

Marius Peter

Spălarea banilor prin criptoactive



Cuprins

Cuvânt-înainte.....	XIX
Abrevieri.....	XXIII
Partea I. Criminalitatea informatică – evoluție, fenomen global și cadru juridic.....	1
Introducere.....	1
Capitolul I. Noțiuni tehnice de bază: sisteme informatice clasice, distribuite și de inteligență artificială (IA)	3
1.1. Date, programe și sisteme informatice.....	3
1.2. Metode și tehnici clasice folosite în activitățile de criminalitate informatică.....	9
1.3. Ecosistemul registrelor distribuite (DLT) sau principiile de bază ale tehnologiei blockchain	20
A. Rețele informatice: client-server sau peer-to-peer (P2P)?	20
B. Registre jurnal: centralizate sau distribuite?	24
C. Procesul criptografic de hashing.....	29
D. Validarea blocurilor de date într-un sistem DLT. Mecanisme de consens.....	30
1.4. Sisteme de inteligență artificială (IA)	35
Capitolul II. De la viruși informatici la ecosistemele infracționale globale. Evoluția criminalității informatice	41
2.1. Perioada pionieratului (anii '70-'90): experimentare și primele infracțiuni.....	41
2.2. Perioada de tranziție (anii '90 - anii 2000): comercializarea criminalității.....	43
2.3. Perioada industrializării (anii 2000-2015): Crime-as-a-Service.....	50
2.4. Perioada actuală (2015-prezent): ecosisteme infracționale complexe și convergență tehnologică	59
Concluzii	73
Capitolul III. Fenomenul global al criminalității informatice în contextul actual.....	76
3.1. Dimensiunea economică și impactul global	76
3.2. Caracteristicile definitorii ale criminalității informatice contemporane	86
A. Transnaționalitatea și provocările jurisdicționale	86
B. Asimetria dintre atacator și victimă.....	90
C. Viteza și automatizarea	93
D. Specializarea și economia infracțională structurată	97
E. Integrarea cu actori statali și zona gri.....	99
2.3. Tendințe emergente (2023-2025).....	103
Concluzii	113

Capitolul IV. Cadrul legislativ. România în context european

și internațional	115
4.1. Strategia internațională de combatere: Convenția de la Budapesta (2001).....	115
4.2. Legislația Uniunii Europene.....	129
4.3. Legislația României - încadrarea în standardele europene.....	143
4.4. Legislația Statelor Unite ale Americii - model comparativ.....	148
4.5. Analiza comparativă - lecții și provocări.....	154
Concluzii	157

Partea a II-a. Ecosistemul blockchain - mediu tehnologic și infracțional 159

Capitolul I. Fundamentele tehnice ale platformelor de tip blockchain.

Ce trebuie să înțeleagă practicienii dreptului?	160
1.1. Arhitectura blockchain - concepte esențiale.....	160
1.2. Tranzacții și imuabilitate.....	168
1.3. Pseudonimizare vs. anonimizare	183
A. Metoda 1. Intersecția cu servicii centralizate care respectă procedurile KYC.....	186
B. Metoda 2. Analiza blockchain (blockchain analytics).....	190
C. Metoda 3. Intersecția cu lumea fizică.....	203
1.4. Contracte inteligente - „codul ca lege”	207
Concluzii	222

Capitolul II. Ecosistemul descentralizat - DeFi, DEX-uri, protocoale.....226

2.1. DeFi (Decentralized Finance) - noua infrastructură financiară	226
2.2. DEX-uri (Decentralized Exchanges) vs. CEX-uri (Centralized Exchanges)	243
2.3. Mixere și protocoale de anonimizare	257
A. Protocolul Tornado Cash	259
B. Protocoale de tip Wasabi Wallet și CoinJoin	265
2.4. Bridge-uri între blockchain-uri și chain-hopping	272
2.5. Monede virtuale stabile (stablecoins) - pivotul către monedă fiduciară	278
Concluzii	283

Capitolul III. De ce mediul blockchain devine mediu infracțional privilegiat? 286

