

ASPECTE PRACTICE DE APLICABILITATE ALE CONTRACTULUI SMART BAZAT PE SISTEMEA BLOCKCHAIN

PRACTICAL ASPECTS OF APPLICABILITY OF THE SMART CONTRACT BASED ON THE BLOCKCHAIN SYSTEM

Cara-Rusnac Aliona, Doctor în drept, Conferențiar Universitar, Departamentul Drept Privat, Facultatea de Drept, Universitatea de Stat din Moldova, ORCID 0000-0002-2026-2206

Abstract: Over the years, a number of applications of blockchain and smart contracts have been proposed in a variety of scenarios and sectors. Such applications use the blockchain to record different types of assets, from financial to public (e.g. vehicle registrations), semi-public (e.g. university degrees) and private (e.g. wills), as well as intangible (e.g. coupons) and tangibles (e.g. e-hotel). room keys) active.

In the following subsections, an overview of the developed/designed applications is reported, grouping them according to their sector and context. The objective here is to provide the reader with a list of existing, to be developed, or potential applications of blockchain and smart contracts to help them understand the huge impact this technology could have on society

Keywords: *contract smart, blockchain, asigurări, industrie, aviație*

De-a lungul anilor, au fost propuse o serie de aplicații de blockchain și contracte smart într-o varietate de scenarii și sectoare. Astfel de aplicații folosesc blockchain-ul pentru a înregistra diferite tipuri de active, de la financiare la publice (de exemplu, registre de vehicule), semipublice (de exemplu, diplome universitare) și private (de exemplu, testamente), precum și intangibile (de exemplu, cupoane) și tangibile (de exemplu, hotel electronic). cheile camerei) active [1].

În următoarele subsecțiuni, este raportată o prezentare generală a aplicațiilor dezvoltate/concepute, grupându-le în funcție de sectorul și contextul lor. Obiectivul aici este de a oferi cititorului o listă de aplicații existente, care urmează să fie dezvoltate, sau potențiale ale blockchain-ului și contractelor smart, pentru a-l ajuta să înțeleagă impactul imens pe care l-ar putea avea această tehnologie asupra societății. Aplicațiile din această zonă se leagă, în general, la adresa portofelului unui utilizator cu informații specifice legate de identitatea, interesele sau acreditările acestuia. Prin semnarea unei tranzacții folosind acreditările stocate în

portofelul său, utilizatorii pot dovedi proprietatea adresei și, prin urmare, își pot dovedi identitatea. Avantajul de a avea o dovadă a identității bazată pe blockchain constă în faptul că nu mai este nevoie să se bazeze pe o autoritate centralizată (ale cărei baze de date ar putea fi vulnerabile la atacuri sau modificări) și că indivizii au control deplin asupra acreditărilor lor. și, prin urmare, a datelor lor de identitate asociate [2].

Un prim exemplu în acest scenariu este Bitcoin Authentication Open Protocol (BitID), un prototip care permite utilizatorilor să se conecteze la unele site-uri web folosind portofelul Bitcoin. Pentru a se autentifica, utilizatorii trebuie să scaneze un cod QR (un cod asemănător unui cod de bare) cu aplicația mobilă a portofelului și să semneze un mesaj cu acreditările lor [2].

Un alt domeniu care primește o atenție din ce în ce mai mare este cunoaște-ți clientul (KYC) procesul de determinare a identității unui client, de exemplu atunci când deschide un cont bancar sau semnează o poliță de asigurare. În acest domeniu, mai multe companii lucrează la dezvoltarea unui KYC bazat pe blockchain. Ideea de bază constă din nou în furnizarea fiecărei persoane cu o adresă unică bazată pe blockchain. Ca un prim pas, identitatea persoanei ar fi verificată de către inspecții/instituții selectați (care ar verifica fizic cartea de identitate a acesteia). Ulterior, de exemplu, în timp ce deschide un cont bancar sau semnează o politică, persoana ar trebui doar să semneze o tranzacție cu acreditările sale, pentru a fi verificată.

