
ROMANIA
SRI
Patria a priori
SERVICIUL ROMAN DE INFORMATII
BULETIN SPECIAL
CYBERINT
BLOCKCHAIN

CE ESTE BLOCKCHAIN

Blockchain-ul sau tehnologia blocurilor, face parte din ansamblul rețelelor de tip tehnologie a registrelor distribuite (*Distributed Ledger Technology* - DLT) și reprezintă seturi de date organizate în blocuri de informație înlănțuite, partajate, replicate și sincronizate între membrii rețelei.

Concret, blockchain reprezintă o rețea/serie de blocuri care pot conține date de orice tip, având ca proprietate particulară faptul că, ulterior validării, datele nu mai pot fi alterate.

În cadrul acestei rețele pot fi introduse permanent noi date, creându-se un nou bloc, fiecare dintre acestea fiind legat criptografic de cel din fața lui și de cel din spatele lui, atât din punct de vedere informațional, cât si temporal.

Structura blockchain-ului este de tip listă simplu înlănțuită. Pentru modificarea datelor existente într-un bloc, este creat un nou bloc care conține date cu privire la modificarea în cauză. Astfel, din rețea nu pot fi șterse înregistrări, orice acțiune regăsindu-se în blocuri sub formă de noi date. Acest sistem conferă securitate informațiilor, întrucât rețeaua este rezistentă la modificări (*tamper resistance*).

Dispozitivele participante în rețeaua blockchain, care descarcă, stochează și actualizează constant întregul registru de date, poartă denumirea de NODURI. Acestea pot îndeplini una sau mai multe funcții conform arhitecturii blockchain-ului.

Știința care stă la baza blockchain-ului este criptografia. Asupra fiecărui bloc este aplicată o funcție criptografică de tip hash, care generează și îi asociază un șir de caractere unic.

CARACTERISTICILE **BLOCKCHAIN**

DESCENTRALIZARE – Rețelele blockchain sunt de tip ***peer-to-peer***, ceea ce presupune eliminarea intermediarilor, datele fiind distribuite în mod simultan la nivelul tuturor nodurilor din rețea. Astfel, este imposibilă alterarea datelor de către o entitate care deține controlul.

TRANSPARENȚĂ - Toate tranzacțiile/operațiunile realizate în cadrul rețelei sunt publice, cunoscute de toate nodurile existente în rețea. În acest sens, este permisă auditarea tuturor acestor operațiuni, în scopul asigurării integrității datelor.

IMUABILITATE - Veridicitatea și integritatea datelor introduse este asigurată printr-un proces de validare multiplă (de către mai multe entități/noduri/peer). Odată introduse în rețea și validate, blocurile nu pot fi modificate/alterate, fiind dependente de funcțiile criptografice de tip hash utilizate pentru realizarea legăturilor dintre blocuri.

VITEZĂ - Întrucât tehnologia blochckain exclude nevoia de aprobare a operațiunilor de către o entitate cu rol central, durata de validare a acestora de către nodurile existente în rețea este considerabil redusă.

ANONIMITATE - În pofida faptului că operațiunile sunt înregistrate, respectiv pot fi auditate, acestea sunt realizate prin intermediul unor conturi/portofele virtuale cărora nu le este asociată identitatea deținătorilor.

Toate aceste caracteristici ale tehnologiei blockchain asigura o securitate sporită a rețelelor prin implementarea criptografiei și prin asigurarea unui control distribuit asupra operațiunilor realizate la nivelul blocurilor.

TIPURI DE **BLOCKCHAIN**

Rețelele de tip blockchain pot fi împărțite în trei mari categorii, în funcție de caracteristicile deținute: blockchain public, blockchain privat și blockchain hibrid.

În cazul blockchain-ului **PUBLIC**, rețeaua nu are restricții privind accesul nodurilor la date, orice persoană/entitate având posibilitatea de a se conecta/efectua operațiuni în cadrul acesteia.

De asemenea, orice dispozitiv poate deveni nod prin descărcarea, stocarea și actualizarea constantă a întregului registru de date. Tocmai de aceea, nivelul de încredere dintre noduri este unul scăzut, aspect compensat prin utilizarea unor algoritmi criptografici complecși în comunicarea dintre noduri.

