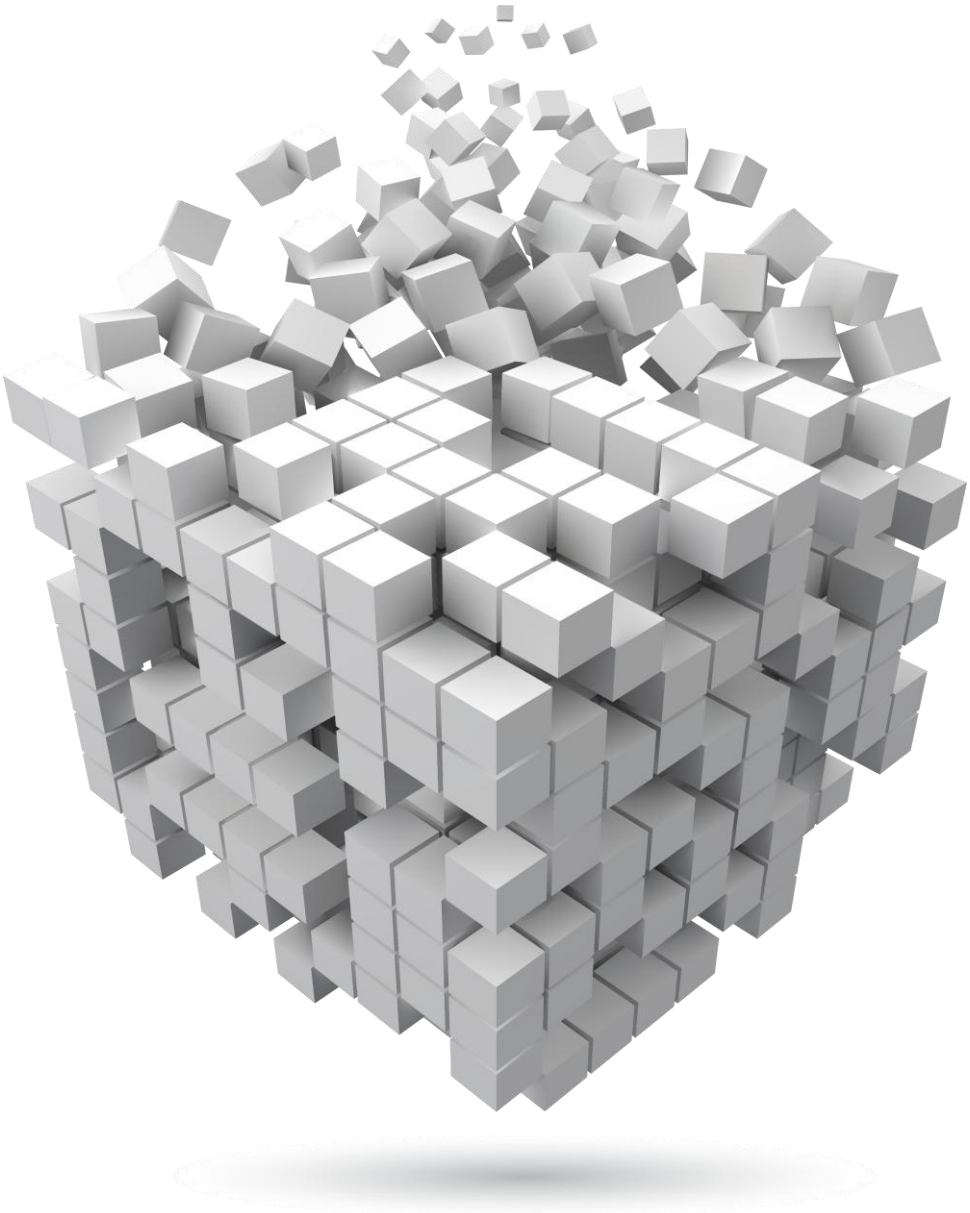
DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ



BLOCKCHAIN

DIN PERSPECTIVA SECURITĂȚII CIBERNETICE

TLP:CLEAR

Cuprins

1. Introducere

1.1. Context și motivație

Tehnologia blockchain a evoluat rapid de la rolul inițial de suport pentru criptomonede, devenind un cadru descentralizat pentru stocarea, verificarea și schimbul de informații. Prin asigurarea integrității datelor și a rezilienței operaționale, blockchain-ul este tot mai des analizat ca soluție pentru consolidarea securității cibernetice. Într-un context marcat de creșterea riscurilor privind manipularea datelor, atacurile asupra infrastructurilor critice și lipsa transparenței în procesele digitale, această tehnologie capătă relevanță strategică pentru instituții publice, operatori de infrastructuri esențiale și comunitatea de securitate.

1.2. Obiectivul documentului

Acest material este un studiu tematic privind potențialul tehnologiei blockchain în consolidarea securității cibernetice. Obiectivul principal este evaluarea aplicabilității acestei tehnologii în contexte operaționale relevante pentru securitatea digitală, identificarea punctelor forte și a limitărilor, precum și prezentarea unor exemple semnificative de implementare.

1.3. Public-țintă

Documentul se adresează:

- specialiștilor în securitate cibernetică;
- factorilor de decizie din instituții publice și din mediul strategic;
- cercetătorilor interesați de integrarea tehnologiilor emergente în ecosistemul digital național.

1.4. Delimitări și metodologie

Studiul nu abordează utilizarea blockchain-ului în contextul criptomonedelor speculative sau dintr-o perspectivă investițională. Accentul este pus pe aplicațiile non-financiare, cu potențial de a susține:

- asigurarea integrității datelor;
- validarea identităților și a evenimentelor digitale;
- trasabilitatea proceselor în infrastructuri critice.

Din punct de vedere metodologic, analiza se bazează pe:

- sinteza literaturii de specialitate (standarde internaționale, documente ENISA);
- clasificări conceptuale (tipuri de blockchain, mecanisme de consens);
- exemple de implementare relevante;
- evaluări SWOT și tendințe de evoluție tehnologică.