Au fost concepute, de asemenea, aplicații mai complexe, al căror scop final este protejarea datelor personale ale utilizatorilor. Astfel de aplicații combină date în lanț și în afara lanțului. De fiecare dată când un utilizator dorește să acorde acces la datele sale unei aplicații externe, utilizatorul își poate dovedi identitatea pe blockchain și poate partaja datele personale legate de adresa ei, care sunt stocate în afara lanțului și criptate. În acest fel, utilizatorul poate decide ce date trebuie partajate cu aplicația externă.

Aplicabilitatea contractului inteligent serviciilor notariale

În context notarial, au fost propuse mai multe aplicații. Unii cercetători au propus înregistrarea în înregistrările publice blockchain, cum ar fi certificatele de căsătorie. O soluție mai complexă prevede posibilitatea de a exprima dorința de a se căsători prin semnarea și trimiterea unei tranzacții la o adresă de contract inteligent (smart) de căsătorie. Contractul inteligent (smart) ar putea codifica și condiții suplimentare care reglementează viața de familie. Cuplul ar putea decide chiar să se bazeze pe contract pentru a-și gestiona bugetul familiei. În cazul divorțului, împărțirea economiilor acumulate s-ar face automat, cu reducerea costurilor în procedurile notariale.

Similar certificatelor de căsătorie, înregistrările privind închirierile și schimburile de proprietăți ar putea fi, de asemenea, stocate pe blockchain. Studii recente au demonstrat avantajele exploatării contractelor smart într-un context imobiliar [3]. În primul rând, bazarea pe un registru unic partajat ar putea reduce fragmentarea informațiilor (de exemplu, casele de închiriere/vânzare sunt de obicei promovate pe o varietate de portaluri). În al doilea rând, identitățile părților implicate pot fi ușor verificate, împreună cu istoricul lor anterior. În al treilea rând, ar putea semna un contract de vânzare/închiriere bazat pe un contract smart. În cele din urmă, suma necesară de bani ar putea fi transferată automat vânzătorului/locatorului. S-a demonstrat că bazarea pe un contract inteligent (smart) pentru achiziționarea proprietății poate reduce timpul de la semnarea unui contract de vânzare până la înregistrarea dreptului de proprietate de la patru luni la două zile [3].

Eforturi considerabile de cercetare au fost dedicate protecției drepturilor de proprietate intelectuală. Din această perspectivă, au fost dezvoltate mai multe platforme pentru a le permite autorilor să demonstreze existența și calitatea de autor a unui document. Prin valorificarea caracteristicilor blockchain de imuabilitate și disponibilitate publică, astfel de platforme stochează hash-ul (rezumatul) documentului împreună cu un marcaj temporal, dovedind astfel existența documentului la un moment dat. Alte platforme fac un pas mai departe și se bazează pe regulile codificate în contracte inteligente (smart) pentru a permite licențierea automată, prin transferul de criptomonede către autor de fiecare dată când conținutul acestuia este vizualizat/ascultat de public [4].

Domeniul de aplicare al contractului inteligent în arealul Finanțelor

Finanțarea și transferurile de bani au fost primele scenarii de aplicație preconizate în inițiativa bitcoin. Deoarece transferurile bitcoin ar putea necesita ceva timp (în medie 10 minute), au fost concepute și alte blockchain-uri, cum ar fi Ripple, care se dorește a fi blockchain-ul adoptat de bănci și garantează un timp de executare al tranzacției de câteva secunde [5]. Unele aplicații interesante au fost create, concepute și în contextul comerțului, un exemplu elocvent dintre ele este EtherDelta, un schimb descentralizat care este gestionat prin contractele inteligente (smart).

Avantajul descentralizării este că utilizatorul nu trebuie să-și furnizeze fondurile unei platforme de tranzacționare deținute de o companie; în schimb, banii sunt stocați pe un contract inteligent (smart), care îi schimbă cu alte jetoane. Contractele inteligente (smart) au fost, de asemenea, utilizate în loteriile online și în sistemele de recompensare asemănătoare piramidei. În mod similar, au fost

folosite în pariurile sportive, pentru a oferi un mediu de pariuri mai transparent și mai ieftin. Trebuie menționate și piețele de predicție. Astfel de piețe se bazează pe ipoteza „*înțelepciunea mulțimii*”, conform căreia predicțiile făcute de grupuri de oameni sunt mai probabil să se întâmple în raport cu cele făcute de un singur individ.