Blockchain-ul **PRIVAT** limitează accesul nodurilor în ceea ce privește introducerea datelor, dar capacitatea dispozitivelor de a dobândi calitatea de nod în cadrul rețelei. Accesul în cadrul rețelei este restricționat către anumite persoane/entități, în funcție de criterii stabilite de deținătorul acesteia.

În ceea ce privește blockchain-ul **HIBRID**, acesta are atât caracteristici specifice blockchain-ului public, cât și celui privat. Rețeaua este vizibilă public, însă accesul în cadrul acesteia este restricționat.

Nodurile îndeplinesc diferite roluri, având totodată acces diferențiat la informațiile din cadrul rețelei.

ARHITECTURA UNUI **BLOCKCHAIN**

Principalele componente ale unui blockchain sunt:

Noduri – reprezintă fiecare entitate din cadrul rețelei care deține o copie actualizată constant a întregului blockchain;

Tranzacții – orice operațiune efectuată asupra datelor din cadrul rețelei blockchain. Acestea includ date precum sursa, destinația și datele vehiculate între acestea;

Blocuri – structuri de date care conțin tranzacții și care sunt distribuite înlănțuit în cadrul rețelei;

Lanț – secvența de blocuri dispuse într-o anumită ordine;

Mineri – noduri specializate care utilizează puterea computațională deținută în vederea verificării blocurilor de tranzacții care sunt, ulterior, adăugate în blockchain;

Consensus/protocol – set de reguli utilizate pentru gestionarea modului de funcționare a rețelei blockchain.

ISTORIA **BLOCKCHAIN**

Blockchain a apărut în anul 2008, în timpul crizei economice mondiale din perioada 2007-2009, când o persoană/ un grup de persoane care activează sub pseudonimul Satoshi Nakamoto a lansat un nou protocol pentru „Sistemul electronic de numerar de tip peer-to-peer", folosind o criptomonedă – Bitcoin.

Protocolul lui **SATOSHI** a stabilit un set de reguli, sub forma unor calcule distribuite, care asigură integritatea datelor schimbate între miliarde de dispozitive fără a trece printr-o terță parte de încredere.

Blockchain-ul **BITCOIN** este public, întrucât oricine poate citi sau scrie date din sau în registru dacă execută software-ul Bitcoin corespunzător. În acest sens, există o oarecare lipsă de încredere în rețea, compensată prin mecanisme suplimentare pentru a arbitra disputele dintre participanți și a proteja integritatea datelor.

Aceasta implică o complexitate ridicată, deoarece nu există o autoritate centrală de arbitraj într-o rețea descentralizată cum este cea a Bitcoin.

Astfel, în blockchain-ul Bitcoin, tranzacțiile noi pot fi adăugate în lanțul de blocuri numai după ce participantul în rețea rezolvă o problemă matematică compleză, proces denumit „minerit/minat" – mining.

Minerii trebuie să „investească"/consume energie și timp pentru a găsi o soluție la această problemă matematică în vederea validării tranzacției.

ETHEREUM

Plecând de la Bitcoin, au fost dezvoltate și alte proiecte de tip blockchain independente. Niciunul nu s-a ridicat însă, până în prezent, la nivelul acestuia, însă au oferit beneficii în ceea ce privește creșterea vitezei, a anonimității sau a capacității de stocare a datelor de mari dimensiuni.

Ethereum este o platformă software distribuită, de tip open-source, bazată pe un blockchain public. Acesta este creat astfel încât tranzacțiile să fie efectuate doar când anumite condiții sunt întrunite.

Regulile care definesc și stabilesc aceste condiții poartă numele de „smart contracts".

Odată ce a fost scris, un smart contract nu mai poate fi modificat și se execută automat în momentul în care condițiile stabilite sunt îndeplinite.

⚠ Spre exemplu, un smart contract poate fi creat pentru a stabili accesul în rețeaua blockchain, în funcție de permisiunile fiecărui utilizator.

RISCURI

Până în prezent, niciun blockchain **NU** a fost compromis.