2. Aspecte de ordin tehnic privind tehnologia blockchain

2.1. Ce este blockchain?

Blockchain-ul este o tehnologie de registru distribuit (Distributed Ledger Technology – DLT) care permite înregistrarea și partajarea securizată a tranzacțiilor sau a altor date într-o rețea descentralizată, fără un administrator central. Datele sunt grupate în blocuri legate criptografic într-o succesiune cronologică, ceea ce asigură transparență, imuabilitate și rezistență la fraudă.[1]

Această tehnologie oferă o modalitate nouă și sigură de stocare și organizare a informațiilor, printr-un registru digital care este distribuit între toți participanții la rețea. Spre deosebire de bazele de date clasice, unde informațiile sunt controlate de o singură autoritate, blockchain funcționează printr-o rețea de computere (numite noduri), fiecare având o copie identică și actualizată a registrului.

Datele sunt înregistrate în blocuri legate între ele într-o ordine cronologică. Fiecare bloc este conectat la cel anterior printr-un cod unic (numit hash), generat automat din conținutul său. Astfel, orice încercare de modificare a unui bloc ar modifica întregul lanț și ar fi imediat identificată de rețea.

Blockchain nu are un punct central de control și se bazează pe consensul participanților pentru a valida noile informații. Criptografia asigură că datele nu pot fi modificate fără autorizare. Acest mod de

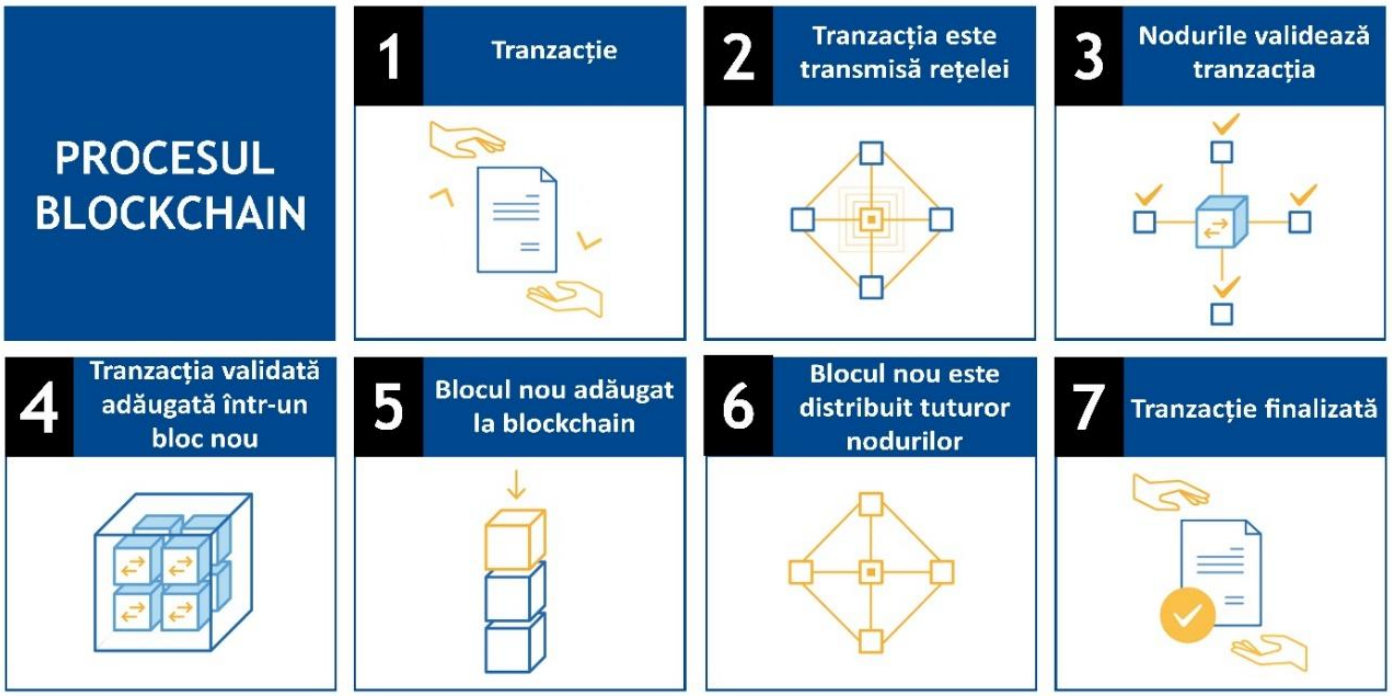
[1] Regulamentul (UE) 2023/1114 al Parlamentului European și al Consiliului din 31 mai 2023 privind piețele în cripto-active (MiCA), Art. 3(1), accesibil pe EUR-Lex: https://eur-lex.europa.eu/eli/reg/2023/1114

funcționare oferă un cadru sigur, transparent și de încredere pentru gestionarea datelor și a tranzacțiilor, fără a depinde de un administrator unic.

2.2. Cum funcționează?

Procesul prin care blockchain gestionează datele urmează o succesiune clară de etape (ilustrate în Figură 1), în care informațiile sunt validate și înregistrate permanent în rețea:

1. **Inițierea tranzacției -** procesul începe când un utilizator inițiază o acțiune, cum ar fi o plată sau un transfer de active digitale. Tranzacția este semnată criptografic cu cheia privată a utilizatorului, ceea ce garantează autenticitatea și integritatea datelor;
2. **Transmiterea în rețea și stocarea în mempool** - tranzacția semnată este propagată în rețea și recepționată de toate nodurile, fiind stocată temporar în mempool – o zonă de memorie destinată tranzacțiilor ce urmează a fi incluse într-un bloc;
3. **Validarea tranzacției** - nodurile implicate în mecanismul de consens verifică:
   - autenticitatea semnăturii digitale;
   - existența fondurilor (în cazul tranzacțiilor financiare);
   - respectarea regulilor rețelei.
4. **Formarea unui nou bloc** - tranzacțiile validate sunt selectate de nodurile producătoare de blocuri (mineri sau validatori), care creează un bloc nou ce include:
   - lista tranzacțiilor validate;
   - hash-ul blocului anterior;
   - propriul hash generat din conținutul curent al blocului.
5. **Adăugarea blocului la lanț** - după validare, blocul este adăugat lanțului existent, consolidând astfel integritatea și continuitatea registrului;
6. **Răspândirea blocului în rețea** - noul bloc este diseminat către toate nodurile, care își actualizează copia locală a registrului, menținând sincronizarea și coerența întregii rețele;
7. **Confirmarea tranzacției** - odată înregistrată într-un bloc valid, tranzacția este considerată confirmată. Totuși, pentru o siguranță sporită, sistemul poate considera tranzacția complet ireversibilă abia după adăugarea mai multor blocuri noi deasupra celui în care aceasta a fost inclusă.