Utilizatorii acestor platforme pot face o ghicire despre o apariție viitoare și, dacă presupunerea lor este corectă, pot primi automat o recompensă, declanșată de un contract inteligent (smart). În acest scop, trebuie remarcat faptul că aceste platforme se bazează puternic pe oracole (de obicei mai multe oracole care adună informații din diferite surse și iau decizii în majoritate) pentru a verifica apariția unui eveniment în lumea reală. O aplicație finală, care a fost concepută, sunt fondurile de pensii bazate pe contracte inteligente (smart) [6]. În această perspectivă, un cetățean care lucrează ar putea trimite în mod regulat bani către un contract inteligent (smart), care apoi, când va veni momentul, ar returna în mod regulat fondurile de pensii. Contractul inteligent (smart) ar putea produce automat previziuni, de exemplu cu privire la beneficiile lunare viitoare așteptate, pe baza contribuțiilor reale.

Aplicabilitatea contractelor inteligente (smart) în Industrie

Acesta este unul dintre sectoarele în care blockchain și contractele smart ar putea oferi beneficii largi. Lanțurile de producție și de aprovizionare, de exemplu, ar putea profita de faptul că blockchain-ul este un registru nemodificat, partajat la nivel mondial, de mai multe organizații. Din această perspectivă, diferiții actori implicați în producția și furnizarea de produse ar putea inspecta sau scrie pe blockchain date legate de mărfuri (prin urmare, informațiile nu ar mai fi fragmentate pe mai multe baze de date). În consecință, de exemplu, s-ar putea cunoaște, în orice moment, stările actuale și anterioare ale unui produs, având garanția că datele introduse nu au fost manipulate [6] sau urmărirea autorului unui document (de exemplu, pentru gestionarea jurnalelor de bord de construcție). Acest lucru ar putea fi deosebit de util în industria aviației, unde fiecare componentă a aeronavei trebuie urmărită cu atenție și unde cantitatea de documente pentru a îndeplini această sarcină într-un mod „tradițional” este uriașă [7]. Nu numai industriile, dar și clienții ar putea beneficia de exploatarea blockchain-ului pentru a stoca informații. De fapt, există mai multe aplicații pentru înregistrarea mărfurilor de valoare pentru a preveni contrafacerea. Cel mai faimos exemplu este proveniența și deținerea diamantelor, autentificarea petrecerilor, dar alte bunuri, cum ar fi biletele pentru sport/muzică, electronice și produse farmaceutice, mașini, comerțul cu amănuntul și alte produse de larg consum precum lemnul au fost, de asemenea urmărite.

În acest context, contractele inteligente (smart) sunt frecvent utilizate pentru a gestiona interacțiunea dintre vânzător și cumpărător, un contract inteligent (smart) codifică regulile pentru livrarea de pizza. Dacă mâncarea este livrată cu întârziere, contractul inteligent (smart) transferă automat înapoi cumpărătorului jumătate din prețul produsului livrat (pizza) [8]. Contractele inteligente (smart) ar putea fi folosite și pentru a converti automat banii cheltuiți în magazine, restaurante etc. în puncte de fidelitate, care ar putea fi apoi schimbate cu reduceri. În scenariul comerțului electronic, soluția prezentată de Monetha se bazează pe contracte inteligente (smart) pentru a schimba automat reputația părților implicate în tranzacții (pe baza „utilității” a fost efectuată tranzacția). O soluție și mai complexă, vizionară este reprezentată de Prophet: aici contractele smart funcționează împreună cu inteligența artificială pentru a sprijini o economie bazată pe cerere și potrivirea cererii și ofertei.

