau derularea procedurii de achiziție	Echipa de implementare evaluată și selectată, managementul implementării planificat, uneltele de management și dezvoltare definite și documentate, infrastructura de development și staging planificată								
Implementarea tehnică inițială	Soluția tehnică implementată și integrată cu un mediu de staging al sistemului de facturare								

	electronică								
Testare și audit	Teste funcționale, teste de scalabilitate, performanță, audit de securitate, backup and restore etc.								
Operaționalizarea sistemului	Introducerea sistemului în producție								

Fig. 1: Diagrama Gantt a activităților de implementare a sistemului

Metodologia de management a proiectului și modelul de dezvoltare

Fiind un sistem strict corelat cu sistemul național pentru facturare electronică, optim ar fi ca gestiunea acestui proiect să se realizeze unitar cu cel al sistemului național, în același cadru instituțional și cu același management.

Precondiții și factori critici pentru succes

Elementul cel mai important este asumarea instituțională a realizării acestei implementări. Detalierea specificației funcționale, a arhitecturii tehnice și a necesarului de infrastructură hardware trebuie să preceadă alocarea efectivă a bugetului. Pentru a asigura distribuția blockchain-ului va fi nevoie de buna conlucrare interinstituțională cu instituțiile care au capacitatea tehnică de găzduire și întreținere a unui nod.

Indicatori pentru monitorizare și evaluare

Indicatori de implementare

Sistem complet funcțional asigură stocarea tuturor facturilor raportate în sistemul național

Indicatori de reziliență

Sistemul funcționează corespunzător fără întreruperi și blocaje chiar în condiții de vârf de sarcină, când au loc multe tranzacții într-un interval scurt de timp

Indicator de performanță

Întârzierea maximă între momentul inițierii tranzacției de către utilizator (contribuabil raportor) și scrierea efectivă în blockchain este redus, maxim de ordinul minutelor, chiar în condiții de vârf de sarcină când numărul de tranzacții este foarte ridicat

Referințe bibliografice

- 1.1. *Directiva 2014/55/UE A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 16 aprilie 2014 privind facturarea electronică în domeniul achizițiilor publice*, <https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32014L0055&from=DE>, accesat noiembrie 2021.
- 1.2. *Raport referitor la tehnologia blockchain: o politică comercială orientată spre viitor (2018/2085(INI))*, https://www.europarl.europa.eu/doceo/document/A-8-2018-0407_RO.html, accesat noiembrie 2021
- 1.3. *eInvoicing Country Factsheets for Each Member State and other countries* <https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/eInvoicing+Country+Factsheets+for+each+Member+State+and+other+countries>, accesat noiembrie 2021
- 1.4. *Politici fiscale: soluțiile UE pentru a preveni fraudele și evaziunea fiscală*, <https://www.europarl.europa.eu/news/ro/headlines/economy/20210415STO02118/solutiile-ue-pentru-a-preveni-fraudele-si-evaziunea-fiscala>, accesat noiembrie 2021.
- 1.5. Barna Tanczos: proiectul pilot de e-facturare trebuie extins pe cât mai multe paliere, <https://www.research.gov.ro/ro/articol/5447/minister-comunicare-barna-tanczos-proiectul-pilot-de-e-facturare-trebuie-extins-pe-cat-mai-multe-paliere>, accesat noiembrie 2021.
- 1.6. *Finanțele au publicat specificațiile tehnice pentru proiectul e-Factura*, <https://www.profit.ro/taxe-si-consultanta/video-finantele-au-publicat-specificatiile-tehnice-pentru-proiectul-e-factura-20394430>, accesat noiembrie 2021.
- 1.7. *Legea nr. 199 din 8 septembrie 2020 privind facturarea electronică în domeniul achizițiilor publice*, accesat noiembrie 2021.
- 1.8. *Caracteristicile facturării electronice în Austria*, <https://edicom.com.ar/factura-electronica/austria>, accesat noiembrie 2021.
- 1.9. *Caracteristicile facturii electronice în Chile*, <https://edicom.com.ar/factura-electronica/chile>, accesat noiembrie 2021.
- 1.10. *Caracteristicile facturii electronice în Germania*, <https://edicom.com.ar/factura-electronica/alemania>, accesat noiembrie 2021.
- 1.11. *Caracteristicile facturii electronice în Italia*, <https://edicom.com.ar/factura-electronica/italia>, accesat noiembrie 2021.
- 1.12. *Caracteristicile facturii electronice în Panama*, <https://edicom.com.ar/factura-electronica/panama>, accesat noiembrie 2021.
- 1.13. *Caracteristicile facturii electronice în Uganda*, <https://edicom.com.ar/factura-electronica/uganda>, accesat noiembrie 2021.
- 1.14. *Caracteristicile facturii electronice în Uruguay*, <https://edicom.com.ar/factura-electronica/uruguay>, accesat noiembrie 2021
- 1.15. *The future of financial infrastructure*, https://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf, accesat noiembrie 2021.
- 1.16. *China – Shenzhen teams up with Tencent to launch blockchain based electronic invoices*, <https://www.chinabankingnews.com/2019/03/18/shenzhen-metro-system-teams-up-with-tencent-to-launch-blockchain-based-electronic-invoices/>, accesat noiembrie 2021.



Proiect:

Proiect selectat în cadrul Programului Operațional Capacitate Administrativă cofinanțat de Uniunea Europeană, din Fondul Social European

Axa Prioritară 1: Administrație publică și sistem judiciar eficiente

Obiectivul specific 1.1: Dezvoltarea și introducerea de sisteme și standarde comune în administrația publică ce optimizează procesele decizionale orientate către cetățeni și mediul de afaceri, în concordanță cu SCAP.

Titlul proiectului: „ Cadru strategic pentru adoptarea și utilizarea de tehnologii inovative în administrația publică 2021-2027 – soluții pentru eficientizarea activității”

COD: SIPOCA 704

Beneficiar: AUTORITATEA PENTRU DIGITALIZAREA ROMÂNIEI

Partener: UNIVERSITATEA TEHNICĂ DIN CLUJ - NAPOCA

Fundamentarea cazului de utilizare și studiu de
evaluare ex-ante pentru
Urmărirea proprietăților, managementul
proprietății asupra terenurilor și utilizarea
terenurilor agricole

Cuprins

Acronime și abrevieri	3
Scopul intervenției	3
Părțile interesate.....	6
Beneficiile estimate.....	6
Factori critici în asociere cu cazurile de utilizare	7
Provocări tehnice în implementarea intervenției.....	9
Procese curente care ar putea fi afectate de dezvoltarea proiectului	10
Obiectivele funcționale	11
Obiectivele de performanță.....	13
Elementele de noutate	15
Criteriile de selecție	15
Descrierea în detaliu a cazului de referință	16
Opțiuni de îmbunătățire	20
Analiza comparativă.....	21
Constrângeri privind implementarea.....	21
Resurse tehnice pentru implementare	22
Resurse umane pentru implementare.....	23
Resurse financiare pentru implementare	24
Resurse logistice pentru implementare.....	24
Riscuri și planuri de contingență.....	25
Interacțiunea cu alte sisteme tehnice	27
Diagrama pentru implementare	27
Metodologia de management a proiectului și modelul de dezvoltare	29
Precondiții și factori critici pentru succes	30
Indicatori pentru monitorizare și evaluare	30
Referințe bibliografice	31

Acronime și abrevieri

Abreviere sau acronim	Expresia completă	Explicație
DLT	Distributed Ledger Technology	Tehnologie de tip registru distribuit.
DIDs	Decentralized identifiers	Tip nou de identificator care permite o identitate digitală descentralizată și verificabilă.
EBSI	European Blockchain Services Infrastructure	Infrastructura europeană pentru servicii blockchain, promovată de Comisia Europeană.
IdM	Identity Management	Cadru de politici și tehnologii pentru a se asigura că utilizatorii potriviți (într-o întreprindere) au acces adecvat la resursele tehnologice.
WOT	web-of-trust	Este un concept utilizat în PGP, GnuPG și alte sisteme compatibile cu OpenPGP pentru a stabili autenticitatea legăturii dintre o cheie publică și proprietarul acesteia.
EVM	Ethereum Virtual Machine	
PGP	Pretty Good Privacy	Program de criptare care oferă confidențialitate criptografică și autentificare pentru comunicarea datelor.
POW	Proof-of-Work	O formă de dovadă criptografică în care o parte demonstrează altora munca pentru a fi remunerat.
PBFT	Practical Byzantine Fault Tolerance	Un sistem care are un nod primar și noduri secundare. Aceste noduri lucrează împreună pentru a ajunge la un consens, făcând din acest sistem una dintre soluțiile la Problema Generalilor Bizantini.

Scopul intervenției

Definirea problemei

În domeniul transferurilor de proprietate asupra pământului și locuințelor, dar și în tema conexă a utilizării terenurilor agricole sunt observate o serie de probleme, recurente la nivel

mondial:

- Complexitatea proceselor legale care corespund cu aceste transferuri, precum și metoda tradițională prin care acestea iau loc, conduc la dificultăți și întâzieri masive în ceea ce privește verificările și înregistrarea datelor;
- Procesul este foarte dependent de activitatea manuală a unor funcționari publici, ceea ce conduce deseori la greșeli în acte;
- Procesul având o miză majoră și implicând mulți decidenți publici este puternic expus faptelor de corupție;
- Este relativ facil pentru vânzători sau cumpărători necinstiți să fraudeze procesul.
- Menținerea actelor de proprietate, de multe ori sub formă fizică, crește riscul de deteriorare sau pierdere a informațiilor vitale pentru realizarea unor transferuri în condiții de siguranță.