Figură 1. Fluxul operațional al înregistrării unei tranzacții într-o arhitectură blockchain distribuită

2.3. Clasificarea blockchain în funcție de nivelul de acces și control

Clasificarea blockchain se bazează pe gradul de acces și control oferit participanților din rețea. În funcție de aceste criterii, pot fi identificate patru tipuri principale de arhitecturi, fiecare asociat cu un set specific de scenarii de utilizare.

Rețelele publice sunt cele mai deschise și transparente forme de blockchain. Ele permit oricărui utilizator să consulte înregistrările și să participe activ la validarea tranzacțiilor, prin mecanisme precum minarea sau staking-ul. Acest model se remarcă printr-un grad ridicat de descentralizare și rezistență la cenzură, fiind implementat în proiecte precum Bitcoin sau Ethereum, unde încrederea este construită prin verificare colectivă și consens distribuit.

La polul opus, **blockchain-urile private** sunt administrate de o singură entitate, care stabilește accesul la rețea și dreptul de validare a tranzacțiilor. Acestea sunt utilizate frecvent în mediul corporativ, unde contează păstrarea confidențialității și asigurarea integrității, precum și monitorizarea și autenticitatea datelor. Deși oferă performanțe operaționale ridicate, aceste rețele pot ridica îngrijorări privind transparența și riscurile de centralizare.

Între aceste două extreme se află **blockchain-urile de consorțiu**, operate de un grup de organizații care își împart responsabilitatea guvernării rețelei. Acest model este potrivit pentru colaborări între entități care au nevoie de o platformă comună, dar care nu doresc să își expună datele publicului larg. Exemple relevante pot fi găsite în sectorul bancar, logistic sau în gestionarea lanțurilor de aprovizionare, unde încrederea și trasabilitatea sunt importante, dar accesul la date trebuie restricționat.

În cele din urmă, **blockchain-urile hibride** combină caracteristici ale rețelelor publice și private, oferind un echilibru între transparență și control. Acest model permite, de exemplu, stocarea internă a datelor sensibile într-o rețea privată, cu posibilitatea de a expune public anumite informații pentru verificare externă. Această abordare este atractivă pentru organizațiile care au nevoi complexe legate de securitate și interoperabilitate. Exemple de astfel de platforme includ Dragonchain, dezvoltat de Disney, și XinFin (XDC Network), care combină confidențialitatea cu verificarea publică a datelor.

2.4. Mecanisme de consens în blockchain

În absența unei autorități centrale, rețelele blockchain se bazează pe mecanisme de consens pentru a asigura validarea tranzacțiilor și menținerea coerenței datelor în cadrul registrului distribuit. Acestea sunt metode prin care participanții din rețea ajung la un acord colectiv asupra stării datelor. Practic, ele garantează că toate nodurile „văd" același registru și că nimeni nu poate modifica informațiile în mod fraudulos - de exemplu, să cheltuiască de două ori aceeași sumă.

Cel mai cunoscut mecanism este **Proof of Work** (PoW) (utilizat de Bitcoin). În acest sistem, computerele din rețea (numite „mineri") concurează pentru a rezolva probleme matematice foarte dificile. Primul care găsește soluția are dreptul să adauge un nou bloc de tranzacții în registru și primește o recompensă. Acest proces consumă multă energie, fiind conceput deliberat să impună costuri ridicate, ca mecanism de descurajare a tentativelor de fraudă. Însă, tocmai din cauza acestui consum mare și a timpului necesar pentru procesare, PoW este uneori considerat ineficient și greu de scalat.

O alternativă mai recentă este **Proof of Stake** (PoS). Aici nu e nevoie de calcule complicate. Participanții blochează o anumită cantitate de criptomonede, numită „stake" și în funcție de cât de mare este acest stake, pot fi aleși să valideze noi blocuri. Este un sistem mai eficient energetic și mai rapid, dar poate duce la o concentrare a puterii în mâinile celor care dețin mai multe fonduri, ceea ce, ridică semne de întrebare privind echitatea.

Există și alte mecanisme, adaptate unor nevoi specifice. De exemplu, **Proof of Authority** (PoA) atribuie rolul de validator doar unor participanți desemnați și verificați de obicei, în rețele private sau între parteneri de încredere. Este rapid și eficient, dar reduce gradul de descentralizare. **Delegated Proof of Stake** (DPoS) funcționează pe baza unui sistem de vot, în baza căruia utilizatorii aleg delegați care se ocupă de validarea tranzacțiilor. Este un model reprezentativ, cu performanță ridicată, dar cu riscul concentrării deciziei în mâinile unui grup mic.

Fiecare mecanism are avantaje și dezavantaje. Alegerea celui potrivit depinde de mai mulți factori: cât de descentralizată trebuie să fie rețeaua, câtă energie se dorește a fi consumată, cât de rapid trebuie să funcționeze și ce nivel de securitate este necesar. În practică, multe rețele combină elemente din mai multe modele pentru a obține echilibrul optim între performanță, siguranță și accesibilitate.

3. Aplicații ale tehnologiei blockchain în domeniul securității cibernetice

Interconectivitatea tot mai accentuată, dependența de sisteme digitale și complexitatea infrastructurilor informatice amplifică expunerea la riscuri cibernetice. În acest context, tehnologia blockchain oferă un model alternativ de gestionare a datelor, în care validarea și controlul sunt distribuite între mai mulți participanți, fără a depinde de un nod central. Prin combinarea criptografiei avansate cu un mecanism de consens colectiv, blockchain susține dezvoltarea unor mecanisme de protecție solide, reziliente și verificabile, capabile să răspundă cerințelor actuale de securitate și încredere operațională.