În cele din urmă, merită remarcat faptul că blockchain-ul ar putea simplifica și procesele de audit. De fapt, dacă toate tranzacțiile dintre companii și persoane ar fi înregistrate pe blockchain, astfel de procese ar fi mai rapide și mai eficiente, cu o reducere dramatică a birocrăției [9].

Domeniul de aplicabilitate al contractelor inteligente (smart) în asigurări

În sectorul asigurărilor, blockchain-ul ar putea aduce schimbări extraordinare. Ar putea fi utilizat, în special în combinație cu senzori Internet of Things (IoT), pentru a îmbunătăți experiența clienților și a reduce costurile de operare. În această perspectivă, contractele smart ar putea codifica regulile pentru o rambursare a daunelor, care ar putea fi declanșată de îndată ce un oracol detectează o situație dată, cum ar fi o întârziere a zborului sau o umiditate sub acoperișul unei clădiri.

O altă utilizare, care vizează reducerea fraudă, se bazează pe un blockchain scris de mai multe părți (de exemplu, nu numai companii de asigurări, ci și ofițeri de poliție, personal medical). Înainte de a plăti o despăgubire sau de a achiziționa un client, companiile de asigurări ar putea verifica reclamațiile și infracțiunile anterioare. În plus, contractele inteligente (smart) ar putea fi utilizate pentru a calcula automat riscul unui client și prima aferentă.

Contractele inteligente (smart) ar putea fi, de asemenea, exploatate într-un scenariu de asigurare cu plata pe utilizare. Senzorii ar putea fi folosiți pentru a activa sau dezactiva automat acoperirea unei polițe, în timp ce înregistrarea de pe blockchain ar fi o dovadă a schimbării. În cele din urmă, contractele inteligente (smart) ar putea fi elementul cheie pentru a sprijini asigurarea peer-to-peer.

Aplicabilitatea în domeniul administrării publice centrale

Mai multe aplicații pentru blockchain și contracte smart au fost propuse în context guvernamental. Estonia a propus recent adoptarea blockchain-ului pentru e-Residency, pentru a crește securitatea managementului identității [10, pag. 470-481].

Alte aplicații includ exploatarea blockchain-ului pentru a înregistra permanent voturile cetățenilor [11] (sau programele politicienilor, pentru a verifica dacă aceștia și-au respectat promisiunile). Un sistem de vot bazat pe blockchain ar putea fi structurat după cum urmează: cetățenilor care pot vota ar putea primi un jeton. Pentru a-și exprima preferința, ar putea trimite tokenul (adică să facă o tranzacție) la adresa portofelului unui politician. Autenticitatea și neschimbabilitatea votului ar fi garantate de blockchain. O soluție mai complexă ar fi să se bazeze pe contracte smart pentru a crea un sistem de guvernare autonom [11], în care cetățenii ar putea sugera modificări ale legilor existente și ar putea vota asupra acestora.

În domeniul sănătății, blockchain-ul ar putea fi utilizat pentru a stoca datele medicale ale pacienților, cu multe avantaje. În primul rând, comunitatea de cercetare ar putea profita de o bază de date medicale largă pentru a efectua analize și studii asupra patologiei existente. În al doilea rând, istoricul medical al fiecărei persoane ar fi înregistrat, îmbunătățind tratamentele medicale (de exemplu, în cazuri urgente, un medic ar putea fi alertat despre alergiile pacientului la tratamentele date). Mai multe companii investighează aceste scenarii, atât în contextul medical, cât și în cel stomatologic. În acest caz, obiectivul este îmbunătățirea calității sistemelor de sănătate. Aici, un contract smart conectează pacienții și furnizorii de servicii medicale, creând automat cea mai potrivită cale de tratament și reducând costurile birocrăției tipice procesului tradițional.