Adițional cu acest subiect este tema utilizării terenurilor agricole. Cu precădere în afara lumii Occidentale (în special în America Latină, Sud-Estul Asiei și Africa), practica arendei pentru exploatarea agricolă este lipsită de înțelegeri formale și se bazează în mod tradițional pe înțelegeri între părți, de multe ori verbale sau lipsite de rigorile tranzacționale ale Occidentului. Această situație permite realizarea unor salturi tehnologice (leapfrogging) pentru a trece direct de la cutumele comunitare la utilizarea tehnologiei blockchain. Problema gestionării terenurilor agricole nu este una localizată, ci reprezintă o situație comună. De pildă, în Africa Sub-Sahariană, aproximativ 90% din terenuri sunt deținute și gestionate cutumiar.

În România, relevanța problemei este în creștere, în contextul unor practici abuzive tot mai des utilizate de proprietarii de terenuri: aceștia refuză să mai încheie contracte formale de arendă cu fermierii care le exploatează terenurile, pentru a beneficia abuziv de subvenții de la *Agencia de Plați și Intervenție pentru Agricultura (APIA)*, deși în practică terenul este lucrat tot de arendași, însă tocmiți la negru.

Obiectivele generale

Obiectivele generale ale intervenției sunt:

- Scăderea cazurilor de fraudă sau erori în cazul transferurilor de proprietăți, prin simplificarea procesului și reducerea factorului uman, supus erorilor sau corupției.
- Reducerea costurilor de administrare ale cărților funciare, prin reducerea necesarului de personal din administrația publică atașată cu acest serviciu public.
- Reducerea timpului necesar pentru procesarea unui transfer de proprietate asupra unor terenuri.

- Reducerea numărului de litigii în ceea ce privește transferul de proprietate asupra terenurilor agricole sau în cazul unor neînțelegeri în cazul utilizării în arendă a terenului.

Obiectivele specifice

Obiectivele specifice ale acestei intervenții sunt:

- Dezvoltarea unui sistem electronic de monitorizare și transfer a proprietății asupra terenurilor, precum și pentru facilitarea, securizarea și transparentizarea proceselor de arendă a terenurilor agricole.
- Conectarea sistemului la actualele baze de date corelate cu acest domeniu.
- Pilotarea sistemului într-un areal geografic controlat, cu colaborarea instituțiilor centrale și locale relevante.
- Analizarea și auditarea rezultatelor pilotului și elaborarea unor concluzii referitoare la eficiența, fezabilitatea și potențialul de extindere al sistemului utilizat în cadrul proiectului-pilot la nivel național pentru gestionarea transferurilor de proprietate și utilizarea terenurilor agricole.

Obiectivele operaționale

Obiectivele operaționale ale intervenției sunt:

- Dezvoltarea infrastructurii tehnologice necesare pentru implementarea proiectului pilot.
- Dezvoltarea unor programe de informare și educare a publicului larg în legătură cu sistemul de transfer electronic al proprietății și gestiunii terenurilor în arendă.
- Dezvoltarea grupurilor de lucru și echipelor de management în cadrul instituțiilor interesate pentru organizarea, implementarea și monitorizarea rezultatelor proiectului pilot.
- Dezvoltarea unei metodologii de evaluare a rezultatelor proiectului pilot în vederea luării unei decizii privind posibila extindere a sistemului la nivel național.

Care sunt granițele de utilizare/aplicabilitate avute în vedere?

Acest document face referire la elaborarea unui proiect pilot pentru testarea cazului de utilizare a tehnologiei blockchain în domeniul urmăririi proprietăților, managementul proprietății asupra terenurilor și utilizarea terenurilor agricole. Doar un număr limitat de dosare vor fi prelucrate prin proiectul pilot, însă acesta va implica și necesita colaborarea tuturor instituțiilor relevante care ar putea fi mai târziu implicate și în implementarea pe scară.

Din punct de vedere tehnic, proiectul pilot va avea ca scop principal evaluarea fezabilității operaționale/financiare, a eficienței și a performanței tehnologiei blockchain într-un astfel de caz de utilizare.

Părțile interesate

Beneficiarii soluției dezvoltate vor fi:

- Agenția Națională De Cadastru și Publicitate Imobiliare (ANCP)
- Oficii de Cadastru și Publicitate Imobiliară (OCPI locale)
- Agenția Domeniilor Statului
- Notari
- Registrul Agricol Național
- Serviciul de taxe și impozite al primăriei locale
- Agenția de Plăți și Intervenție pentru Agricultură (APIA)

Utilizatorii soluției tehnice vor fi:

- Cetățeni români cu domiciliul în țară care sunt fie proprietari de terenuri, fie cumpărători.
- Specialiștii desemnați de către instituțiile publice implicate în organizarea și monitorizarea procesului de transfer a proprietății și a utilizării terenurilor agricole.

Beneficiarii și utilizatorii soluției tehnice dezvoltate pentru implementarea proiectului pilot vor fi consultați permanent în procesul de luare a deciziilor cu privire la soluția propusă. Acest lucru se va realiza prin organizarea de sondaje pe bază de chestionare la care sunt invitate să participe toate părțile interesate. Promovarea chestionarelor se va face prin trimiterea de e-mail-uri către personalul instituțiilor publice vizate, către cetățenii care își declară interesul prin intermediul platformelor online ale instituțiilor care își asumă rolul de promotori ai proiectului, dar și prin rețelele sociale.

Beneficiile estimate

Beneficiile implementării unui sistem de management al proprietății asupra terenurilor și utilizarea terenurilor agricole bazat pe tehnologia blockchain sunt:

- **Sporirea calității datelor și reducerea erorilor umane.** Logica sistemelor bazate pe tehnologii ale registrelor distribuite, precum tehnologia blockchain, în particular este construită în jurul unui sistem de validări criptografice și definirea regulilor prin contracte programabile, auto-executabile. Această logică aplicată în domeniul managementului transferului proprietăților și în utilizarea terenurilor agricole înseamnă o reducere a posibilității de eroare sau fraudă umană, care altminteri reprezintă un factor perturbator considerabil la nivel social.
- **Reducerea timpilor de procesare a tranzacțiilor și a costurilor aferente.** Domeniul operațiunilor funciare este unul notoriu pentru termenii de procesare lungi, care derivă din actuala arhitectură a fluxurilor operaționale necesare pentru a finaliza tranzacțiile, dar și din lipsa digitalizării instituțiilor implicate. Prin utilizarea tehnologiei blockchain, există posibilitatea de a realiza un salt quantic (*leapfrogging*) în calitatea și viteza serviciilor publice oferite, ceea ce ar poziționa România ca un lider regional în implementarea de tehnologii inovatoare, ar crește încrederea cetățenilor în actul de guvernare central și local și ar reduce costurile administrative.
- **Reziliența la atacuri cibernetice și fraudă.** Natura distribuită a nodurilor care validează tranzacțiile implică faptul că un atac cibernetic asupra unui nod izolat nu poate propaga influențe malițioase și modificări false în rețea. Acest aspect crește reziliența întregului sistem și oferă o plasă adițională de verificare împotriva încercărilor de fraudare a sistemului. Adițional, se elimină posibilitatea ca un vânzător să încerce dubla vânzare a unei proprietăți. La fel cum în aplicațiile financiare sistemele tehnologice bazate pe blockchain opresc posibilitatea de a realiza dubla cheltuire a fondurilor, în domeniul trasabilității proprietății, orice tentativă de a duplica operațiuni de vânzare sau de a realiza vânzări fără drepturile de a o face devin automatic imposibile.
- **Transparentizarea procesului electronic de transfer asupra proprietății.** Posibilitatea de a interoga operațiunile într-o bază de date distribuită publică, fără a genera costuri adiționale (și în conformitate cu respectarea datelor cu caracter personal) va permite o creștere a încrederii cetățenilor în activitatea instituțiilor implicate în acest proces.

Factori critici în asociere cu cazurile de utilizare

Factorii critici care ar putea influența sau afecta în mod negativ adoptarea unui sistem de transfer a proprietății și management a terenurilor agricole pe tehnologia blockchain pot fi împărțiți în următoarele categorii:

Factori critici privind cerințele tehnice

- Posibilele vulnerabilități de securitate privind interfațarea cu sistemul actual; cu alte cuvinte, securizarea procesului prin utilizarea tehnologiei blockchain nu promite ca premisele (documentele inițiale) de la care pornesc premisele tranzacțiilor nu sunt falsificate sau nu prezintă alte erori;
- Asigurarea scalabilității la scară națională și a disponibilității continue a sistemului pentru a putea face față la un număr mare de tranzacții într-un interval scurt de timp;
- Capacitatea de procesare și stocare suficientă;
- Absența standardizării limbajelor de programare;
- Imaturitatea generală a tehnologiei blockchain și posibilitatea apariției unor inovații tehnice ulterior dezvoltării sistemului;
- Capacitatea tehnică necesară pentru asigurarea interoperabilității sistemului propus cu alte aplicații și servicii publice online existente sau care urmează a fi dezvoltate.