Una dintre trăsăturile fundamentale ale tehnologiei blockchain este capacitatea sa de a garanta integritatea datelor în mod nativ. Fiecare bloc din registru este legat criptografic de cel anterior, iar modificarea oricărei informații necesită validarea de către întreaga rețea. Acest proces, intenționat dificil, protejează împotriva coruperii și manipulării. Acest model este relevant pentru gestionarea informațiilor critice, cum ar fi loguri de securitate, evidențe digitale, rapoarte de incident sau dovezi de conformitate.

Transparența este un alt beneficiu major. În rețelele publice, orice tranzacție este vizibilă și verificabilă de către oricine, susținând posibilitatea completă de audit. În rețelele private sau de consorțiu, accesul poate fi restricționat la entități autorizate, păstrând urmărirea în timp real într-un cadru controlat. Acest lucru este deosebit de util în sectoarele reglementate sau în activitățile de investigare post-incident.

Infrastructurile critice pot beneficia semnificativ de modelul distribuit oferit de blockchain, care elimină punctele unice de eșec și reduce suprafața de atac asociată arhitecturilor centralizate. Într-un astfel de cadru, compromiterea unui singur nod nu afectează funcționarea generală a rețelei, ceea ce crește semnificativ reziliența operațională.

În plus, blockchain permite automatizarea unor procese de securitate prin utilizarea contractelor inteligente (smart contracts). Acestea pot implementa politici de acces, gestiona răspunsuri automate la incidente sau facilita schimbul securizat de informații între entități de încredere, reducând riscul de eroare umană și accelerând capacitatea de reacție.

Printre cele mai promițătoare direcții de aplicare se numără:

- **Gestionarea identității digitale**: modelele auto-suverane oferă utilizatorilor control direct asupra propriilor date, eliminând dependența de baze centralizate, vulnerabile la atacuri;
- **Securitate endpoint**: blockchain poate susține o rețea de încredere pentru partajarea descentralizată a semnăturilor de malware și a indicatorilor de compromitere (IoC);
- **Vot electronic**: tehnologia oferă posibilitatea de verificare, transparență și integritate, fără a compromite confidențialitatea alegătorilor;
- **Protecția drepturilor de autor**: conținutul digital poate fi înregistrat criptografic într-un registru distribuit, oferind o evidență care poate fi verificată, a momentului creației și a autorului.

Prin aceste caracteristici, blockchain nu este doar o tehnologie promițătoare, ci un instrument strategic, adaptabil și scalabil, capabil să răspundă unor nevoi reale de securitate în medii critice. El susține o nouă paradigmă a încrederii în sistemele informatice, una distribuită, verificabilă și rezilientă.

3.1. Exemple de implementare

Tehnologia blockchain își găsește aplicabilitate într-o gamă largă de domenii, atât în sectorul public, cât și în cel privat, așa cum este ilustrat în *Figură 2*, susținând securitatea, integritatea și validarea corectă a datelor. Exemplele de mai jos prezintă modalități concrete de utilizare în contexte diverse.

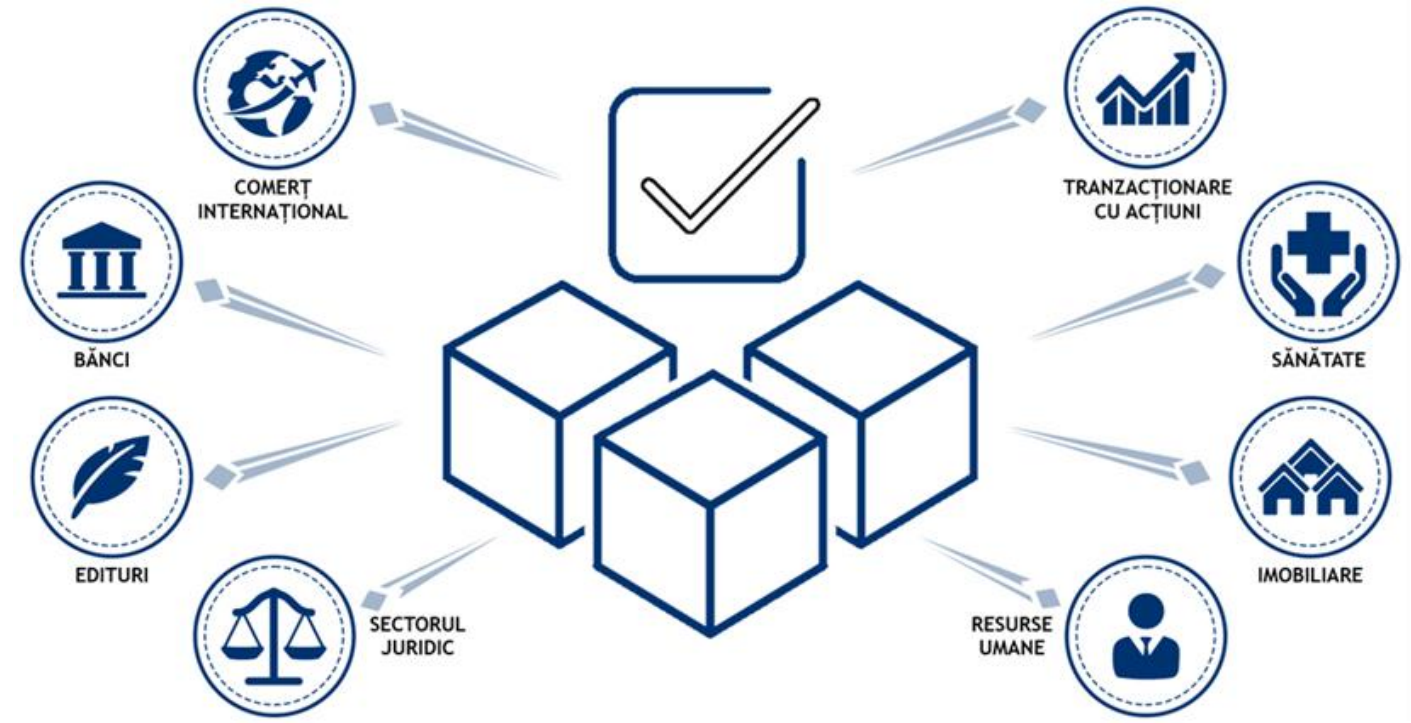
PolySwarm - detectarea descentralizată a amenințărilor cibernetice. PolySwarm este o platformă care valorifică principiile blockchain pentru a crea un ecosistem colaborativ de identificare a amenințărilor informatice. Printr-un marketplace descentralizat, experți independenți și furnizori de soluții antivirus contribuie la detectarea de malware și alte forme de atac cibernetic. Participanții sunt recompensați în token-uri Nectar (NCT) pentru contribuțiile valide, stimulând astfel o competiție constructivă și rapidă în domeniul analizei de securitate. Acest model promovează diversitatea surselor de analiză și reduce dependența de mecanisme centralizate de detecție.[2]

