



ACADEMIA
DE BLOCKCHAIN INTELLIGENCE

MODULUL 2

Blockchain și MiCA în practică

Blockchain și MiCA în practică

Operațiuni risc și conformitate pentru CASP

Acest curs reprezintă al doilea modul al programului de formare Blockchain Intelligence Academy și se adresează persoanelor care cunosc noțiunile fundamentale prezentate în Modulul 1 sau dețin cunoștințe echivalente.

Cursul explică modul în care informațiile blockchain sunt utilizate în activitatea operațională a furnizorilor de servicii de criptoactive, a instituțiilor financiare și a autorităților. Participanții vor lucra cu tranzacții, adrese, date despre clienți și indicatori de risc, pentru a înțelege cum este construită și documentată o decizie.

Regulamentul privind piețele criptoactivelor, MiCA, este prezentat din perspectivă tehnică și operațională. Cursul oferă o hartă de orientare asupra tipurilor de criptoactive, serviciilor furnizate de un CASP, autorizării, supravegherii, guvernantei și protecției clienților. Nu urmărește realizarea unei analize juridice articol cu articol și nu înlocuiește consultanța juridică specializată.

Participanții vor înțelege și relația dintre MiCA, regulile privind informațiile care însoțesc transferurile de criptoactive și obligațiile de prevenire și combatere a spălării banilor. Aceste cadre vor fi delimitate clar, pentru a evita atribuirea tuturor obligațiilor operaționale direct Regulamentului MiCA.

Cursul este orientat spre exerciții, demonstrații și situații reale. Participanții vor analiza alerte, vor corela date on-chain cu informații KYC și bancare, vor identifica informațiile care lipsesc și vor formula o concluzie documentată.

Recomandăm participarea la primele două module de pregătire ale Blockchain Intelligence Academy, pentru a facilita înțelegerea noțiunilor de bază.



OBIECTIVELE CURSULUI

Prin participarea la acest curs, se urmărește:

1. Dezvoltarea capacității de a interpreta tranzacții și activitatea adreselor blockchain în contexte operaționale.
2. Înțelegerea rolului unui CASP și a principalelor servicii reglementate de MiCA.
3. Înțelegerea implicațiilor practice ale autorizării, supravegherii, guvernancei și protecției clienților.
4. Corelarea datelor blockchain cu informații KYC, date bancare și informații interne despre client.
5. Identificarea indicatorilor de risc și diferențierea acestora de dovezi sau concluzii definitive.
6. Dezvoltarea autonomiei în luarea și justificarea deciziilor de închidere, monitorizare sau escaladare a unui caz.
7. Înțelegerea fluxului de analiză și raportare a tranzacțiilor suspecte către ONPCSB, atunci când sunt îndeplinite condițiile legale.
8. Standardizarea informațiilor pentru colaborarea dintre CASP, instituții financiare, funcții de conformitate și autorități.

GRUP ȚINTĂ

Cursul se adresează profesioniștilor din sectorul financiar-bancar, specialiștilor în conformitate, prevenirea spălării banilor, administrarea riscurilor, audit și control intern, precum și reprezentanților furnizorilor de servicii de criptoactive.

Este relevant pentru personalul instituțiilor publice și al autorităților, operatorii fintech, echipele care gestionează clienți sau tranzacții cu criptoactive și profesioniștii care trebuie să interpreteze informații produse de block explorers ori platforme de analiză.

Cursul este potrivit și pentru managerii care coordonează procese de autorizare, supraveghere, monitorizare, raportare sau colaborare interinstituțională.

CONȚINUTUL CURSULUI

Competența 1: Analiza practică a informațiilor blockchain

- Verificarea tranzacțiilor
- Identificarea rețelei, activului, transaction hash-ului, adreselor, valorii, comisionului, statusului și blocului.
- Interpretarea activității on-chain

Transferuri native, transferuri de token, internal transactions, interacțiuni cu smart contracts și approvals.

- Adrese și entități

Diferența dintre o adresă EOA, o adresă de contract, un multisig și un cont intern al unei platforme.