Factori critici de cost

- Costurile inițiale de dezvoltare și implementare ridicate;
- Costurile legate de mentenanța pe termen mediu și lung a sistemului;
- Costurile utilizării noului sistem în paralel cu cel tradițional cel puțin pentru durata pilotării programului, pentru a se ține cont de accesul scăzut la resurse informatice în România și la nivelul scăzut de competențe digitale în rândul populației;
- Planificarea alocării unor bugete semnificative pe termen lung pentru a asigura succesul și buna funcționare a sistemului din partea mai multor instituții implicate în proiect;
- Costurile asociate cu recrutarea și/sau instruirea personalului instituțiilor responsabile pentru a putea înțelege și opera din logica noului sistem.

Factori critici privind calitatea

- Ușurința de utilizare a sistemului pentru utilizatorii nespecializați;
- Menținerea încrederii utilizatorilor în sistem.

Factori critici privind ușurința execuției

- Existența unui număr suficient de specialiști în dezvoltarea de infrastructuri de date complexe și cu cerințe crescute de securitate și integritate și de interfețe de utilizator care să răspundă tuturor cerințelor funcționale;
- Existența unui număr suficient de persoane din instituțiile implicate în proiect care să aibă o înțelegere suficient de bună a modului de funcționare a sistemului pentru a-l putea utiliza cu succes.

Factori critici sub aspect economic (efecte colaterale negative, costuri de oportunitate)

- Asigurarea finanțării pentru dezvoltarea sistemului tehnic (hardware/software);
- Asigurarea finanțării pentru mentenanța pe termen lung a sistemului tehnic (hardware/software);
- Asigurarea finanțării pentru instruirea personalului specializat din instituțiile interesate;
- Asigurarea finanțării pentru promovarea inițiativei și educarea publicului larg în legătură cu aceasta pentru a ajunge la un număr suficient de mare de utilizatori care să facă fezabilă funcționarea sistemului.

Factori critici sub aspect legal

- Lipsa unor reglementări și cadre legale adecvate pentru acomodarea dezvoltării, testării și implementării (atât în regim de proiect pilot cât și la scară largă) a sistemului de management a proprietății asupra terenurilor și utilizarea terenurilor agricole;
- Asumarea tuturor implicațiilor introducerii acestui sistem, inclusiv a riscurilor și posibilității unui eșec;
- Probleme legate de respectarea reglementărilor privind confidențialitatea și protecția datelor personale ale utilizatorilor (ex. GDPR).

Provocări tehnice în implementarea intervenției

- **Limitări de performanță & scalabilitate.** Una dintre problemele care apar cel mai des în cadrul sistemelor tehnice care folosesc tehnologia blockchain este performanța și viteza de procesare a operațiunilor (tranzacțiilor). Aceste caracteristici sunt strâns legate de tipul de blockchain ales și de mecanismele de consens ale acestuia, care pot face diferența în ceea ce privește viteza de procesare. În cazul unui sistem național pentru transferul proprietății asupra terenurilor agricole și de management ale acestora, sistemul ar trebui construit în așa fel încât să poată susține un număr foarte mare de tranzacții precum și înregistrarea unui volum mare de date, într-o formulă descentralizată, care să poată fi

accesate la viteze rezonabile și fără a se crea congestii în rețea. Prin urmare, proiectul pilot ar trebui să implementeze o arhitectură tehnică scalabilă care să poată fi extinsă la o scară largă în viitor fără să fie afectată performanța și viteza de procesare.

- **Securitate.** Un sistem național pentru transferul proprietății asupra terenurilor agricole și de management ale acestora va trebui să fie securizat corespunzător împotriva tuturor tipurilor de atacuri cibernetice sau încercări de manipulare de date semnalate de specialiști în trecut și descoperite pe parcursul elaborării proiectului. Deși tehnologia blockchain va contribui în mod semnificativ la securitatea sistemului, ea nu va putea răspunde în mod adecvat la toate riscurile de securitate la care un astfel de sistem ar fi expus, deoarece această tehnologie nu poate proteja toate informațiile care circulă pe internet și nu poate face ca serverele și infrastructura să fie complet rezistente la amenințări avansate persistente. De aceea, securitatea sistemului se va număra printre cele mai complicate aspecte ale intervenției și va necesita contribuții și implicare din partea unui număr cât mai mare de specialiști cu experiență cât mai vastă.
- **Consumul de energie.** Tehnologia blockchain incorporează procese care utilizează cantități mari de energie (protocoale, mecanisme de consens, comunicare peer-to-peer, criptare asimetrică, etc). Tipul de blockchain care va fi ales pentru acest proiect va trebui să fie eficient din punct de vedere energetic, fără a face însă compromisuri în ceea ce privește alte caracteristici tehnice care fac tehnologia să fie valoroasă în acest caz de utilizare.
- Alocarea și asumarea de roluri tehnice a tuturor actorilor instituționali implicați în proiect.
- Integrarea cu alte sisteme naționale (ex. identitatea digitală și registrul agricol național, cartea funciara etc.).

Procese curente care ar putea fi afectate de dezvoltarea proiectului

Dezvoltarea și implementarea unui proiect pilot pentru managementul proprietății asupra terenurilor și utilizarea terenurilor agricole nu va avea efecte perturbatoare asupra activității instituțiilor implicate sau asupra cetățenilor care doresc să îl utilizeze, deoarece va rula în perioada pilot în paralel cu sistemul clasic prin care aceste operațiuni sunt realizate. În etapa de scalare există posibilitatea de a exista sincope, ca urmare a necesității de a instrui un număr mare de funcționari publici, însă aceste efecte pot fi mediate prin alocarea corespunzătoare de timp și buget pentru scalarea corespunzătoare a eforturilor.

Obiectivele funcționale

Caracteristicile dorite a fi regăsite în cadrul soluției tehnice/tehnologiei

- *Auditabilitate* – Procesele de audit ar trebui să fie independente de infrastructura tehnică și interfețele software și să fie bazat pe dovezi matematice incontestabile.
- *Accesibilitate* – Sistemul de înregistrare a transferurilor de proprietate și management al terenurilor agricole ar trebui proiectat în așa fel încât să fie cât mai intuitiv, rapid de utilizat și ușor de înțeles și folosit pentru toți potențialii utilizatori, de la personalul instituțiilor publice cu roluri active și până la toți utilizatorii sistemului (părți contractuale cu drepturi asupra respectivei proprietăți).
- *Confidențialitate* – Este posibil să fie menținută confidențialitatea părților într-o tranzacție și în același timp tranzacția în sine să fie interogată anonim pe blockchain și dovedită validitatea ei. Pentru acest deziderat procesul de decriptare ar trebui să implementeze mecanisme criptografice care să prevină corelarea informației decriptate cu cea care rămâne criptată, mai exact să prevină corelarea identității părților cu tranzacția de către publicul neautorizat.
- *Legitimitate* – Înscrierea de tranzacții autorizate prin utilizarea de chei private și semnături digitale calificate va conferi un plus de legitimitate, nu doar în ceea ce privește transferurile de proprietate, dar și în utilizarea pentru arenda terenurilor, prin înscrierea permanentă în blockchain a acordurilor între părți în ceea ce privește exploatarea agricolă a terenurilor.
- *Verificabilitate publică și individuală* – Verificabilitatea înseamnă existența unor procese pentru auditarea tranzacțiilor pentru a garanta corectitudinea acestora. Aceasta ar trebui să poată fi făcută atât de către instituțiile guvernamentale relevante și auditori independenți.
- *Disponibilitate* – sistemul de înregistrare a transferurilor de proprietate și management al terenurilor agricole ar trebui să fie disponibil și funcțional pe întreaga durată de viață a proiectului, fără niciun fel de întrerupere (excluzând eventuale nevoi de mentenanță, acolo unde este strict necesar).
- *Recuperare* – în cazul unor pierderi de date sau întreruperi în transmiterea acestora, sistemul ar trebui să aibă capacitatea de a recupera datele într-un timp cât mai scurt și fără a risca compromiterea acestora.
- *Eficiență* – Tranzacțiile realizate sunt distribuite în registru aproape instantaneu. Nu vor mai exista perioade semnificative de întârziere între diversele etape ale procesului cauzate de transportul fizic de documente, comunicare inter-instituțională defectuoasă sau alte imperfecțiuni ale sistemului tradițional.

- *Rezistență la fraudă sau eroare umană* – Fiecare tranzacție pe blockchain este realizată de către părți cu o cheie privată, care este o semnătură digitală calificată și oferă dovada criptografică că tranzacția provine de la un deținător de drept asupra cheii (și implicit deține drepturile necesare pentru a iniția tranzacția). Pe măsură ce verificările adiționale încep să fie adăugate în fluxul procesului, această funcționalitate va oferi o protecție crescută la orice tentativă de fraudă și împiedică intervențiile exterioare (de pildă realizate de către funcționari sau alți operatori ai sistemului).
- *Scalabilitate* – Sistemul este gândit din start să poată procesa o cantitate de tranzacții corespunzătoare cu scalarea la nivel național al sistemului.
- *Configurabil* – Modificări legislative sau metodologice privind fluxul procedural pot fi codificate în variante noi ale contractelor inteligente, permițând actualizarea sistemului la noile cernite legale, fără a produce o perturbare a sistemului.
- *Trasabilitate* – Fiecare tranzacție și operațiune realizată prin intermediul sistemului este stocată permanent în sistem, oferind un istoric complet al tranzacțiilor care nu mai este supus problemelor de gestionare ale documentelor fizice (se reduc costurile cu stocarea datelor, scade riscul deteriorării arhivei etc.).