În scenariul educațional, blockchain-ul ar putea fi folosit pentru a înregistra competențele dobândite de către cursanți [12, pag. 49]. Având toată istoria lor anterioară stocată într-un singur loc (compartit), cursanții ar putea identifica mai ușor competențele care le lipsesc și să planifice cum să le obțină, sau pentru a determina locurile de muncă pentru care să aplice. În mod similar, în scenariul de gestionare a datelor cu caracter personal, fiecărui cursant ar putea primi o adresă de portofel, care ar putea acționa ca un container de competențe. În unele cazuri, hash-ul unui certificat poate fi, de asemenea, stocat. Bazându-se pe blockchain, fraudarea cererilor de muncă ar putea fi redusă pe scară largă, deoarece personalul de resurse umane ar putea accesa cu ușurință istoricul de formare anterioară a unei persoane. O altă aplicație interesantă se bazează pe contractele smart pentru a calcula recompensele care urmează să fie acordate studenților (pe baza notelor lor), încurajând astfel învățarea.

Domeniul Software și Internet de aplicare al contractului inteligent (smart)

În contextul IoT, blockchain-ul ar putea aduce mai multe beneficii. De exemplu, ar putea fi folosit pentru a stoca jurnalele de sistem, făcând astfel imposibil ca un atacator să șteargă sau să modifice istoricul evenimentelor. În contextul internetului, blockchain-ul a fost folosit pentru stocarea numelor de domenii, cu scopul de a înlocui serverele de sisteme de nume de domenii (DNS) cu altele bazate pe blockchain [13]. Din nou, în contextul internetului, contractele smart au fost folosite în cloud. Stocare [14]. În acest scenariu, utilizatorii pot închiria spațiu pe hard disk-urile lor, iar un contract smart le-ar oferi automat o rambursare. Sisteme precum acesta împart porțiuni din fișierele criptate ale utilizatorilor între mai multe noduri de computer și, înainte de a le stoca, își calculează hash-ul pentru a descoperi dacă același fișier a fost deja stocat în rețea (evitând astfel duplicatele) [14].

În scenariul IoT, blockchain-ul și contractele inteligente (smart) oferă infrastructură pentru o interacțiune sigură și automată între dispozitive. De exemplu, mecanismul criptografic ar putea fi utilizat în timpul autentificării dispozitivelor IoT. Scenariile mai complexe se bazează pe contracte smart și oracole pentru a permite aparatelor smart să interacționeze cu lumea reală. În această perspectivă, o mașină de spălat smart ar putea comanda (și plăti automat) piese de schimb în cazul unei defecțiuni. O altă aplicație este legată de rețelele smart. În acest caz, contractele smart pot permite schimburile automate de energie între clădiri, permițând astfel vecinilor să cumpere/să vândă energie electrică.

După cum sa menționat anterior, contractele inteligente (smart) pot permite crearea de organizație descentralizată autonomă (decentralized autonomous organization DAO), care sunt una dintre coloana vertebrală a economiei de schimb. Grupuri de indivizi pot coopera pentru a oferi comunității bunuri corporale și intangibile valoroase. Comunitatea ar putea decide apoi cum să evalueze activul și să recompenseze creatorul/furnizorul [15]. Aplicațiile existente de economie de partajare se vor baza în curând pe tehnologia blockchain. De exemplu, mai multe companii reproduc servicii precum Airbnb, Uber sau Amazon's Mechanical Turk. În cele din urmă, trebuie menționat că partajarea casei bazată pe blockchain ar putea beneficia de dulapuri smart care să permită accesul numai după rezervare.

Consecințele cu impact social al contractului inteligent (smart)

În domeniul social, au fost propuse mai multe aplicații bazate pe blockchain pentru a promova bunăstarea și a proteja drepturile omului în țările în curs de dezvoltare. De exemplu, pentru a crește incluziunea financiară, identificarea bazată

pe blockchain a fost folosită cu succes. Blockchain-ul va permite, de asemenea, persoanelor fără conturi bancare să fie implicate în schimburi de bani, deoarece toată lumea poate crea o adresă de portofel pentru a primi/trimitte bani. În plus, comisioanele de tranzacție mai mici pun bazele micro plăților și transferurilor de bani mai accesibile [16, pag.3]. În cele din urmă, contractele smart ar putea fi folosite pentru urmărirea fondurilor donatorilor, pentru a se asigura că ajung la beneficiarul vizat.