3.1. Câteva cazuri de fraude majore.....	288
A. Atacuri de tip social engineering. Cazul Ronin Bridge (Axie Infinity)	288
B. Cazul Bybit: 1,5 miliarde USD prin manipularea unei semnături.....	291
C. Seria de atacuri asupra CoinsPaid, Alphapo, WazirX (2023)	295
D. Concluzii.....	298
3.2. Caracteristicile care facilitează criminalitatea.....	300
A. Pseudonimizarea - suficientă pentru operare, depășibilă pentru investigație.....	300
B. Viteza și ireversibilitatea - atacul finalizat înainte de răspuns.....	304
C. Elementul nativ de extraneitate - jurisdicția ca obstacol greu de depășit	307
D. Lipsa intermediarilor reglementați - inexistența „punctelor de control”	310

Cuprins

E. Complexitatea tehnică – asimetria cunoștințelor.....	314
3.4. Ecosistemul infracțional matur.....	330
Concluzii	339
Partea a III-a. De la mecanisme tehnice specifice platformelor distribuite la încadrarea juridică în norma de incriminare	341
Capitolul I. Infracționalitatea „clasică” din mediul blockchain. Provocările unei noi realități tehnologice	342
Introducere	342
1.1. Infracțiunile informatice clasice în fața paradigmei blockchain	344
A. Accesul ilegal redefinit: de la sistem informatic la logica sistemului	345
B. Alterarea integrității datelor și perturbarea funcționării sistemelor informatice în mediul blockchain	360
C. Infracțiuni informatice fără obiect în registrul public - art. 361 și 364 din Codul penal	379
1.2. Infracțiunile patrimoniale clasice (furt, înșelăciune, șantaj), comise prin intermediul sistemelor informatice	389
A. Atacuri pentru obținerea ilegală de active (furtul, înșelăciunea)	395
B. Ransomware-ul: șantajul informatizat	412
C. Piața neagră online (darknet): infracțiuni adiacente facilitate de ecosistemul cripto	423
D. Criptomoneda: motorul ecosistemului darknet	428
E. Încrederea automatizată prin tehnologie: rolul escrow-ului și al contractelor inteligente.....	431
F. Eficiența și ireversibilitatea: atribute comerciale decisive.....	434
1.3. Provocări investigative și puncte critice pentru circuitul infracțional	436
A. Provocările fundamentale ale anchetei.....	436
B. Strategii investigative și puncte critice pentru circuitul infracțional	440
C. Cooperarea interinstituțională și cadrele juridice necesare	443
Concluzii	446
Capitolul II. Infracțiuni native în blockchain: zone gri și necesitatea interpretării	450
Introducere	450
2.1. Exploatarea contractelor inteligente și ale protocoalelor DeFi	453
A. Fapta prevăzută de legea penală	453
B. Săvârșirea cu vinovăție	456
C. Caracterul nejustificat și imputabilitatea	459
2.2. Rug pulls și exit scams.....	461
A. Anatomia unei lansări frauduloase	463
B. Fapta prevăzută de legea penală	469
C. Intenția frauduloasă în arhitectura proiectului.....	469

D. Caracterul nejustificat și imputabilitatea.....	473
2.3. Schemele Ponzi și fraudele de investiții crypto.....	476
A. Iluzia profitului rapid	476
B. Fapta prevăzută de legea penală	479
C. Săvârșirea cu vinovăție	482
D. Caracterul nejustificat și imputabilitatea	484
2.4. Manipularea piețelor în ecosistemul crypto.....	485
A. Mecanisme vechi, putere nouă.....	485
B. Fapta prevăzută de legea penală	488
C. Săvârșirea cu vinovăție	489
D. Caracterul nejustificat și imputabilitatea	490
Concluzii	493
Capitolul III. Provocări probatorii și strategii investigative.....	497
Introducere	497
3.1. De la adresă blockchain la persoană fizică - metoda celor trei cercuri	498
A. Cercul 1. Analiza on-chain – construirea comportamentului entității digitale	498
B. Cercul 2. Legătura cu serviciile centralizate - intersecția cu lumea reglementată.....	501
C. Cercul 3. Dovada controlului și a intenției în lumea fizică	508
3.2. Stabilirea jurisdicției: de la locul săvârșirii la locul impactului și al controlului exercitat de autor	512
A. Provocarea: actul de executare algoritmic săvârșit „nicăieri” și „pretutindeni”	512
B. Criterii de stabilire a jurisdicției în practica națională și internațională	516
C. Cauze-pilot: analiza unor hotărâri (naționale și internaționale) relevante	520
3.3. Conservarea și administrarea probelor digitale: capturarea fantomei imutabile	522
A. Specificul probei on-chain: necesitatea „certificării”, nu a „conservării”	523
B. Lanțul siguranței custodiale pentru probele digitale auxiliare.....	526
3.4. Cooperarea internațională - între reacția lentă a mecanismelor MLAT și urgența blockchain-ului	530
A. Limitările mecanismelor MLAT în fața vitezei mediului crypto	533
B. Canale alternative mai flexibile	536
C. Echipele Comune de Investigație (JIT): cadrul suprem al cooperării integrate	539
Concluzii.....	541
3.5. Dovedirea elementului subiectiv - marea provocare	542
A. Anatomia intenției în spațiul digital: de la concept la indicii probatorii.....	544
B. Strategii tipice de dovedire a intenției frauduloase.....	546
C. Instrumentele procurorului: de la expertiza tehnică la psihologia digitală	549