Obiectivele de performanță

Caracteristicile de performanță tehnică ale soluției

- **Scalabilitate.** Se vor căuta soluții tehnice de ultimă oră pentru asigurarea scalabilității infrastructurii blockchain. Unul dintre modurile prin care un sistem blockchain poate fi scalat ar fi prin paralelizarea datelor, cunoscută și ca mecanism de *sharding*. Sharding - Într-o rețea tradițională blockchain, tranzacțiile și blocurile sunt validate de toate noduri participante. O abordare a scalării ar fi fragmentarea blockchain-ului, care este numit sharding. Fragmentarea este o tehnică care este utilizată pe scară largă în bazele de date. Date sunt împărțite orizontal în bucăți, fiecare numită un shard (ciob), pentru a oferi un nivel ridicat de performanță. Acesta este însă doar un exemplu de îmbunătățire a scalabilității unei rețele de blockchain; este necesară o investigație detaliată pentru identificarea celei mai bune, mai sigure și mai eficiente abordări pentru cazul specific al proiectului.
- **Securitate.** Sistemul tehnic va trebui să parcurgă un proces complex de dezvoltare și evaluare a măsurilor de securitate de la toate nivelurile și punctele de acces, care să includă evaluarea și certificarea sistemului, elaborarea unei strategii de securitate cibernetică pe termen mediu și lung, teste de sistem concursuri de identificare a problemelor și erorilor, instruire a personalului cu privire la factorii de securitate.
- Alegerea tipului de blockchain utilizat pentru a garanta un echilibru între securitate, performanță și scalabilitate viitoare. În acest sens, ar trebui să se țină cont de factori precum:
 - *Mecanismul de consens* - Tehnica sau mecanismul prin care o tranzacție este propagată, validată și finalizată într-o rețea blockchain este denumită protocol sau algoritm consens. Și acest mecanism de consens este, de asemenea, responsabil pentru realizarea unui echilibru fin între gradul de descentralizare, scalabilitate și securitate pe care îl deține o rețea blockchain. Prin urmare, alegerea mecanismului de consens este direct legată de modul în care funcționează rețeaua blockchain.
 - *Latența rețelei* - Într-o arhitectură distribuită, acesta este cel mai important factor care afectează performanța generală a rețelei. Atunci când o tranzacție urmează să fie validată, aceasta trebuie difuzată către toate nodurile și răspunsul acestora trebuie colectat pentru consens majoritar. Așadar, a avea o lățime de bandă dedicată rețelei ajută la minimizarea întârzierilor rețelei și la îmbunătățirea capacității generale.

- *Infrastructura nodurilor* - Nodurile de blockchain cuprind un motor de execuție și o bază de date care este găzduită local sau în cloud. În absența resurselor de infrastructură dedicate (adică CPU, memorie, hard disk), performanța nodului este cel mai probabil să fie afectată. Astfel, este imperativ ca dimensionarea infrastructurii și alocarea adecvată IOPS (operațiuni de intrare pe secundă) să fie asigurate.
- *Numărul de noduri* - Pe măsură ce numărul de noduri crește, cu atât crește și timpul necesar propagării unei tranzacții și obținerea consensului și asta degradează performanța generală. Ar trebui introduse mecanisme de reducere a cheltuielilor de comunicare și de a permite nodurilor să se bazeze pe istoricul validării unui nod lider și / sau alte noduri.
- *Dimensiunea tranzacției* - Întrucât tranzacțiile sunt transmise prin rețea către toate nodurile, sarcinile utile mai mari necesită mai mult timp pentru replicare între noduri. Deci, una dintre cele mai bune practici este stocarea încărcăturilor utile mari și a documentelor într-un spațiu de stocare offchain (sau utilizând un sistem de stocare descentralizat, precum o bază de date Cassandra sau un sistem extern, precum IPFS) și înregistrarea referințelor acestora pe blockchain.
- *Capacitatea de stocare pe noduri și de adăugare de noi noduri în rețea* - De obicei, rețelele blockchain acceptă depozitele de date pereche cheie-valoare pentru a menține tranzacția și starea registrului integrat. Există o cantitate semnificativă de operațiuni citire-scriere, iar eficiența bazei de date subiacente este un factor cheie în influențarea performanței întregii rețele. Fiecare nod participant la rețeaua blockchain, în formula inițială, trebuie să fie o replică integrală a celorlalte noduri, și să conțină atât registrul imutabil de date cât și datele stocate în baza de date în vederea asigurării disponibilității și reconstrucției informației. Ulterior, se poate testa și varianta în care unele dintre nodurile din rețea să fie de dimensiuni mai mici și să conțină doar informații parțiale relevante pentru nodul respectiv (în funcție de modul de distribuție a rețelei – ex. pe criterii geografice sau demografice). Fiecare nod trebuie însă să conțină/integreze cel puțin următoarele componente informatice, chiar dacă nu sunt replici complete ale nodurilor full: registrul distribuit, baza de date, interfața API și componentele de securitate.
- *Coada de tranzacții* - O rețea blockchain cuprinde mai multe noduri și oferă în mod colectiv o disponibilitate ridicată, dar capacitatea de gestionare a tranzacțiilor fiecărui nod individual determină câte tranzacții vor fi acceptate din aplicațiile client pentru procesare ulterioară. Și acest lucru are un efect direct asupra randamentului general al rețelei.

Elementele de noutate

Ce factori negativi doriți să eliminați în totalitate?

- Riscurile de fraudare ale tranzacțiilor și caracterul verbal al înțelegerilor pentru exploatarea terenurilor, care cauzează diverse probleme administrative și fiscale.

Ce factori negativi doriți să diminuați?

- Lipsa încrederii în instituțiile și autoritățile statului.
- Riscul de erori în procesarea tranzacțiilor.
- Timpii de procesare crescuți în procesarea tranzacțiilor.

Ce elemente doriți să le aduceți peste standardele actuale?

- Interconectarea în sistem a unor serii de actori, precum sistemul bancar.
- Securitatea și posibilitatea de verificare a integrității fiecărei tranzacții.

Ce elemente noi doriți să creați și ce rezolvă acestea?

- Un sistem administrativ online, modern și eficient pentru urmărirea proprietăților, managementul proprietății asupra terenurilor și utilizarea terenurilor agricole

Criteriile de selecție

Dincolo de codarea fluxului procedural în contractele inteligente, un criteriu de selecție vital îl reprezintă proprietățile infrastructurii (*stack-ul* tehnologic) utilizate pentru implementarea proiectului. Metodologia propusă pentru alegerea protocolului blockchain recomandat este de a da note de la 1 la 10 pe o serie de criterii, în conformitate cu necesitățile menționate anterior. O serie de detalii tehnice nu sunt menționate, dar vor fi reflectate în valoarea notelor.

Criteriu	Hyperledger	Ethereum	R3 Corda
Permit implementarea studiilor de caz discutate	Da (10)	Da (10)	Da (9)
Permit arhitectura hibridă	Da (10)	Da (10)	Da (10)
Permite arhitectura cu permisiuni	Da (10)	Da (10)	Da (10)

Permite contracte inteligente	Da (10)	Da (10)	Da (9)
Scalabilitate	10	9	10
Securitate	8	9	10
Interoperabilitate	10	9	8
Open source	Da (9)	Da (10)	Da (8)
Consens	Customizabil (10)	Customizabil (9)	Customizabil (8)
Ecosistem (componente și dezvoltatori)	10	10	7
Limbaje suportate	Go, Java, JavaScript (10)	Go, Python, C++ (protocol), Solidity, Vyper, Yul (contracte inteligente) (10)	Kotlin, Java (9)
Modularizabil	10	10	10
Perspective de dezvoltare	9	10	8
Suportă BaaS	Da cu Hyperledger Cello (open source solution) - 10	Da, prin Microsoft Azure si Consensus - 9	Da, prin Microsoft Azure - 8
Total puncte	136	135	134

Descrierea în detaliu a cazului de referință

La nivel mondial există o serie consistentă de proiecte care utilizează tehnologia blockchain pentru managementul transferului proprietății asupra terenurilor sau pentru facilitarea proceselor de închiriere și exploatare agricolă a terenurilor. Între acestea regăsim:

Ghana

În ciuda faptului că guvernul din Ghana luptă împotriva acestora, corupția și nepotismul din preajma tranzacțiilor de pământuri sunt greu de eradicat. Platforma Bitland înregistrează datele imobilelor și ale proprietarilor în blockchain, oferind un jurnal pe termen lung al acestora, fără să mai poată fi modificat.

În Ghana, peste 80% dintre proprietăți nu au documentația care să le ateste legal proprietarul (Mwanza & Wilkins, 2018).