- Informație on-chain și informație off-chain

Ce poate fi observat public și ce informații pot fi obținute numai de la client, bancă, CASP sau altă instituție.

- Explorare și platforme de analiză

Diferențe de acoperire, etichetare, scoruri și metodologie. Limitele instrumentelor și necesitatea verificării informațiilor.

- Nivelul de certitudine

Separarea faptelor observabile de etichete, indicatori, asocieri, ipoteze și concluzii.

Competența 2: MiCA și funcționarea operațională a unui CASP

- Prezentarea generală a MiCA

Scopul regulamentului și locul acestuia în activitatea cu criptoactive.

- Tipuri de criptoactive în contextul MiCA

Tokenuri raportate la active, tokenuri de monedă electronică și alte criptoactive. Introducere în noțiunile ART și EMT.

- Serviciile furnizate de un CASP

Custodie, operarea unei platforme, schimb, executarea ordinelor, transfer și alte servicii relevante.

- Autorizarea din perspectivă operațională

Identificarea serviciilor, responsabilități, politici, sisteme, resurse și informații care trebuie documentate.

- Supravegherea

Informațiile pe care organizația trebuie să le poată prezenta, modul de documentare a controalelor și răspunsul la solicitările autorităților.

- Guvernanță și protecția clienților

Responsabilități, conflicte de interese, gestionarea activelor clienților, reclamații, externalizare și păstrarea evidențelor.

Competența 3: Monitorizarea tranzacțiilor și analiza unitară a riscului

- Profilul clientului

Identitatea, activitatea declarată, sursa fondurilor și comportamentul așteptat.

- Date KYC și date bancare

Corelarea identității verificate și a operațiunilor fiat cu activitatea on-chain.

- Indicatorii de risc

Volum, frecvență, fragmentare, contrapărți, expunere la servicii cu risc și neconcordanțe față de profil.

- Expunerea directă și indirectă

Interpretarea distanței față de o adresă sau entitate etichetată și limitele concluziilor automate.

- Adrese negăzduite

Identificarea și evaluarea riscurilor asociate transferurilor către sau dinspre portofele care nu sunt administrate de un furnizor.

- Travel Rule

Rolul informațiilor despre inițiator și beneficiar și delimitarea acestor cerințe față de obligațiile MiCA.

Competența 4: Decizia escaladarea și raportarea

- De la alertă la caz

Verificarea alertei, colectarea informațiilor și identificarea elementelor care necesită investigație suplimentară.

- Autonomia în decizii

Alegerea justificată între închiderea alertei, solicitarea de informații, monitorizarea suplimentară și escaladare.

- Alerta și suspiciunea

Diferența dintre un scor de risc, un indicator, o anomalie și o suspiciune justificată.

- Raportarea către ONPCSB

Rolul entității raportoare, fluxul intern de analiză și informațiile tehnice care pot susține un raport de tranzacție suspectă.

- Audit trail

Documentarea surselor, verificărilor, raționamentului, aprobărilor și deciziei finale.

Competența 5: Standardizare și colaborare interinstituțională

- Mecanismul unitar de analiză

O succesiune comună pentru identificarea rețelei, verificarea tranzacției, evaluarea riscului și formularea deciziei.

- Fișa standard de caz

Rețea, activ, transaction hash, adrese, valoare, surse, etichete, indicatori, informații lipsă, certitudine și acțiune recomandată.

- Interoperabilitatea informațiilor

Folosirea unor câmpuri și termeni comuni pentru transmiterea și reproducerea analizei.

- Fragmentarea informației

Riscurile care apar atunci când banca, CASP-ul, analistul, conformitatea și autoritatea dețin separat părți ale aceluiași caz.