VeChain – monitorizare în timp real a lanțurilor de aprovizionare. VeChain este o platformă blockchain destinată sectorului enterprise, orientată către digitalizarea și securizarea fluxurilor de aprovizionare. Sistemul combină funcționalitățile blockchain cu dispozitive Internet of Things (IoT) pentru a urmări

[2] *PolySwarm - detectarea descentralizată a amenințărilor cibernetice*, online: https://messari.io/project/polyswarm/profile

complet bunurile, de la producător până la consumatorul final. Această abordare oferă o soluție scalabilă pentru controlul circulației produselor, prevenind frauda, contrafacerea și pierderile de date.[3]

Estonia și securizarea datelor medicale prin Guardtime - Estonia este un exemplu de referință în integrarea blockchain în serviciile publice, în special în domeniul sănătății. În colaborare cu compania Guardtime, autoritățile estoniene au implementat infrastructura *Keyless Signature Infrastructure* (KSI) pentru a garanta integritatea și posibilitatea de verificare a istoricului înregistrărilor medicale. Fiecare accesare, modificare sau actualizare a datelor este înregistrată automat și poate fi validată criptografic, fără a dezvălui conținutul în sine. Această abordare asigură un nivel ridicat de transparență pentru audit, previne manipularea și consolidează încrederea cetățenilor în sistemul de sănătate digital.[4]



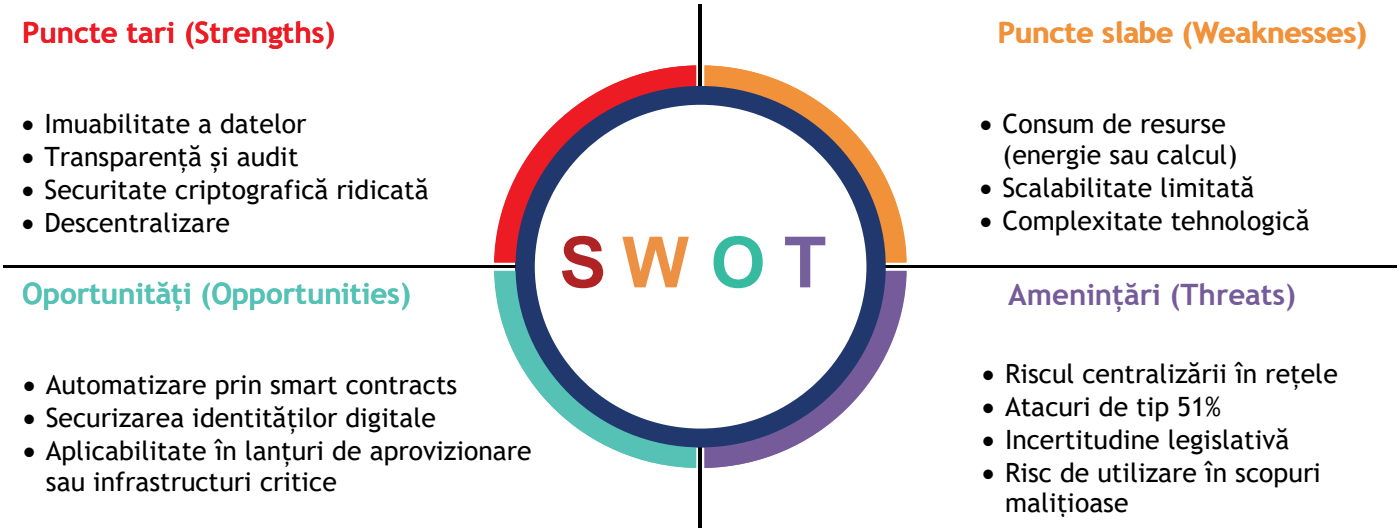
Figură 2. Domenii de utilizare a blockchain în mediul public și privat

[3] *VeChain – Trasabilitate în timp real pentru lanțurile de aprovizionare:* https://medium.com/@web3author/blockchain-meets-supply-chain-how-vechain-is-disrupting-traditional-management-d868204409

[4] *Estonia și securizarea datelor medicale prin Guardtime:* https://estonianworld.com/technology/estonia-to-protect-patient-records-with-guardtime-blockchain-technology/

3.2. Analiza SWOT a implementării blockchain în securitatea cibernetică

Înainte de adoptarea tehnologiei blockchain în cadrul strategiilor de securitate cibernetică, este importantă realizarea unei analize SWOT. Această metodă oferă un cadru structurat pentru evaluarea factorilor interni (puncte tari și puncte slabe) și externi (oportunități și amenințări) care pot influența succesul adoptării. Prin această abordare, organizațiile pot fundamenta decizii informate și elabora strategii care valorifică avantajele oferite de blockchain, iar riscurile și limitările asociate se pot atenua.