Deși poate nu pare foarte important ca în zona rurală, un cetățean să nu fie titularul oficial

al pământului, dacă tot îl lucrează – titular sau nu –, calitatea de proprietar de pământ îi permite să ceară împrumuturi de la bănci sau ajutor de la stat pentru activități agricole. De asemenea, rezolvarea problemei lipsei documentelor contribuie la stabilizarea socială, în contextul în care multe terenuri ajung să fie disputate prin violențe.

Banca Mondială listează Ghana cu un indice al dificultății înregistrării terenurilor pe locul 119 din 190 (Banca Mondială, 2018). Rapoarte adiționale descriu lipsa de transparență sau responsabilitate din partea agențiilor guvernamentale implicate în proces.

O inițiativă care abordează tema cu o potențială soluție a fost realizată într-o colaborare între Ministrul Terenurilor și a Resurselor Naturale din Ghana și IBM. Memorandumul de înțelegere a fost semnat în 2018, având ca scop adoptarea unui registru funciar bazat pe tehnologia blockchain, într-un parteneriat pentru implementare semnat între parteneri tehnologici din Ghana și IBM. Această inițiativă construiește peste munca începută în 2014 prin Bitland, un proiect conceput în totalitate de Ghana. Cu toate acestea, ineficiențe în implementarea proiectului încă persistă. Un aspect interesant al soluției implementate este că suportul în sine pentru blockchain, nodurile-calculator, se confruntă cu o problemă majoră în Ghana: lipsa frecventă a electricității. De aceea, Bitland este nevoită să construiască centre unde să găzduiască nodurile, centre care servesc și ca locații de educare a populației despre soluția bazată pe blockchain.

Un factor adițional care împiedică implementarea eficientă a proiectului o reprezintă poziția antagonică pe care autoritățile ghaneze o au asupra criptomonedelor și a altor active criptografice. Comisia de Securitate și Schimburi din Ghana a fost ezitantă să emită o reglementare în ceea ce privește aceste active și a încurajat activ investitorii să stea deoparte de ele. Deși cele două elemente nu sunt direct corelate, apropierea conceptuală a proiectelor bazate pe tehnologia blockchain de activele criptografice constituie un factor care transferă percepția negativă între cele două, îngreunând adopția la nivel național a unor soluții extrem de utile.

India

Similar cu soluția din Ghana, guvernul regional Andhra Pradesh cooperează cu firma suedeză ChromaWay pentru gestiunea titlurilor de proprietate din acest stat indian.

Suedia

Oficiul de cadastru suedez („Lantmäteriet”) se bazează pe blockchain pentru a avea și duce mai departe un jurnal clar al tranzacțiilor imobiliare din țară – nu titlurile de proprietate în sine. Mai mult, soluția a fost dezvoltată utilizând contractele inteligente („smart contracts”), în vederea menținerii compatibilității cu cerințele europene GDPR. Din acest motiv, contractele propriu-zise se păstrează offline.

Deși procesul de transfer imobiliar funcționează destul de bine în Suedia, autoritățile au

fost interesate să afle dacă ar putea fi îmbunătățit folosind tehnologia blockchain, în special, făcându-l mai rapid, mai transparent și mai puțin costisitor. În acest scop, Lantmäteriet a colaborat cu băncile, autoritățile fiscale, dezvoltatorii de blockchain și alte părți interesate pentru a cartografia procesul de transfer imobiliar pe blockchain (nu transferul titlului) și ulterior a folosit această hartă pentru a completa o dovadă de succes a conceptului pentru un astfel de transfer.

Soluția a fost un blockchain privat dezvoltat special pentru proiect. Scopul a fost de a asigura verificarea tehnică a datelor și a tranzacțiilor. Nodurile nu votează tranzacțiile, ci se ocupă doar de respectarea protocolului. Stimularea de a crea blocuri constă în modelele de afaceri ale părților și în cerințele legale care conduc procesul de vânzare a bunurilor imobile până la punctul în care tranzacția este înregistrată în registrul funciar.

Utilizatorii platformei folosesc semnături electronice (cum ar fi Telia ID) pentru a semna documente online în motorul de contract. Contractele sunt apoi validate de nodurile din rețea și stocate offline într-o bază de date separată. După ce au fost realizate și validate toate măsurile necesare, factura de vânzare merge la registrul funciar (care nu se află în blockchain). În timp ce contractele sunt stocate în afara lanțului – din motive GDPR, printre altele – anumite date personale care trebuie făcute publice într-o tranzacție imobiliară din Suedia sunt publicate în primele etape.

Deși în prezent nu există planuri de implementare a sistemului într-un cadru live – un contract de vânzare a proprietății în Suedia trebuie, prin lege, să fie pe hârtie și nu digital – proiectul a câștigat multă atenție ca un caz de test pentru utilizarea tehnologiei blockchain în guvern, precum și o sursă de învățare importantă.

Progresul realizat și economiile generate sunt remarcabile, oferind un grad semnificativ de validare a conceptului într-o țară dezvoltată. Se estimează că peste 100 milioane de euro se pot economisi anual prin eliminarea documentelor pe suport de hârtie, reducerea fraudei și creșterea vitezei tranzacțiilor, conform firmei de consultanță Kairo Future, care este de asemenea implicată în proiect.

Marea Britanie

Oficiul de cadastru britanic („HM Land Registry”) colaborează cu firma de software Methods, pentru a dezvolta o soluție blockchain pentru înregistrarea tranzacțiilor imobiliare și a titlurilor de proprietate.

Estonia

Estonia, pionieră în domeniul blockchain, a lansat „Succession Registry” (en. Registrul de succesiune) în 2012. De altfel, Estonia a trecut o mare parte din procesele guvernamentale nu doar în mediul digital, ci și pe blockchain. Până în prezent, peste 1 milion de imobile și terenuri au fost înregistrate în sistemul estonian. Corelat cu sistemul de informații geografice (GIS), registrul funciar electronic livrează o vizualizare geografică în timp real a proprietăților, ceea ce

conferă avantaje multor provideri de servicii care necesită localizare (curierat, servicii poștale, imobiliare etc.).

Este estimat ca utilizarea acestui sistem digital a redus timpul de procesare pentru tranzacțiile cu proprietăți **de la 3 luni la 8 zile**.

Georgia

În 2016, guvernul din Georgia a inițiat o colaborare cu firma Bitfury, în privința trecerii înregistrărilor funciare pe sistem blockchain. Un an mai târziu, l-a urmat guvernul ucrainean, cu sistemul Exonum, tot pentru imobiliare.

O analiză academică realizată în 2019 (Shang & Price, 2019) subliniază importanța calității datelor în acest proces și de asemenea a unei vaste implicări cu publicul ținta. În 2018, Georgia a înregistrat peste 1,5 milioane de titluri de proprietate pe sistemul lor baza pe blockchain, validând scalabilitatea unui asemenea sistem.

Acest proiect este parte dintr-o inițiativă mai largă de a atrage investitori instituționali și a limita corupția. Indicatori cheie precum Indicele Percepției asupra Corupției continuă să arate o evoluție pozitivă a Georgiei din acest punct de vedere, nu în mică măsură ca urmare a implementării unor asemenea proiecte ce utilizează tehnologia blockchain. De asemenea, eficacitatea social-económica a unor asemenea soluții este validată și de studii ale Băncii Mondiale, ce indică o creștere economică constantă și o menținere a șomajului la un nivel scăzut.

În comparație cu proiectul din Ghana, este foarte interesant de remarcat importanța componentei de educație publică în eficiența proiectelor blockchain implementate. În cazul Georgiei, succesul implementării contrastează cu realizările din Ghana ca urmare a unei campanii eficiente de comunicare publică cu cetățenii, precum și datorită calității datelor utilizate în proces.

Acest proiect a evidențiat de asemenea avantajele financiare ale implementării unui sistem bazat pe tehnologia blockchain. **Dacă înainte de implementare părțile plăteau la notar între 50 și 200 USD per operațiune, mutarea procesului în blockchain a scăzut costurile de procesare a tranzacției la doar 10 cenți.**

SUA, Zambia, Rwanda, Mexic și Saint Kitts and Nevis

Încă din 2018, firma Medici Land Governance a semnat acorduri cu guvernele din Zambia, Rwanda, Mexico, Saint Kitts and Nevis, pentru menținerea de sisteme blockchain în scopul securizării titlaturilor și tranzacțiilor pământurilor din aceste țări. Desigur, în SUA, sistemul funcționează doar în unele state, notabile fiind Vermont și Delaware.

Elveția

Digitalizarea pe blockchain a registrului de pământuri elvețiene a început din 2018, bineînțeles în orașul elvețian Zug. Sistemul oferă și posibilitatea diverșilor actori – antreprenori,

avocați, bănci, notari și alții – să-și digitalizeze fluxul de lucru, folosindu-se de facilitățile oferite prin sistemul blockchain guvernamental.

Rusia

În cadrul programului „Economia digitală” lansat în 2017, Rusia dorește trecerea registrului de cadastru pe blockchain. Biroul federal de înregistrare, cadastru și cartografiere (Rosreestr) a fost primul care a înregistrat o tranzacție imobiliară în cadrul sistemului.

Japonia

Diverse entități publice și private din Japonia aveau deja propriile baze de date imobiliare, când, în 2017, statul a decis unificarea și protejarea lor prin intermediul tehnologiei blockchain. Acest proiect este extrem de binevenit în contextul în care aproximativ 20% din terenul agricol nu avea proprietarul în viață, deoarece procedura de succesiune nu fusese pornită.