În concluzie afirmăm necesitatea aprofundării studiilor în acest domeniu, deoarece este un domeniu necesar pentru economia tehnologizată, elaborarea cadrului normativ care va fi prielnic dezvoltării acestui contract, deoarece în actualele condiții acest contract se dezvoltă sporadic. Contractele inteligente ne permit să automatizăm procese complexe în mai mulți pași. Credem că integrarea continuă a blockchain-urilor în domeniul IoT va provoca transformări semnificative în mai multe industrii, aducând noi modele de afaceri și făcându-ne să reconsiderăm modul în care sunt implementate sistemele și procesele existente.

Referințe bibliografice:

1. L. Capital, Bitcoin Series 24: The Mega-Master Blockchain List, 2014. [online] <http://www.ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list> [citat 17.09.2023].
2. V. L. Lemieux, *In Blockchain We Trust? Blockchain Technology for Identity Management and Privacy Protection* (2017), p. 57.
3. Deloitte Center for Financial Services, *Blockchain in Commercial Real Estate: The Future Is Here*, 2017, [online] <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-dcfs-blockchain-in-cre-the-future-is-here.pdf> [citat 17.09.2023].
4. Beck R., Becker C., Lindman J., Rossi M., [online] *Opportunities and Risks of Blockchain Technologies*, https://drops.dagstuhl.de/opus/volltexte/2017/7363/pdf/dagrep_v007_i003_p099_s17132.pdf, [citat 17.09.2023].
5. Jarrett A., *Ripple and R3 Team up with 12 Banks to Trial XRP for Cross-Border Payments*, 2016, [online] <https://ripple.com/insights/ripple-and-r3-team-up-with-12-banks-to-trial-xrp-for-cross-border-payments/> [citat 17.09.2023].
6. Beck R., Becker C., Lindman J., Rossi M., [online] *Opportunities and Risks of Blockchain Technologies*, https://drops.dagstuhl.de/opus/volltexte/2017/7363/pdf/dagrep_v007_i003_p099_s17132.pdf, [citat 17.01.2023].

7. Mansfield-Devine S., Beyond Bitcoin: Using Blockchain Technology to Provide Assurance in the Commercial World <https://www.sciencedirect.com/science/article/abs/pii/S1361372317300428> [citat 17.01.2023].
8. Sheridan I., *MiFID II in the context of Financial Technology and Regulatory Technology (2017) 12 (4)* Capital Markets Law Journal, 417–427.
9. Psaila S., *Blockchain: A Game Changer for Audit Processes*. <https://www2.deloitte.com/mt/en/pages/audit/articles/mt-blockchain-a-game-changer-for-audit.html> [citat 17.01.2023].
10. Sullivan C., Burger E., *E-Residency and Blockchain*, 2017, Computer Law & Security Review, p. 470–481.
11. S. Ølnes, Beyond Bitcoin Enabling Smart Government Using Blockchain Technology, (2016). International Conference on Electronic Government and the Information Systems Perspective. Is there a publisher? Pp. 253–64.
12. S. Huckle M. White, *Socialism and the Blockchain*, (2016) 8:4 Future Internet, Grech A., Camilleri A. F. ş.a. Blockchain in Education, JRC for Policy Report, 2017, p. 49.
13. Kalodner H., Carlsten M., Ellenbogen P., Bonneau J., Narayanan A., *An Empirical Study of Namecoin and Lessons for Decentralized Namespace Design*, În: Workshop on the Economics of Information Security (WEIS), 2015, pag.
14. Christidis K., Devetsikiotis M., *Blockchains and Smart Contracts for the Internet of Things*, <https://ieeexplore.ieee.org/document/7467408>
15. Pazaitis A., P. De Filippi, Kostakis V., *Blockchain and Value Systems in the Sharing Economy: The Illustrative Case of Backfeed 2017: 125* Technological Forecasting and Social Change, 105–15.
16. Thomason J., *Blockchain: An Accelerator for Women and Children's Health?* Global Health, 2017, pag. 3.