Figură 3. Analiza SWOT a implementării blockchain în securitatea cibernetică

Puncte tari:

- Imuabilitatea datelor - odată înregistrată, informația nu poate fi modificată fără consensul rețelei, garantând integritatea și credibilitatea istoricului digital;
- Transparență și audit - toate tranzacțiile sunt vizibile și verificabile de către participanții autorizați, facilitând auditul și detectarea tentativelor de manipulare;
- Securitate criptografică ridicată - datele sunt protejate prin algoritmi criptografici avansați, ceea ce reduce riscul accesului neautorizat;
- Descentralizare - elimină punctele unice de eșec și reduce dependența de un administrator central, sporind reziliența operațională.

Puncte slabe:

- Consum de resurse (energie sau calcul) – algoritmi precum PoW necesită putere computațională mare, generând costuri energetice ridicate;
- Scalabilitate limitată – numărul tranzacțiilor procesate pe secundă este adesea redus comparativ cu soluțiile centralizate, afectând timpii de răspuns;
- Complexitate tehnologică – implementarea și întreținerea blockchain-ului presupun expertiză tehnică specializată și resurse semnificative.

Oportunități:

- Automatizare prin smart contracts – permite execuția automată a unor procese, reducând erorile umane și accelerând operațiunile;
- Securizarea identităților digitale – modelele descentralizate de identitate oferă control direct utilizatorilor și reduc riscul compromiterii datelor;
- Aplicabilitate în lanțuri de aprovizionare sau infrastructuri critice – oferă mecanisme robuste de monitorizare și verificare a fluxurilor, sporind încrederea și reducând frauda.

Amenințări:

- Riscul centralizării în rețele – în practică, puterea de validare se poate concentra în mâinile unui număr redus de actori, contrar principiului descentralizării;
- Atacuri de tip 51% – controlul majoritar al resurselor rețelei poate permite modificarea tranzacțiilor și compromiterea integrității registrului;
- Incertitudine legislativă – lipsa unor reglementări clare și unitare poate descuraja investițiile și adopția pe scară largă;
- Risc de utilizare în scopuri malițioase – tehnologia poate fi exploatată pentru activități ilegale, cum ar fi spălarea de bani sau finanțarea activităților criminale.

3.3. Provocări și limitări

Deși tehnologia blockchain aduce o serie de avantaje clare în ceea ce privește securitatea cibernetică, implementarea sa nu este lipsită de obstacole. Limitările țin atât de natura tehnică a sistemelor distribuite, cât și de provocările practice asociate integrării acestora în infrastructuri existente, adesea rigide sau suprasolicitate. Una dintre cele mai frecvente critici vizează problema scalabilității. Multe rețele blockchain întâmpină dificultăți în procesarea unui volum ridicat de tranzacții într-un interval scurt de timp, ceea ce poate deveni o barieră semnificativă în contexte care necesită o reacție aproape instantanee, cum este cazul detecției și răspunsului la incidente cibernetice.

Soluțiile propuse, precum rețelele de tip layer-2 sau mecanismele de sharding, oferă direcții promițătoare, însă nu constituie încă soluții scalabile la nivel generalizat. Pe lângă provocările legate de performanță, un alt aspect critic este consumul energetic, în special în cazul rețelelor bazate pe mecanisme de consens de tip PoW. Deși alternative mai eficiente precum PoS, câștigă tot mai mult teren, sustenabilitatea energetică rămâne o preocupare legitimă, în special pentru organizațiile care respectă criterii stricte de eficiență și responsabilitate ecologică.

Integrarea blockchain într-o arhitectură IT existentă presupune, de regulă, un proces complex, care necesită adaptări semnificative atât din punct de vedere tehnic, cât și organizațional. Lipsa de interoperabilitate între diferitele tipuri de blockchain și sistemele tradiționale poate genera blocaje în implementare, în timp ce necesitatea unui nivel ridicat de expertiză poate transforma orice inițiativă într-un proiect costisitor, cu riscuri de depășire a bugetului sau a termenelor stabilite.

Contractele inteligente, deși importante pentru automatizarea proceselor, vin la rândul lor cu riscuri specifice. Codul sursă trebuie verificat riguros înainte de implementare, întrucât orice eroare, odată introdusă în blockchain, devine dificil de corectat. În lipsa unor audituri de securitate și a mecanismelor de actualizare controlată, contractele inteligente pot constitui puncte de vulnerabilitate. În plus, incertitudinile juridice reprezintă o barieră importantă pentru adoptarea pe scară largă.

Absența unor reglementări clare, unitare și aplicabile transfrontalier creează neîncredere, mai ales în domenii sensibile precum sănătatea, finanțele sau administrația publică. În lipsa unui cadru normativ bine definit, organizațiile ezită să adopte această tehnologie, temându-se de incompatibilități cu legislația existentă sau de lipsa recunoașterii legale a datelor înregistrate pe blockchain.

Chiar dacă blockchain este conceptualizat ca o tehnologie fundamental descentralizată, în practică, unele implementări pot duce la forme de centralizare mascată. În cazul rețelelor PoW, puterea de calcul se concentrează adesea în centre de minare specializate, iar în rețelele PoS, acumularea de capital de către un număr restrâns de participanți poate genera dezechilibre similare celor existente în modele centralizate. Înțelegerea acestor limite constituie un punct de plecare important pentru o evaluare realistă a blockchain ca soluție de securitate.

Doar printr-o abordare critică, susținută de planificare atentă și adaptare tehnologică, organizațiile pot valorifica potențialul real al acestei tehnologii, fără a-i subestima complexitatea.

4. Tendințe emergente în tehnologia blockchain și securitatea cibernetică

Pe măsură ce nevoile organizațiilor în materie de securitate digitală se diversifică, iar atacurile informatice vizează din ce în ce mai frecvent infrastructuri esențiale, tehnologia blockchain evoluează din faza exploratorie spre o adopție strategică, susținută de soluții emergente menite să îmbunătățească scalabilitatea și reziliența. Această tranziție este susținută de o serie de tendințe tehnologice care indică o maturizare semnificativă a domeniului.