Au fost observate atacuri derulate asupra platformelor de exchange de criptomonedă, fără a afecta însă rețeaua blockchain.

Un potențial risc al tehnologiei blockchain este reprezentat de monopolizarea rețelei de o entitate care ar putea astfel să acceseze și să realizeze modificări asupra datelor înregistrate, fenomen cunoscut ca "51% attack".

Prin deținerea a 51% din puterea computațională necesară validării noilor înregistrări din cadrul rețelei, atacatorul poate decide ce operațiuni să valideze, alterând autenticitatea datelor și încrederea membrilor în rețea și/sau în entitatea inițiatoare/deținătoare. Cu toate acestea, un astfel de atac este greu de realizat, fiind necesare resurse enorme. Acesta ar putea fi preîntâmpinat prin implementarea unor funcționalități care să descurajeze orice tentativă.

De asemenea, în cadrul unei rețele private sau hibride, identitatea reală a membrilor poate fi cunoscută, astfel încât, cu ajutorul caracteristicii de transparență a tehnologiei, poate fi identificată entitatea responsabilă de alterarea datelor.

OPORTUNITATE

Încă de la apariția tehnologiei, companii private și-au îndreptat atenția către integrarea blockchain-ul în activitățile pe care le derulează, în vederea eficientizării acestora.

⚠ Utilitatea blockchain este evidențiată la nivel mondial prin multiple studii și sondaje ale unor companii specializate în consultanță.
În prezent, după cum relevă un studiu al Forumului Economic Mondial, tehnologia blockchain este utilizată de cel puțin 40 de bănci centrale și în peste 200 de inițiative publice din 45 de țări la nivel mondial.

Această evoluție nu se limitează la sectorul privat. Din perspectiva sectorului public și al îmbunătățirii serviciilor furnizate cetățenilor, implementarea unor tehnologii de tip blockchain ar putea aduce beneficii în ramuri precum managementul identității (documente de identitate, acte de căsătorie,

pașapoarte, permis de conducere etc.), securizarea datelor în aviație, optimizarea sistemului de colectare a taxelor, gestionarea registrelor medicale, gestionarea în mod integrat a parcursului școlar al cetățenilor, asigurarea securității cibernetice, securizarea lanțului de aprovizionare, managementul proprietății și cadastrarea terenurilor agricole.

Cu toate acestea, anterior inițierii unor proiecte blockchain, trebuie să se ia în considerare dacă tehnologia este potrivită pentru nevoile organizației, întrucât NU toate problemele necesită o soluție blockchain. Pentru o ca o soluție blockchain să fie întradevăr eficientă, trebuie îndeplinite următoarele patru condiții:

1. mai multe părți generează tranzacții care presupun modificări într-o bază de date distribuită;
2. părțile trebuie să aibă încredere ca tranzacțiile sunt valabile;
3. intermediarii nu sunt de încredere în arbitrarea adevărului;
4. securitate sporită pentru a asigura integritatea sistemului.

USE CASES – DOMENIUL SĂNĂTĂȚII

Tehnologia blockchain prezintă numeroase OPORTUNITĂȚI pentru domeniul sănătății, însă aceasta nu este pe deplin matură, neexistând, până în prezent, niciun mecanism care să poată fi implementat în viitorul apropiat.

Un transfer al informațiilor din domeniul sănătății într-un sistem bazat pe blockchain poate facilita cooperarea dintre organizații, întrucât acesta are potențialul de a reduce/elimina interacțiunea și costurile intermediarilor. De asemenea, tehnologia blockchain poate transforma serviciile medicale, plasând pacientul în centrul ecosistemului sănătății și contribuind la creșterea nivelului de siguranță, confidențialitate și interoperabilitate a datelor din domeniul medical.

Una dintre cele mai importante aplicații blockchain este reprezentată de dosarele medicale electronice. În momentul în care se generează și se semnează o înregistrare medicală, aceasta poate fi scrisă în blockchain, care va furniza dovada și va asigura încrederea că nu poate fi alterată, integritatea acesteia fiind asigurată. Același concept poate fi aplicat și în cazul studiilor clinice.