Cuprins

D. Provocări și limite: când intenția nu rezultă dincolo de orice îndoială rezonabilă	553
Concluzii	557
Partea a IV-a. Arhitectura tehnică a spălării banilor prin blockchain	561
Introducere	561
Titlul I. Anonimizarea tehnică imediată	563
Introducere	563
Capitolul I. Mixers și tumblers: arhitectura tehnică a anonimatului financiar.....	565
1.1. Perspectiva tehnică: fragmentarea deterministă a traseelor	565
1.2. Încadrarea juridică și controversa instrumentelor de confidențialitate.....	571
1.3. Cazuri emblematice: de la Bitcoin Fog la Tornado Cash.....	577
A. ChipMixer (2011-2023)	577
B. Bitcoin Fog (2011-2021)	579
C. Tornado Cash (august 2022 - prezent)	581
Concluzii	582
Capitolul II. Chain hopping (bridge hopping): fragmentarea jurisdicțională a traseelor	585
2.1. Dincolo de limitele mixerului pe un singur blockchain	585
2.2. Perspectiva tehnică: exploatarea discontinuității registrelor	587
2.3. Încadrarea juridică și provocarea jurisdicțională multiplicată	597
2.4. Cazuri emblematice: de la Ronin la Axie Infinity.....	603
A. Atacul Ronin Network	603
B. Atacul Wormhole Bridge	606
C. Dispariția fondurilor platformei FTX	608
Capitolul III. Privacy coins: confidențialitatea ca arhitectură fundamentală.....	611
3.1. De la disimularea post-factum la anonimatul nativ	611
3.2. Perspectiva tehnică: radiografia confidențialității criptografice	615
3.3. Încadrarea juridică, reacția organismelor de reglementare și răspunsul piețelor.....	622
3.4. Cazuri emblematice: AlphaBay, Hydra și ecosistemul darknet	629
A. AlphaBay Market	629
B. Hydra Market	631
C. WannaCry Ransomware	633
Concluzii	635
Capitolul IV. Exfolierea lanțurilor de tranzacții: fragmentarea sistematică	637
4.1. Complementaritatea cu mecanismele de disimulare primară	637
4.2. Perspectiva tehnică: anatomia fragmentării progresive.....	638