O direcție importantă este extinderea serviciilor de tip *Blockchain-as-a-Service (*BaaS*)*, oferite de mari furnizori cloud precum Microsoft Azure, Amazon Web Services și IBM. Aceste soluții permit organizațiilor să testeze și să implementeze rapid aplicații blockchain fără a investi semnificativ în infrastructuri proprii, facilitând astfel adoptarea în sectoare critice precum sănătate, logistică, servicii financiare și nu în ultimul rând, securitate cibernetică.

În paralel, dezvoltarea de mecanisme blockchain orientate către protejarea infrastructurilor critice capătă tot mai multă relevanță. Prin replicarea distribuită a datelor și integrarea cu sisteme automate de alertare, blockchain oferă un cadru solid, capabil să susțină detectarea rapidă a incidentelor și reacția coordonată în fața acestora.

Utilizarea tehnologiei în gestionarea identității digitale este tot mai răspândită. Modelele descentralizate de tip *Self-Sovereign Identity* (SSI) oferă utilizatorilor control direct asupra propriilor date, eliminând nevoia bazelor de date centralizate, vulnerabile la atacuri. Aceste modele sunt tot mai relevante în ecosisteme care necesită autentificare rapidă, dar sigură, fără a compromite confidențialitatea.

Contractele inteligente, deja utilizate pentru automatizarea proceselor, devin tot mai sofisticate. Ele permit implementarea de politici de acces, reacții automate la comportamente suspecte sau aplicarea regulilor de confidențialitate într-un mediu distribuit. Această automatizare contribuie la reducerea timpului de reacție și a dependenței de operatori umani în procese critice.

O tendință distinctă o reprezintă integrarea blockchain-ului cu alte tehnologii emergente. În combinație cu inteligența artificială (IA), blockchain oferă un cadru de date verificabil, în care IA poate identifica tipare de risc. În tandem cu Internet of Things (IoT), tehnologia contribuie la securizarea datelor generate de dispozitive conectate, garantând autenticitatea și integritatea acestora. Pentru a sprijini aceste utilizări avansate, sunt dezvoltate activ soluții menite să depășească limitările de scalabilitate. Tehnici precum fragmentarea rețelelor (sharding), rețelele de tip *layer-2* și canalele de plată sporesc capacitatea de procesare și reduc costurile, facilitând utilizarea blockchain-ului în medii cu activitate intensă.

Pe măsură ce aceste progrese tehnice se consolidează, apare tot mai pregnantă și nevoia unui cadru legal și normativ clar. Inițiative precum regulamentul MiCA, promovat de Uniunea Europeană, vizează crearea unei reglementări unitare pentru piețele de active digitale și aplicațiile bazate pe blockchain. Concomitent, standardizarea tehnică are ca obiectiv interoperabilitatea între rețele și integrarea cu sistemele existente, condiții esențiale pentru dezvoltarea arhitecturilor hibride și multi-platformă.

Aceste tendințe reflectă atât o maturizare tehnologică, cât și una instituțională. Blockchain-ul nu mai este perceput doar ca o soluție experimentală, ci ca un instrument strategic, adaptabil și scalabil, care poate fi integrat eficient în strategiile de securitate cibernetică ale organizațiilor ce urmăresc reziliență, control distribuit și posibilitatea de verificare a datelor.

5. Concluzii

Caracteristicile definitorii ale tehnologiei blockchain – *imutabilitatea*, *descentralizarea* și *transparența* – oferă metode fiabile de validare, urmărire și protecție a datelor, contribuind la rezolvarea unor provocări din domeniul securității informatice. De la gestionarea identităților digitale și protejarea infrastructurilor critice, până la automatizarea politicilor de acces și consolidarea proceselor de detecție, blockchain-ul își demonstrează utilitatea în numeroase aplicații din domeniul securității cibernetice.

Cu toate acestea, adoptarea pe scară largă rămâne condiționată de depășirea unor obstacole tehnice și instituționale. Limitările de performanță, cerințele energetice ridicate asociate anumitor algoritmi de consens și dificultățile de integrare în arhitecturi IT preexistente impun eforturi susținute de optimizare. De asemenea, conturarea unui cadru de reglementare clar și previzibil reprezintă un factor-cheie pentru consolidarea încrederii și stimularea adopției responsabile. Pe fondul acestor provocări, evoluțiile recente indică o tendință de maturizare a tehnologiei. Integrarea cu soluții de IA, dezvoltarea standardelor tehnice și apariția unor modele scalabile și interconectabile contribuie la extinderea reală a potențialului blockchain-ului în domeniul securității informatice.

Astfel, fără a fi o soluție universală, blockchain-ul poate deveni o componentă strategică a arhitecturii defensive a organizațiilor care urmăresc să își sporească reziliența, transparența operațională și controlul asupra datelor. Utilizată în mod responsabil, această tehnologie oferă premise solide pentru construirea unui ecosistem digital mai sigur și mai transparent.

Autor: Daniel Abotezătoaei
Revizori: Aurel Huștea, Cristian Nistor, Cornel Argint, George Bobric