Brazilia

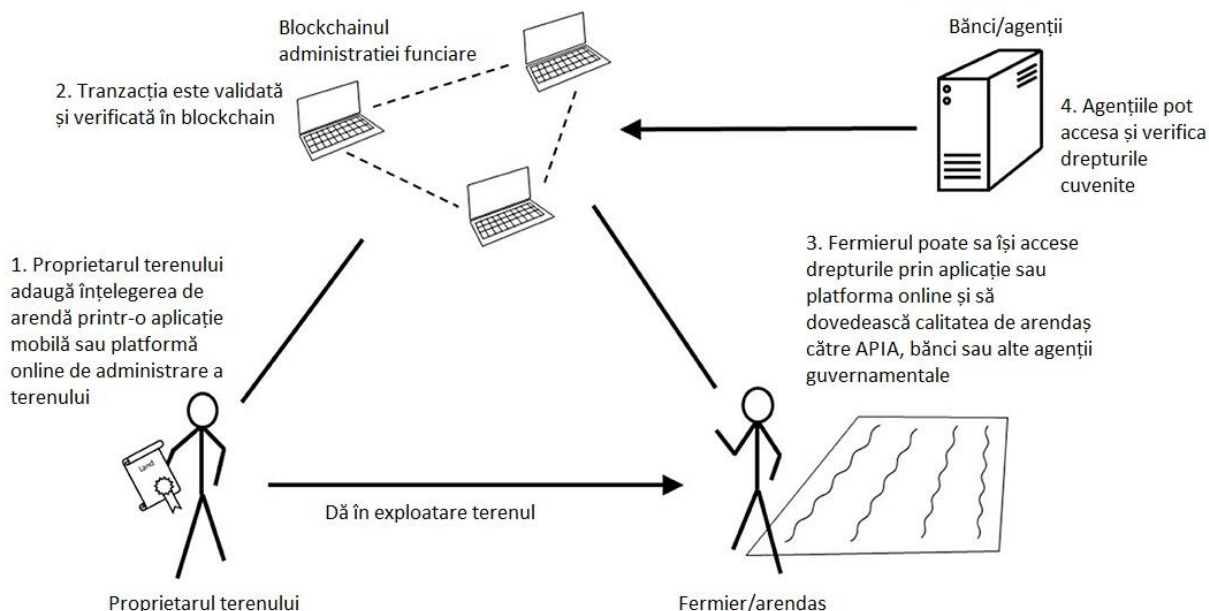
Din 2017, primăriile din Pelotas și Morro Redondo colaborează cu firma americană Ubiquity pentru trecerea informațiilor de proprietate imobiliară pe blockchain. Din cauza corupției și a lipsei unui for central pentru registrul titlurilor de proprietate, fraudă era răspândită, însă proiectul-pilot a avut succes și este în curs de extindere pentru toată țara. Acesta a fost primul proiect de acest fel în America Latină.

Malta

Nu doar transferurilor de proprietate fac obiectul tranzacțiilor utilizând sisteme bazate pe tehnologia blockchain. Susținând potențialul de a utiliza tehnologia pentru managementul utilizării terenurilor agricole, Malta a implementat un sistem prin care orice contract de închiriere va fi înregistrat pe blockchain, în paralel cu modificări ale legilor ce guvernează acest domeniu. Inițiativa asigură securitatea procesului, previne alterarea înregistrărilor și asigură faptul că doar persoanele autorizate pot să acceseze înregistrările.

Opțiuni de îmbunătățire

Schema propusă în cadrul particular al problemei înregistrării arendei în România are următoarea arhitectură logică:



În ceea ce privește arhitectura unui sistem pentru urmărirea transferurilor de proprietate, arhitectura prezentată de sistemele implementate în Suedia sau Georgia este suficient de eficientă și clară pentru a nu fi nevoie de o adaptare la nevoile locale.

Analiza comparativă

Comparație între cele mai cunoscute platforme blockchain din perspectiva scalabilității:

Framework	Year Release	Generation Time	Hash Rate	Transactions Per Sec	Cryptographic Algorithm	Mining Difficulty	Power Consumption	Reward/Block	Scalability
Bitcoin	2008	9.7 min	899.624 Th/s	4.6 max 7	ECDSA	High (around 165,496,835,118)	Very High	25 BTC	Very Low
Ethereum	2015	10 to 19 s	168.59 Th/s	15	ECDSA	High (around 10,382,102)	High	5 ether	Low
Hyperledger Fabric	2015	10 ms	NA	3500	ECC	No mining required	Very Low	No built-in cryptocurrency	Good
Litecoin	2011	2.5 min	1.307 Th/s	56	Scrypt	Low 55,067	Moderate	25 LTC	Moderate
Ripple	2012	3.5 s	NA	1500	RPCA	No mining required	Very Low	Base Fee	Good
Dogecoin	2013	1 min	1.4 Th/s	33	Scrypt	Low 21,462	Low	10,000 Doge	Low
Peercoin	2012	10 min	693.098 Th/s	8	Hybrid	Moderate (476,560,083)	Low	67.12 PPC	Low

Constrângeri privind implementarea

Cu toate că potențialul pentru utilizarea tehnologiei în domeniul urmăririi proprietăților, managementul proprietății asupra terenurilor și utilizarea terenurilor agricole este evidențiat de multitudinea de proiecte implementate sau în curs de implementare care prezintă avantaje dovedite, este necesar să fie luate în calcul și limitările pe care această implementare le prezintă:

- a. Soluția blockchain nu este o rezolvare magică pentru problemele de contestare a proprietății, dar nici pentru erori de introducere a datelor de către factorul uman. Aceste probleme țin de aspecte instituționale și legale ale administrării terenurilor. Cu alte cuvinte, calitatea datelor utilizate la începutul fluxului într-un proces bazat pe tehnologia blockchain sunt determinante pentru utilitatea proiectului. În acest sens, litigiile existente reprezintă un impediment major în eficientizarea sistemului, care nu pot fi rezolvate prin utilizarea tehnologiei. Privind jumătatea plină a paharului, odată implementat, un asemenea sistem ar elimina sau limita masiv existența unor asemenea litigii, cel puțin din perspectiva existenței dovezilor privind trasabilitatea proprietății și a altor sarcini pe respectivul teren.
- b. Cu toate că sistemul este imutabil și protejat criptografic, există în continuare vulnerabilitatea ca unui actor ce deține chei de securitate să îi fie furate acestea. În acel moment, sistemul este expus cibernetice. De aceea, factorul educațional este critic, pentru a educa utilizatorii în gestiunea cheilor private. Un alt factor care trebuie luat serios în calcul este auditarea contractelor inteligente, deoarece potențiale porțițe logice (*loopholes*) în acestea pot vulnerabiliza sistemul împotriva exploatării malițioase de către hackeri.
- c. Utilizarea tehnologiei blockchain ca arhivă este însă nedovedită pe durate extrem de lungi de timp. Deși o arhivă fizică bine întreținută poate să dureze sute de ani, linkuirea datelor *offchain* și stocarea pe servere descentralizate pot reprezenta probleme de stocare în asemenea orizonturi de timp. Pentru continuitatea generațională a datelor, stocarea lor depinde de factori instituționali, umani și tehnologici.
- d. Natura digitală a tranzacțiilor prezintă riscul de a elimina din sistem părțile cu o alfabetizare digitală redusă sau inexistentă. Pentru a nu deveni un factor discriminator în acest sens, este nevoie ca implementarea unui asemenea sistem să fie corelată cu o campanie masivă și susținută de educare nu doar a populației ci și a funcționarilor publici care vor interacționa cu sistemul.

Resurse tehnice pentru implementare

Resursele tehnice necesare pentru implementarea unui sistem de urmarire a proprietăților, managementul proprietății asupra terenurilor și utilizarea terenurilor agricole bazat pe blockchain în regim de proiect pilot se împart în două categorii: resurse hardware și resurse software.

Componentele minime pe care acest sistem va trebui să le includă sunt următoarele:

- Resurse de stocare și procesare (hardware) – cloud sau on-premise:
 - Servere pentru baze de date tradiționale;
 - Servere cu rol de noduri blockchain;
 - Infrastructură middleware (componente care asigură conectarea bazelor de date cu motorul/motoarele blockchain utilizate și sincronizarea datelor între acestea).
- Interfețe software distincte pentru următoarele categorii de utilizatori:
 - Administratori (personal al instituției/instituțiilor cu rol central în dezvoltarea și gestionarea sistemului);
 - Instituții secundare (instituții cu rol secundar în desfășurarea proiectului pilot, al căror personal va avea diverse roluri în cadrul ecosistemului tehnic);
 - Cetățeni, în rolul de părți în tranzacții în domeniul funciar.

Resurse umane pentru implementare

Planificarea, dezvoltarea și implementarea unui sistem de urmarire a proprietăților, managementul proprietății asupra terenurilor și utilizarea terenurilor agricole bazat pe blockchain în regim de proiect pilot și evaluarea rezultatelor acestui pilot în vederea posibilității de a extinde sistemul la nivel național sunt activități care vor necesita implicarea unui număr mare de specialiști și reprezentanți ai instituțiilor publice relevante.