A. Peel chain	638
B. Smurfing	640
C. Combinarea cu alte mecanisme de disimulare	642
D. Instrumentele de detecție	644
4.3. Încadrarea juridică și provocarea probatorie în cazul mecanismelor de fragmentare	646
A. Provocări probatorii specifice în faza de anchetă	648
B. Provocări probatorii specifice în fața instanței	651
C. Aspecte procedurale specifice	653
4.4. Cazuri emblematic: de la Bitfinex la Twitter Hack	654
A. Bitfinex Hack (august 2016)	654
B. Schema Ponzi PlusToken (2018-2019)	655
C. Atacul asupra Twitter (iulie 2020)	657
Concluzii	659
Titlul II. Legitimizarea prin instrumente financiare descentralizate (DeFi)	661
Introducere	661
Capitolul I. DEX-uri și conversii descentralizate: spălarea prin ecosistemul financiar fără porți de verificare	663
1.1. De la anonimizare tehnică la legitimizare prin utilizare	663
1.2. Perspectiva tehnică: arhitectura schimburilor fără intermediari	664
A. Mecanismele tehnice de conversie utilizate în spălarea fondurilor	667
B. Vulnerabilități și limitări ale DEX-urilor în activitățile de spălare a banilor	671
1.3. Încadrarea juridică și dilema instrumentelor neutre	673
A. Nevoia de reglementare vizează punctele de interfață	676
B. Elementul probator în investigații DEX	679
C. Cooperarea internațională și provocări jurisdicționale	682
D. Provocări specifice în procedurile penale	682
1.4. Cazuri emblematic: de la Uranium Finance la Poly Network	684
A. Atacul asupra Uranium Finance	684
B. Atacul asupra Poly Network	687
C. Atacul asupra DAO Marker	690
D. Atacul de tip Front-End asupra BadgerDAO	694
1.5. Statistici Chainalysis 2023 privind spălarea de bani prin DEX-uri	698
Capitolul II. Protocoale de lending și scheme de self-lending: justificarea prin mecanisme aparent legitime	702
Introducere: de la conversie la construcția narațiunii de legitimitate	703
2.1. Perspectiva tehnică: arhitectura împrumuturilor descentralizate	703
A. Mecanismul fundamental Compound/Aave	704
B. Exploatarea pentru spălarea banilor – schemele de tip self-lending	707
C. Variante sofisticate	708

Cuprins

D. Flash Loans în contextul lending – manipulare și obscurizare	714
E. Exploatarea pentru disimulare și obscurizare	716
F. Vulnerabilități și limitări.....	719
2.2. Încadrarea juridică și provocarea demonstrării scopului ilicit	723
A. Elementul subiectiv – dovada intenției de disimulare	724
B. Provocări distinctive în proceduri penale.....	728
C. Scenarii de contestare din partea apărării	729
D. Cooperarea internațională – complexități jurisdicționale.....	734
2.3. Cazuri emblematice: de la Harvest Finance la Cream Finance	736
A. Exploatarea platformei Harvest Finance	736
B. Exploatarea protocolului Cream Finance	740
C. Atacul asupra protocolului bZx	746
2.4. Statistici generale Chainalysis/Elliptic privind spălarea banilor prin mecanisme de creditare descentralizată	750
Capitolul III. Maximizarea profitului și furnizarea de lichiditate:	
legitimizarea prin amestecare cu capitalul organic al pieței.....	754
Introducere. De la transformare și justificare la integrare completă.....	754
3.1. Perspectiva tehnică: generarea de randament descentralizat.....	756
A. Mecanismul fundamental: bazine de lichiditate în DEX-uri	757
B. Complexitatea maximă: obținerea de randamente succesive.....	762
C. Împrumuturi rapide pentru obținerea de randamente – legitimare aparentă.....	764
D. Vulnerabilități și limitări.....	766
E. Blockchain analytics – recunoașterea tiparelor.....	768
3.2. Încadrarea juridică și provocarea probatorie	770
A. Elementul subiectiv – dovedirea intenției.....	770
B. Provocări distinctive în proceduri penale.....	774
C. Argumente aduse de apărare.....	776
D. Cooperarea internațională – provocări.....	780
3.3. Cazuri emblematice: de la Meerkat Finance la Uranium Finance	781
A. Cazul Meerkat Finance	781
B. Atacul asupra protocolului Venus.....	786
C. Atacul asupra protocolului Indexed Finance.....	790
D. Din nou despre atacul asupra BadgerDAO	795
3.4. Statistici Chainalysis/Elliptic privind spălarea prin mecanisme de tip yield farming	797
Titlul III. Construcția narațiunii	803
Introducere. De la camuflarea originii la fabricarea unei legende credibile	803
Capitolul I. Platforme de pariuri și jocuri de noroc: legenda	
„câștigătorului norocos”	805
1.1. Perspectiva tehnică: arhitectura platformelor descentralizate de gambling și gaming	807