- Rolul persoanei care analizează informațiile blockchain

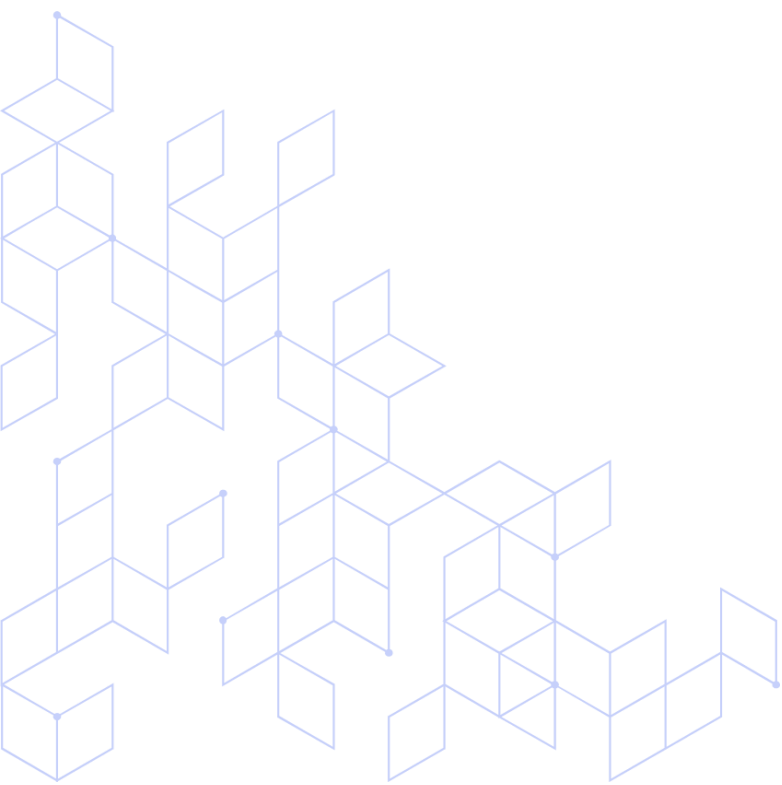
Competențe tehnice, gândire analitică, documentarea incertitudinii, comunicare și respectarea procedurilor.

- Selecția și dezvoltarea personalului

Utilizarea unui profil comun de competențe pentru selectarea, evaluarea și menținerea specialiștilor.

Competența 6: Studii de caz și exerciții practice

- verificarea unei tranzacții și identificarea rețelei corecte;
- analiza unui transfer de token și a unei interacțiuni cu un smart contract;
- compararea informațiilor furnizate de două platforme;
- corelarea unei tranzacții bancare cu o retragere de criptoactive;
- evaluarea unei alerte asociate unei adrese cu risc;
- identificarea informațiilor care lipsesc;
- formularea și justificarea unei decizii;
- completarea unei fișe standardizate de caz;
- simularea transmiterii informațiilor între bancă, CASP, conformitate și autoritate.