Numărul și categoriile de specialiști pe care un astfel de proiect îl necesită pot fi specificate cu mai multă acuratețe după o analiză foarte detaliată a proiectului, însă se pot menționa deja o serie de domenii și subiecte în care sunt necesare aptitudini avansate pentru dezvoltarea proiectului:

- Arhitecturi software
- Infrastructuri hardware
- Analiză de business
- Tehnologia blockchain/DLT
- Securitate cibernetică
- Criptografie
- Design UX/UI, design grafic, design web/mobile
- Dezvoltare aplicații web, mobile
- Mentenanță sisteme informatice – hardware & software
- Înțelegerea fluxurilor de documente în domeniul transferului de proprietate și a managementului terenurilor agricole

- Tehnologie și inovație în sectorul public
- Educație și comunicare publică
- Managementul schimbării
- Audit sisteme tehnice
- Analiză de impact.

Resurse financiare pentru implementare

Implementarea proiectului pilot pentru introducerea unui sistem de urmarire a proprietăților, managementul proprietății asupra terenurilor și utilizarea terenurilor agricole bazat pe tehnologia blockchain va implica o serie de costuri semnificative pentru care instituția/grupul de instituții responsabile cu implementarea vor trebui să identifice surse de finanțare stabile și sustenabile. Proiectarea costurilor poate fi făcută separat pentru proiectul pilot și pentru posibila extindere a acestuia la scară largă, însă cele două dimensiuni ale proiectului trebuie bine corelate astfel încât pilotul să reprezinte o resursă utilă din punct de vedere al estimării costurilor unui proiect la nivel național.

Categoriile de costuri asociate cu proiectul pilot sunt următoarele:

- Costuri de analiză de business/cercetare/elaborare proiect tehnic;
- Costuri de dezvoltare și licențe software;
- Costuri de infrastructură hardware;
- Costuri de integrare cu sisteme existente;
- Costuri pentru resurse umane;
- Costuri de testare;
- Costuri de mentenanță;
- Costuri de monitorizare/evaluare.

Resurse logistice pentru implementare

Din punct de vedere logistic, pentru dezvoltarea și implementarea proiectului va fi nevoie de resurse precum dispozitive de lucru adecvate din punct de vedere al performanței (PC, laptop) pentru toți actorii implicați în faza de dezvoltare a proiectului, dar și de resurse și materiale educaționale și informative pentru utilizatorii finali ai soluției (personal al instituțiilor, cetățeni).

Riscuri și planuri de contingență

Riscuri de finanțare

- Reducerea/eliminarea finanțării pentru implementarea unui proiect sau ulterior, în implementarea pe scară largă în toate tipurile de alegeri – risc mediu.

Riscuri legislative

- Incompatibilitatea gestiunii electronice a managementul proprietății asupra terenurilor și utilizarea terenurilor agricole cu legislația din România – risc ridicat.

Riscuri ale costurilor de întreținere

- Reducerea/eliminarea finanțării pentru mentenanța pe termen lung a sistemului de management al proprietății asupra terenurilor și utilizarea terenurilor agricole – risc mediu.

Riscuri de ocupare

- Lipsa de specialiști care să dezvolte, testeze, administreze și întrețină sistemul – risc mediu.
- Lipsa personalului instruit în modul de operare a sistemului în cadrul instituțiilor relevante – risc mediu.
- Un număr insuficient de membri ai publicului larg care să fie dispuși să participe în proiectul pilot – risc scăzut.

Riscuri operaționale

- Întârzieri față de planul de execuție pentru dezvoltarea componentelor software sau hardware – risc ridicat.
- Probleme de disponibilitate a specialiștilor implicați în proiect sau lipsa unui număr suficient de specialiști (manageri de proiect, specialiști hardware/software, alte resurse umane importante) – risc mediu.
- Întreruperi în serviciile de electricitate sau internet care să pericliteze buna funcționare a sistemului – risc scăzut.

Riscuri de planificare

- Estimarea necorespunzătoare a duratei de lucru pentru diferite faze ale proiectului – risc ridicat.

Riscuri de schimbare a opțiunilor politice (riscuri decizionale)

- Opreire/inconsistență a finanțării pe termen lung a proiectului – risc ridicat.
- Absența unui climat politic favorabil pentru dezvoltarea/extinderea/mentenanța proiectului – risc ridicat.

Riscuri legate de procedurile de achiziții publice

- Dificultăți și neclarități în elaborarea documentației necesare pentru demararea achizițiilor publice (caietelor de sarcini), în special datorită numărului mare de părți interesate și de componente ale sistemului – risc mediu.
- Lipsa furnizorilor suficient de experimentați/specializați pe cerințele unui sistem de urmarire a proprietăților, managementul proprietății asupra terenurilor și utilizarea terenurilor agricole bazat pe tehnologia blockchain – risc mediu.
- Întârzieri cauzate de potențialele contestații la atribuirea unor contracte de achiziții publice care ar putea prelungi durata de dezvoltare a sistemului astfel încât proiectul pilot să nu se poată desfășura în condiții optime conform planului – risc mediu.

Riscuri reputaționale (influența opiniei publice)

- Orice problemă de funcționare a sistemului, în cadrul proiectului-pilot, ar putea genera o respingere a acestuia din partea opiniei publice, chiar dacă problemele identificate ar putea fi corectate până la implementarea pe scară largă – risc ridicat.

Riscuri ale schimbărilor tehnologice

- Deși a apărut în urmă cu mai mult de un deceniu, tehnologia blockchain încă e în plină dezvoltare, atât din punct de vedere tehnic și al performanței, cât și din punct de vedere al aplicabilității și fezabilității în diverse cazuri de utilizare. Prin urmare, unul dintre riscurile asociate tehnologiei blockchain este acela ca un sistem dezvoltat în următorii 3-5 ani să ajungă să fie perimat și să nu mai facă față cerințelor și așteptărilor de performanță, eficiență și scalabilitate la foarte puțin timp de la lansare – risc mediu-ridicat.
 - Sistemul de urmarire a proprietăților, managementul proprietății asupra terenurilor și utilizarea terenurilor agricole bazat pe tehnologia blockchain ar trebui construit în așa fel încât să poată fi actualizat și îmbunătățit cu efort tehnic, operațional și financiar minim, inclusiv să ofere posibilitatea de schimbare a soluției blockchain utilizate.

Riscuri ale volumului de activitate estimat

- O rată de utilizare/adopecție scăzută a sistemului care să îl facă inefficient din punct de vedere financiar și operațional – risc ridicat.

- În cazul în care autoritățile naționale decid că este oportună extinderea sistem de urmarire a proprietăților, managementul proprietății asupra terenurilor și utilizarea terenurilor agricole în urma rezultatelor pilotului, va fi necesară impunerea unor praguri minime de utilizare care vor trebui atinse odată cu primele utilizări pe scară largă ale sistemului pentru ca autoritățile să poată decide dacă acesta rămâne sau nu funcțional pe termen lung și un plan de contingență pentru scoaterea din uz a sistemului în cazul în care nu se dovedește a fi sustenabil.

Interacțiunea cu alte sisteme tehnice

Sistemul va interacționa cu următoarele aplicații:

- Sistemul informatic de gestionare a registrului agricol național;
- Sistemele electronice ale ANCPI;
- Sistemele electronice ale Direcțiilor de Taxe și Impozite Locale;
- Sistemele electronice ale Agenției de Plăți și Intervenție pentru Agricultură (APIA);
- Sistemul Național de Interoperabilitate – lansat în noiembrie 2021, posibilitate de extindere pentru mai multe instituții/servicii publice în următorii ani;
- Platforma Software Centralizată pentru Identificare Digitală (PSCID) – conform Autorității pentru Digitalizarea României, PSCID va reprezenta un punct unic de intrare pentru acces la toate platformele de servicii publice – planificat pentru finalizare în 2023.

Diagrama pentru implementare

Stadiile de implementare ale sistemului de urmarire a proprietăților, managementul proprietății asupra terenurilor și utilizarea terenurilor agricole, de la conceptualizarea inițială și până la implementarea proiectului pilot vor fi definite folosind conceptul de Technology Readiness Level (TRL) utilizat la nivelul Comisiei Europene.