A. Mecanismele tehnice de spălare prin jocuri.....	815
B. Vulnerabilități și limitări ale jocurilor pentru activitățile de spălare a banilor	821
1.2. Încadrarea juridică și dovedirea caracterului fals al narațiunii	823
A. Elementul subiectiv – intenția de a crea o narațiune falsă	824
B. Provocări specifice în proceduri penale	826
C. Cooperarea internațională – provocări extreme.....	828
1.3. Cazuri emblematic: de la PlusToken la Conti Ransomware.....	830
A. PlusToken: Ponzi-ul care a convertit fraudă în „noroc”	831
B. Conti: profesionalizarea spălării în atacuri de tip ransomware	831
C. CriptoRom Networks: de la promisiuni romanțate la arhitecturi de legitimare.....	833
1.4. Statistici privind spălarea banilor prin platforme de pariuri și jocuri de noroc în mediul crypto	837
A. Raportul Chainalysis 2023.....	837
B. Ghidul FATF – 2023 (Financial Action Task Force)	838
C. Lecții pentru practicianul dreptului.....	840
Capitolul II. Simularea activităților de mining și staking:	
fabricarea istoriei tehnice	845
Introducere. Exploatarea imposibilității verificării trecutului	845
2.1. Perspectiva tehnică: arhitectura mining/staking și fabricarea evidențelor	849
A. Mining – fundamentele tehnice relevante	850
B. Staking – Proof-of-Stake și vulnerabilități similare	851
C. Simularea mineritului (mining-ului)	853
D. Simularea activităților de mining prin manipularea istoricului tranzacțional	855
E. Fabricarea documentației – consolidarea narațiunii false	856
F. Simularea activităților de staking – estomparea originii capitalului.....	857
G. Vulnerabilitățile interne ale simulării activităților de mining și staking.....	859
2.2. Încadrarea juridică și demonstrarea falsității narațiunii tehnice.....	861
A. Elementul subiectiv – intenția de a disimula printr-o narațiune falsă	862
B. Provocări distinctive în procedurile penale.....	864
2.3. Cazuri emblematic: de la BitConnect la Ruja Ignatova	866
A. Schema BitConnect: piramida financiară reinventată ca legendă de mining timpuriu.....	867
B. Schema OneCoin: Ruja Ignatova și industrializarea narațiunii de minerit fals	869
C. Escrocherii în contextul ofertelor ICO	871
2.4. Statistici generale privind narațiunile fictive de mining/staking în spălarea banilor	874
Capitolul III. Proiecte crypto false ca metodă de integrare	877
Introducere. Fabricarea întregului context economic	877

Cuprins

3.1. Perspectiva tehnică: arhitectura lansărilor de tokenuri și exploatarea lor	879
A. Fundamentele tehnice ale unui ICO – arhitectura invizibilă a unui token.....	879
B. Mecanismele tehnice de spălare prin oferte inițiale de tokenuri	881
C. Vulnerabilitățile spălării de bani prin oferte inițiale sau lansare de token.....	886
3.2. Încadrarea juridică și dezmembrarea ecosistemului economic fictiv.....	889
3.3. Cazuri emblematic: de la Centra Tech la OneCoin.....	890
A. Centra Tech – transformarea unei iluzii tehnologice în mecanism de fraudare a investitorilor.....	891
B. Bitconnect – ICO-ul care a amplificat o schemă Ponzi într-un mecanism global de disimulare a fondurilor	895
C. Cazul PlexCoin – reacția rapidă a autorităților în cazul unui risc sistemic.....	897
Titlul IV. Integrarea în economia reală	900
Capitolul I. Tranzacții P2P/OTC și servicii integrate:	
 poarta către economia tradițională	902
1.1. Pragul critic al integrării în economia la vedere.....	902
1.2. Piețele P2P: anonimatul prin descentralizare	903
1.3. Tranzacții de tip OTC: volum mare fără întrebări.....	908
1.4. Servicii financiare integrate sau de tip „matrioșcă”	915
1.5. Strategii investigative și probatorii	921
Capitolul II. Monede virtuale stabile ca pivot spre monede fiduciare:	
 ieșirea din virtual	926
2.1. Stablecoins: aparența stabilității, realitatea disimulării.....	927
2.2. Conversiile repetate: când volatilitatea zero devine armă	931
2.3. ATM-uri crypto: anonimatul fizic în era digitală	936
2.4. Carduri crypto: digitalul anonim în analogic	941
2.5. Distribuția geografică: sub radar prin fragmentare spațială	944
2.6. Concluzii investigative: de la digital la fizic, de la cod la cash	947
Capitolul III. Integrarea finală în economia reală: închiderea buclei	952
3.1. Reconectarea la sistemul financiar tradițional.....	953
3.2. Achiziții de bunuri de lux: averea digitală care poate fi atinsă.....	957
3.3. Investiții aparent legitime: afaceri ca mecanisme de spălare.....	963
3.4. Reconectarea bancară: de la crypto înapoi la IBAN.....	970
3.5. Provocări probatorii și strategii investigative.....	975
3.6. Dimensiunea preventivă: construirea rezilienței sistemului.....	978
3.7. Concluzii: lanțul complet – de la program informatic la active imobiliare.....	983
Titlul V. Disimularea continuă	986
Capitolul I. Structurarea și fragmentarea tranzacțională:	
 arta de a rămâne sub radar	988
1.1. Conceptul de structurare: de la banking tradițional la blockchain.....	989