Partajarea și schimbul dosarelor pacienților între medici și organizații medicale este un proces complicat, pe fondul aspectelor administrative și de confidențialitate. În plus, este dificil de urmărit utilizarea și distribuirea datelor din dosar. Tehnologia blockchain poate reprezenta o soluție viabilă la această problemă, întrucât permite înregistrarea fiecărui pas al procesului și poate furniza dovezi în cazul unui comportament defectuos.

Pe lângă managementul datelor pacienților, blockchain prezintă un potențial considerabil pentru utilizarea în sectorul medical, deschizând calea către numeroase aplicații care ar putea face industria medicală mai accesibilă, mai sigură și mai eficientă:

- managementul datelor demografice privind sănătatea populației;
- asigurarea securității datelor utilizate pentru studiile clinice;
- urmărirea traseului comercial al medicamentelor.

Pentru început, organizațiile pot lua în considerare tehnologia blockchain pentru a verifica digital identitatea unui pacient, date genetice sau istoricul rețetelor. De exemplu, poate fi implementat un concept ce oferă pacienților dreptul de proprietate completă asupra dosarelor medicale, permițându-le să acorde și să revoce accesul la datele lor. Medicii pot emite prescripții pe blockchain.

Organizațiile pot alege să utilizeze un blockchain public sau un blockchain hibrid prin care să se permită accesul unui grup predeterminat. Punerea în aplicare necesită, de asemenea, selectarea unui protocol blockchain și a unui framework care ghidează structura de dezvoltare de aplicații și platforme.

Accesarea rețelei blockchain se poate realiza prin intermediul unei interfețe (API) user-friendly, astfel încât orice utilizator, inclusiv cei care nu dețin cunoștințe tehnice, poate efectua operațiuni conform cu rolul și permisiuni deținute.

De-a lungul timpului, au existat numeroase ATACURI CIBERNETICE asupra sistemului de sănătate, precum și breșe de securitate, care au facilitat accesul atacatorilor cibernetici la date private. Proprietățile inerente ale blockchain pot crea un nou nivel de securitate pentru organizațiile din sistemul sănătății.

Fiecare participant conectat la rețeaua blockchain deține o cheie privată, cunoscută doar de deținător, și o cheie publică, vizibilă celorlalți participanți în rețea.

Perechea este legată criptografic, astfel încât identificarea este posibilă doar într-o singură direcție, folosind cheia privată. Blockchain-ul, prin utilizarea perechilor de chei, oferă protecție asupra datelor și le permite pacienților să-si dezvăluie identitatea și atributele în fața organizațiile specifice din sistemul de sănătate.

În plus, potențialul de compromitere a unei chei private a unui singur pacient poate limita daunele adverse, deoarece acest proces se realizează în mod individual fiecărui utilizator, neexistând o modalitate prin care atacatorii, printr-o singură acțiune, să poată compromite un set de chei private aparținând mai multor utilizatori.

Toate organizațiile din domeniul sănătății conectate la blockchain pot menține propria copie actualizată a datelor din blockchain și, ca urmare, în cazul în care un bloc trebuie ajustat, este necesară aprobarea modificării de către 51% dintre participanții la rețea.

Această caracteristică îmbunătățește securitatea datelor din sectorul sănătății si poate reduce riscul de apariție al incidentelor de securitate cibernetică.

CONCLUZII

În timp ce tehnologia blockchain ar putea avea un potențial semnificativ de a îmbunătăți interoperabilitatea, securitatea și confidențialitatea datelor, este important să fie luate în calcul și limitele tehnologiei.

Blockchain-ul nu este un substitut pentru o bază de date clasică. Soluțiile blockchain nu sunt optimizate pentru date de volum mare.

Soluțiile blockchain sunt proiectate pentru înregistrarea evenimentelor de date, tranzacții specifice, care sunt menite să fie distribuite într-o rețea, în situații în care transparența și colaborarea sunt criterii necesare.

Organizațiile care decid să implementeze blockchain trebuie să proiecteze și să integreze soluții care să susțină procesele de business în ceea ce privește eficientizarea:

- verificării și autentificării informațiilor
- transferurilor de date

www.sri.ro