Bibliografie

1. Blockchains, 1. (2023). *Disadvantages of blockchain.* Preluat de pe https://101blockchains.com
2. Blockchains, 1. (2023). *Top 10 blockchain use cases 2023.* Preluat de pe https://101blockchains.com
3. Deloitte. ((n.d.)). *An internal auditor's guide to blockchain: Auditing blockchain environments.* Deloitte.
4. Deloitte. ((n.d.)). *When two chains combine: Supply chain meets blockchain.* Deloitte EMEA Blockchain Lab.
5. Deloitte. (2019). *Risk considerations in blockchain technology: An internal auditor's guide.* Deloitte Development LLC.
6. ENISA. (2021). *Crypto Assets: Introduction to Digital Currencies and Distributed Ledger Technologies.* Preluat de pe https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Crypto%20Assets%20Introduction%20to%20Digital%20Currencies%20and%20Distributed%20Ledger%20Technologies.pdf
7. ENISA. (2021, Feb 09). *Solving the Cryptography Riddle: Post-quantum Computing & Crypto-assets Blockchain Puzzles.* Preluat de pe https://www.enisa.europa.eu/news/enisa-news/solving-the-cryptography-riddle-post-quantum-computing-crypto-assets-blockchain-puzzles
8. Limited, D. T. (2018). *An internal auditor's guide to blockchain: Blurring the line between physical and digital* . Deloitte.
9. LOȘONȚI, M.-C. (2018). *IdentityChain: Sistem pentru administrarea identității digitale prin blockchain.* Undergraduate thesis, Universitatea Politehnica din București.
10. Maleh, Y. S. (2020). *Blockchain for cybersecurity and privacy: Architectures, challenges, and applications.* CRC Press.
11. Mathew, A. R. (2019). *Cyber security through blockchain technology.* Preluat de pe International Journal of Engineering and Advanced Technology (IJEAT): https://doi.org/10.35940/ijeat.A9836.109119
12. Office, U. G. (2022). *Blockchain: Emerging technology offers benefits for some applications but faces challenges.* GAO-22-104625.
13. Oracle. (2022). *Oracle OCI Blockchain Platform: Interconnect and automate your enterprise's ecosystem.* Preluat de pe https://www.oracle.com/blockchain/cloud-platform/
14. Piscini, E. D. ((n.d.)). *Blockchain & cyber security: Let's discuss.* Deloitte EMEA Grid Blockchain Lab.
15. Piscini, E. D. ((n.d.)). *Introduction to blockchain: Auditing blockchain environments.* Deloitte.
16. Piscini, E. S. (2017). *Taking blockchain live: The 20 questions that must be answered to move beyond proofs of concept.* Deloitte Development LLC.
17. Research, G. ((n.d.)). *Public token infrastructure.* Alphabill.

Glosar de termeni

Termen	Definiție extinsă
51% Attack	Atac posibil într-o rețea blockchain în care un actor sau un grup de actori controlează peste 50% din puterea de calcul sau de validare, permițându-le să modifice ordinea tranzacțiilor, să dubleze cheltuielile sau să blocheze validarea unor operațiuni
Blockchain-as-a-Service (BaaS)	Model de livrare a tehnologiei blockchain prin platforme cloud, care permite companiilor să dezvolte și să ruleze aplicații blockchain fără a gestiona infrastructura proprie
Blockchain public / privat / consorțiu / hibrid	Tipuri de blockchain diferențiate prin nivelul de acces și control: public - oricine poate participa; privat - controlat de o singură entitate; consorțiu - operat de mai mulți parteneri; hibrid - combină caracteristici din celelalte
Cadru normativ	Ansamblu de reguli, legi și reglementări care guvernează utilizarea tehnologiilor digitale, inclusiv blockchain, în scopul asigurării conformității, securității și protecției datelor
Canale de plată (layer-2)	Soluții de tip layer-2 care permit efectuarea de tranzacții între două părți fără a fi necesară înregistrarea fiecărei operațiuni pe blockchain-ul principal, reducând costurile și timpii de procesare
Contracte inteligente (smart contracts)	Secvență de cod rulată pe blockchain care execută automat acțiuni atunci când sunt îndeplinite anumite condiții. Elimină nevoia de intermediari și este utilizată în aplicații precum plăți automate sau controlul accesului
Endpoint Detection and Response (EDR)	Tehnologie de securitate cibernetică care monitorizează continuu dispozitivele finale (endpoints) pentru a detecta, analiza și răspunde în mod automat la amenințări sau comportamente suspecte
Hash	Funcție criptografică ce transformă datele într-o valoare unică, folosită pentru verificarea integrității și legarea blocurilor într-un blockchain
Layer-1	Rețeaua blockchain de bază, pe care sunt înregistrate toate tranzacțiile. Asigură securitatea, consensul și arhitectura principală pe care se pot construi soluții Layer-2
Layer-2	Set de soluții dezvoltate peste blockchain-ul de bază pentru a îmbunătăți scalabilitatea, reducând costurile și timpii de procesare. Exemple includ rețele secundare sau canale de plată
Mempool	Zonă temporară de stocare a tranzacțiilor validate local, dar neincluse încă într-un bloc. Minerii sau validatorii aleg tranzacții din mempool pentru a le include în blocuri.
Minare (mining)	Procesul prin care nodurile dintr-o rețea blockchain, numite mineri, validează tranzacții și adaugă noi blocuri la lanț, rezolvând probleme criptografice complexe. Este specific mecanismului PoW
Proof of Stake (PoS)	Mecanism alternativ de consens în care participanții blochează criptomonede („stake”) pentru a obține dreptul de validare. Consumă mai puține resurse decât PoW și este folosit în rețele precum Ethereum 2.0
Proof of Work (PoW)	Mecanism de consens care presupune rezolvarea unor probleme matematice complexe de către participanți (mineri). Validarea tranzacțiilor se bazează pe efort computațional și este utilizată de Bitcoin
Distributed Ledger	Bază de date replicată între mai multe locații sau participanți, fără administrator central, care asigură transparență și integritate prin consens
Self-Sovereign Identity (SSI)	Model de identitate digitală descentralizată care oferă utilizatorilor control complet asupra propriilor date personale. Elimină dependența de furnizori centrali și îmbunătățește protecția datelor
Sharding	Tehnică de fragmentare a rețelei blockchain în unități mai mici (shards) care procesează tranzacții în paralel, îmbunătățind viteza și eficiența generală a rețelei
Stake	Suma de criptomonede blocată de un participant într-un sistem PoS pentru a obține dreptul de a valida tranzacții. Cu cât „stake-ul” este mai mare, cu atât cresc șansele de selecție ca validator
Validator	Participant într-un sistem blockchain care validează tranzacții și propune noi blocuri. În consensul PoS sau PoA, validatorii înlocuiesc minerii din PoW și contribuie la securitatea rețelei
Staking	Procesul prin care deținătorii de criptomonede blochează o parte din activele lor pentru a ajuta la validarea tranzacțiilor pe un blockchain. În schimbul acestui serviciu, ei primesc recompense, similar cu a primi dobândă într-un cont bancar