1.2. Transpunerea structurării în ecosistemul blockchain.....	992
A. Dimensiunea 1. Fragmentarea tehnică prin scindarea valorii.....	994
B. Dimensiunea 2. Temporizarea	995
C. Dimensiunea 3. Distribuția geografică și între platforme	997
D. Dimensiunea 4. Utilizarea de intermediari umani (smurfi)	999
1.3. Indicatori statistici și tehnici de detectare automatizată.....	1001
A. Indicatorul 1. Prejudicata valorilor uniforme (round number bias)	1004
B. Indicatorul 2. Frecvența temporală regulată (periodic timing)	1005
C. Indicatorul 3. Tiparul de împrăștiere (fan-out) urmat de integrare (fan-in)	1006
1.4. Evoluția tacticilor de structurare și contramăsuri	1008
A. Randomizare controlată.....	1008
B. Structurarea intermediară.....	1010
1.5. Aspecte de calificare juridică și construcție probatorie	1012
Capitolul II. Zgomotul tranzacțional și tehnici de confuzie:	
când volumul ia locul disimulării.....	1017
2.1. Filosofia zgomotului: ascunderea prin abundență	1018
2.2. Atacuri de dispersie inversate: contaminarea cu microtranzacții	1020
A. Mecanismul tehnic al împrăstierii inversate	1022
B. Impactul investigativ și contramăsuri	1025
C. Ilustrare practică și recomandări procedurale.....	1027
2.3. Salturile între blockchain-uri ca metodă de disimulare	1029
A. Logica discontinuității: de la zgomot intern la fragmentare interlanț	1030
B. Mecanismele tehnice ale salturilor între blockchain-uri - recapitulare	1031
C. Cum pot fi exploatate aceste mecanisme în scop de disimulare.....	1034
D. Impactul cumulativ asupra investigației.....	1035
E. Indicatori de detectare pentru chain hopping.....	1037
2.4. Manipularea volumelor și tranzacții circulare	1039
A. Scopul manipulării volumelor: între simulare economică și sabotaj analitic.....	1040
B. Detectarea tranzacțiilor circulare.....	1042
C. Combinarea tehnicilor: zgomot stratificat.....	1044
2.5. Provoacări probatorii și strategii de răspuns ale organelor de anchetă	1046
Capitolul III. Arbitrajul jurisdicțional și structuri corporate offshore:	
navigarea fragmentării legale globale	1048
3.1. Conceptul de „arbitraj jurisdicțional”: exploatarea asimetriilor legislative	1049
3.2. Tipologia jurisdicțiilor: de la prietenoase la ostile	1051
A. Jurisdicții cu reglementare strictă și cooperare ridicată.....	1054
B. Jurisdicții cu reglementare emergentă sau selectivă	1055
C. Paradisuri fiscale și jurisdicții offshore tradiționale.....	1057
D. Jurisdicții non-cooperante sau ostile	1058
3.3. Structuri corporative offshore: anatomia opacității	1059
A. Societăți fără substanță economică (shell companies).....	1061