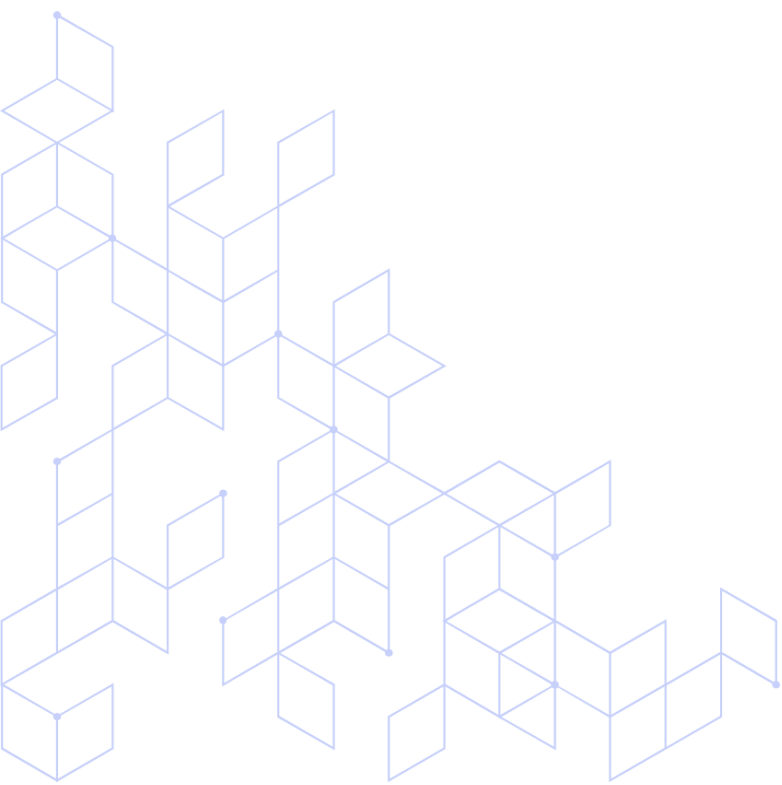
TRAINER

Ciprian Iacob

este specialist în tehnologie și antreprenor, cu experiență în dezvoltarea și coordonarea unor proiecte complexe în domeniile blockchain, criptoactivelor, fintech și transformării digitale.

În ultimii ani, a fost implicat în cadrul Institutului Național de Cercetare-Dezvoltare în Informatică - ICI București în dezvoltarea unor inițiative și infrastructuri digitale care integrează tehnologii emergente, de la blockchain și active digitale până la soluții de interoperabilitate și aplicații bazate pe inteligență artificială.

Experiența sa combină perspectiva tehnică cu cea operațională și strategică, incluzând proiectarea de produse și arhitecturi digitale, analiza ecosistemelor blockchain și înțelegerea mecanismelor de trasabilitate, risc și conformitate asociate criptoactivelor. În activitatea de formare, urmărește să transforme concepte tehnice complexe în modele clare și aplicabile, folosind demonstrații, studii de caz și situații reale pentru a conecta tehnologia blockchain cu procesele și provocările întâlnite de instituții, companii și profesioniști.



DURATA CURSULUI

1 zi (6 ore, în intervalul 10:00 – 16:00)

INSCRIEREA

Se realizează prin e-mail: cicc@ici.ro.

DEZVOLTAREA COMPETENȚELOR

Participanții vor primi o diplomă de participare, eliberată de ICI București, ce va include suplimentul descriptiv al competențelor specifice dobândite.

Acest modul de pregătire este recomandat pentru a putea participa ulterior la modulele practice de curs ale Blockchain Intelligence Academy.

ICI București a inițiat demersurile formale pentru includerea ocupației de „analist blockchain” atât în clasificarea ocupațiilor din România, cât și la nivel european. La finalizarea acestor demersuri în premieră la nivel european, ce vizează profesionalizarea domeniului „blockchain intelligence”, participanții la curs vor fi notificați asupra posibilității de a beneficia de avantajele acestei noi ocupații.

TAXA DE PARTICIPARE

Taxa de participare: 1200 lei

ALTE INFORMAȚII DE INTERES:

Despre software-ul de blockchain intelligence al Chainargos

ChainArgos este o companie de blockchain intelligence, recunoscută pentru descoperirea subcolateralizării cripto-activelor stabile în valoare de 1,4 miliarde de dolari BUSD pe platforma globală Binance.

ChainArgos oferă soluții avansate de blockchain intelligence, concentrându-se pe analiza detaliilor financiare ale tranzacțiilor. Aceste soluții facilitează investigațiile și analizele economice, oferind o perspectivă obiectivă asupra raționamentului din spatele fluxurilor complexe de tranzacții.

Compania colaborează cu instituții financiare, autorități de reglementare, agenții de aplicare a legii, institute de cercetare, universități și furnizori de servicii de criptoactive la nivel global. De asemenea, ChainArgos beneficiază de susținerea unor instituții media de renume, precum Bloomberg, Wall Street Journal, Forbes, Fortune, Thomson Reuters și South China Morning Post.

Participanții vor avea acces la platforma de analiză blockchain ChainArgos pe durata cursului și ulterior pe o perioadă limitată, pentru exersarea noțiunilor prezentate.



INSTITUTUL NAȚIONAL DE CERCETARE - DEZVOLTARE
ÎN INFORMATICĂ - ICI BUCUREȘTI