Activitate		Rezultat	An implementare									
			1	1, 5	2	2, 5	3	3, 5	4	4, 5	5-7	8
Pregătirea proiectului pilot și a	2 ani: Proiectare, dezvoltare, implementare	Sistem prototip verificat										

Activitate			Rezultat	An implementare										
				1	1, 5	2	2, 5	3	3, 5	4	4, 5	5-7	8	10
procedurilor de evaluare/analiză	back-end și front-end		(TRL4 [Eroare! Fără sursă de referință., Eroare! Fără sursă de referință.])											
	0,5 ani: Formare personal și teste beta	0,5 ani: Formare personal, training pe sistemul dezvoltat	Tehnologie validată în mediu relevant (TRL5)											
		0,5 ani: Testare beta de către utilizatori	Tehnologie demonstrată în mediu relevant (TRL6)											
	1 an: „Smoke testing”, ucenic non-producție		Sistem model și prototip demonstrate în mediu operațional (TRL7)											
	0,5 ani: Analiză comparativă rezultate sistem nou/sisteme existente de referință		Sistem complet și validat (TRL8)											

Activitate	Rezultat	An implementare										
		1	1, 5	2	2, 5	3	3, 5	4	4, 5	5-7	8	10
1 an: Optimizare/eliminarea defectelor raportate de utilizatori	Sistem validat în mediul operațional (TRL9)											
Operaționalizarea sistemului de urmărire a proprietăților, managementul proprietății asupra terenurilor și utilizarea terenurilor agricole pentru desfășurarea proiectului pilot	Desfășurarea proiectului pilot											
	Analizarea și evaluarea rezultatelor pilotului											

Metodologia de management a proiectului și modelul de dezvoltare

Proiectul introducerii unui sistem de urmărire a proprietăților, managementul proprietății asupra terenurilor și utilizarea terenurilor agricole bazat pe tehnologia blockchain în România este format din mai multe categorii de activități, iar fiecare dintre aceste părți poate fi considerată un proiect în sine din punct de vedere al disciplinei managementului de proiect: software, hardware, logistică, aliniere legislativă, campanii de educație și informare. Fiecare categorie de activități va trebui să fie gestionată de una sau mai multe instituții diferite, care vor aplica metode de management și dezvoltare cel mai probabil diferite pentru a ajunge la rezultatele dorite, însă această variantă este preferabilă aplicării unei metodologii rigide de-a

lungul întregului proiect care să fie impusă tuturor instituțiilor și entităților implicate, fapt care ar putea duce la blocaje din cauza lipsei de experiență sau de personal specializat în aplicarea metodologiei respective. Evaluarea metodelor de management și a rezultatelor acestora în diferitele componente ale proiectului pilot poate fi efectuată odată cu evaluarea generală a pilotului, iar eventualele modificări vor putea fi aplicate când (și dacă) proiectul pilot va fi extins pe scară largă ulterior.

Cu toate acestea, este însă nevoie și ca o instituție cheie să preia conducerea întregului proiect pilot pentru a urmări toate aceste subproiecte ale celorlalte instituții, astfel încât proiectul pilot să poată fi pregătit corespunzător din toate punctele de vedere și să se poată desfășura în condiții optime. Ținând cont de contextul legislativ și de experiența instituțională, cea mai potrivită instituție care să supravegheze întregul proiect ar fi Agenția Națională De Cadastru și Publicitate Imobiliare (ANCPPI).

Precondiții și factori critici pentru succes

Pentru ca proiectul să poată avea succes, este nevoie ca următoarele precondiții să fie îndeplinite:

- Legislație care să permită implementarea unui sistem electronic de urmărire a proprietăților, managementul proprietății asupra terenurilor și utilizarea terenurilor agricole bazat pe tehnologia blockchain;
- O colaborare continuă între instituțiile implicate în proiect, indiferent de posibilele schimbări care ar putea avea loc la nivel politic;
- Efectuarea unei analize ex-ante extrem de detaliate în legătură cu proiectul, care să ia în considerare toate direcțiile potențiale de impact ale acestuia, atât la nivel tehnic, cât și la nivel politic, social, economic. Planul de dezvoltare și implementare care va reieși din analiză va trebui să detalieze cu exactitate obiective generale și intermediare, resurse umane, tehnice și financiare necesare pentru fiecare fază a proiectului, calendar de implementare, plan de lansare etc.

Indicatori pentru monitorizare și evaluare

Indicatori de ieșire:

- Sistemele informatice create pentru implementarea proiectului pilot, pe baza cărora se poate construi în continuare pentru ca sistemul să fie extins la nivel național.
- Procesul de evaluare a proiectului pilot le va permite autorităților statului să facă

observații și să tragă concluzii importante nu numai despre atingerea obiectivelor proiectului în sine, ci și despre calitatea și eficiența colaborării dintre mai multe instituții-cheie ale statului, cu implicații pentru alte proiecte și planuri viitoare de colaborare (fie aspecte pozitive ale experienței, fie constatări importante cu privire la aspectele care au nevoie de îmbunătățiri majore). În baza acestor observații făcute prin intermediul procesului de evaluare a proiectului pilot, autoritățile vor putea decide și asupra continuării sau abandonării implementării sistemului la nivel național.

Indicatori de rezultat:

- Un proiect pilot pentru implementarea unui sistem de urmarire a proprietăților, managementul proprietății asupra terenurilor și utilizarea terenurilor agricole bazat pe tehnologia blockchain care se desfășoară cu succes, fără incidente sau probleme majore, ar putea determina extinderea pe scară largă a acestui sistem, oferind un acces mai bun cetățenilor la servicii publice rapide, ieftine și eficiente.

Indicatori de impact:

- O eficientizare a procesului de transfer al proprietăților și de gestiune a terenurilor agricole ar eficientiza activitatea economică în sectorul agricol și nu numai, cu beneficii la nivelul întregii societăți și a economiei naționale.
- Un sistem de urmărire a proprietăților, managementul proprietății asupra terenurilor și utilizarea terenurilor agricole bazat pe blockchain care funcționează conform standardelor impuse de contextul național și internațional ar poziționa România ca lider în domeniile guvernării digitale, inovației și tehnologiei, iar țara ar putea reprezenta un exemplu și pentru alte state care sunt interesate de implementarea unui asemenea sistem.

Referințe bibliografice

2. Desiree Daniel and Chinwe Ifejika Speranza, *The Role of Blockchain in Documenting Land Users' Rights: The Canonical Case of Farmers in the Vernacular Land Market* - <https://www.frontiersin.org/articles/10.3389/fbloc.2020.00019/full>
3. Krishnapriya S, Greeshma Sarath, *Securing Land Registration using Blockchain*, <https://www.sciencedirect.com/science/article/pii/S1877050920311649>
4. Daniel, D., Sutherland, M., and Ifejika Speranza, C. (2019). *The role of tenure documents for livelihood resilience in Trinidad and Tobago*. Land Use Policy 87:104008. doi: 10.1016/j.landusepol.2019.05.027

5. Nasarre-Aznar, S. (2018). *Collaborative housing and blockchain*. Administration 66, 59–82. doi: 10.2478/admin-2018-0018
6. Maria Kaczorowska, *Blockchain-based Land Registration: Possibilities and Challenges* <https://journals.muni.cz/mujlt/article/view/11622/10849>
7. Rizzo, P., 2015. Coindesk. [Online] <https://www.coindesk.com/debate-factom-land-title-honduras>.
8. Mwanza, K. & Wilkins, H., 2018. Reuters.com. [Online] <https://www.reuters.com/article/us-africa-landrights-blockchain/africanstartups-bet-on-blockchain-to-tackle-land-fraud-idUSKCN1G00YK>
9. Reese, F., 2017. Coindesk. <https://www.coindesk.com/blockchain-land-registry-solution-seeking-problem>
10. P Singh 2020 IOP Conf. Ser.: Earth Environ. Sci. 614 012055, <https://iopscience.iop.org/article/10.1088/1755-1315/614/1/012055/pdf>
11. Kazi Masudul Alam, J.M. Ashfiqur Rahman, Anisha Tasnim, Aysha Akther, *A Blockchain-based Land Title Management System for Bangladesh*, Journal of King Saud University - Computer and Information Sciences, 2020, ISSN 1319-1578, <https://www.sciencedirect.com/science/article/pii/S1319157820304912>
12. Aitken, R. (2016). *Bitland's African Blockchain Initiative Putting Land On The Ledger*. <https://www.forbes.com/sites/rogeraitken/2016/04/05/bitlands-african-blockchain-initiative-putting-land-on-the-ledger/?sh=7545c04d7537>
13. De, N. (2017). *The Indian state of Andhra Pradesh is working with startup ChromaWay on a land registry pilot that uses blockchain to track the ownership of property*. <https://www.coindesk.com/andhra-pradesh-partners-with-chromaway-to-develop-blockchain-land-registry>
14. Kim, C. (2018). *Sweden's land registry authority and a group of participating banks, businesses and startups have completed the third phase of an ongoing blockchain pilot*. <https://www.coindesk.com/sweden-demos-live-land-registry-transaction-on-a-blockchain>
15. HM Land Registry. (2018). *HM Land Registry to explore the benefits of blockchain*. <https://www.gov.uk/government/news/hm-land-registry-to-explore-the-benefits-of-blockchain>
16. (2020). *KSI blockchain in Estonia*. <https://e-estonia.com/wp-content/uploads/2020mar-faq-ksi-blockchain-1-1.pdf>
17. Perez, E. (2019). *Blockchain Registers for Recording Ownership Rights Around the World*. <https://cointelegraph.com/news/blockchain-registers-for-recording-ownership-rights-around-the-world>
18. Jackson, M. (2019). *Real Estate Projects in Russia will Now Use Blockchain Technology for*

Obvious Benefits. <https://www.financeknown.com/real-estate-projects-in-russia-will-now-use-blockchain-technology-for-obvious-benefits/>

19. IBM. (2019). *French National Council of Clerks of Commercial Courts announce the deployment of a blockchain network developed by IBM, to streamline the management of commercial and corporate registry.* <https://newsroom.ibm.com/2019-03-14-French-National-Council-of-Clerks-of-Commercial-Courts-announce-the-deployment-of-a-blockchain-network-developed-by-IBM-to-streamline-the-management-of-commercial-and-corporate-registry>
20. Nikkei. (2017). *Japan to tidy up scattered property records.* <https://asia.nikkei.com/Markets/Property/Japan-to-tidy-up-scattered-property-records>