Cuprins

B. Stratificarea corporativă (corporate layering): piramide de entități.....	1063
C. Trust-uri și fundații: opacitate prin construcții fiduciare.....	1064
3.4. Strategii de detectare și de penetrare a structurilor offshore	1065
A. Strategia 1. Identificarea punctelor de concentrare a controlului	1067
B. Strategia 2. Colaborare internațională intensivă și coordonată	1068
C. Strategia 3. Utilizarea mecanismelor de sancționare și listare	1070
D. Strategia 4. „Urmărește banii” prin analiză comportamentală consolidată	1071
3.5. Evoluția legislativă: închiderea golurilor juridictionale	1072
A. Directive europene succesive (4AMLD, 5AMLD, 6AMLD).....	1074
B. Regula „informația însoțește transferul” (travel rule) în materia activelor virtuale – standardizarea globală a trasabilității	1079
C. Inițiative de transparență globală: Crypto-Asset Reporting Framework (CARF) – fiscalitatea ca instrument de vizibilitate sistemică	1082
3.6. Concluzii. Răspunsul judiciar la fragmentarea juridictională globală.....	1085
A. Asimetria dintre criminalitatea globală și răspunsul fragmentat.....	1086
B. Principii strategice pentru investigații multi-jurisdicționale eficiente.....	1088
C. Dimensiunea tehnologică: instrumente care reduc dependența de cooperare juridictională	1091
D. Aspecte de calificare juridică și construcție probatorie în instanță	1094
E. Privind în perspectivă: către un sistem global de transparență crypto?	1096
F. Integrarea cu celelalte tehnici de disimulare: vedere de ansamblu.....	1097
Partea a V-a. Spălarea banilor în blockchain și cadrul legislativ național	1101
Introducere	1101
Capitolul I. Cadrul juridic al spălării banilor. România în context comparat.....	1103
1.1. Legislația română privind spălarea banilor	1103
1.2. Cadrul european și internațional – armonizare și diversitate.....	1113
1.3. Diversitatea abordărilor naționale – când standardul probator determină eficiența	1117
Concluzii	1125
Capitolul II. Dubla provocare – dovedirea infracțiunii predicat și a spălării banilor în blockchain.....	1127
2.1. Provocări probatorii și legătura lor cu infracțiunea predicat (recapitulare)	1127
2.2. Scenarii practice în care infracțiunea predicat nu poate fi suficient dovedită	1130
A. Scenariul 1. Infracțiunea predicat identificată tehnic, autor neidentificat la standardul probator cerut	1130
B. Scenariul 2. Infracțiunea predicat se află în zonă juridică gri – incertitudinea calificării	1132
C. Scenariul 3. Infracțiunea predicat comisă în jurisdicție non-cooperantă – imposibilitatea obținerii probelor	1134

D. Scenariul 4. Infrațiunea predicat comisă în trecutul îndepărtat – degradarea și/sau dispariția probelor	1136
2.3. Paradoxul probator în contextul blockchain.....	1138
A. Cazul tipic. Arhitectură perfectă de spălare cu infrațiune predicat nedovedită.....	1138
2.4. Implicații practice pentru autoritățile judiciare naționale – strategii și limitări.....	1145
A. Strategii defensive ale autorului – exploatarea cerințelor probatorii	1145
Strategia 1. Mixarea originilor multiple – crearea incertitudinii despre sursa specifică	1146
Strategia 2. Trecerea timpului – hibernarea fondurilor pentru erodarea probelor	1147
Strategia 3. Segregarea geografică între infrațiunea predicat și procesul de spălare a activelor.....	1149
B. Strategii ofensive ale procurorului – posibilități reale și limitări structurale	1151
Capitolul III. Soluții posibile și perspective de lege ferenda.....	1160
3.1. Limitele abordării actuale – constatare realistă, nu critică.....	1160
3.2. Soluții legislative posibile – modificări de substanță	1162
A. Opțiunea 1. Atenuarea standardului probator pentru infrațiunea predicat în cazuri crypto	1162
B. Opțiunea 2. Incriminarea ca infrațiune independentă a faptei de structurare, divizare, fragmentare a fondurilor (structuring).....	1165
C. Opțiunea 3. Confiscarea activelor nedovedite ca urmare a inversării sarcinii probei (Unexplained Wealth Orders)	1169
3.3. Soluții practice sub legislația actuală – îmbunătățiri incrementale.....	1173
A. Investiții în creșterea capacității investigative și în specializarea investigatorilor.....	1173
B. Cooperare internațională prin echipe comune de anchetă	1175
C. Valorificarea proactivă a rapoartelor Oficiului Național de Prevenire și Combatere a Spălării Banilor	1176
D. Selectivitate strategică	1176
3.4. Perspective realiste: termen scurt, mediu și lung	1177
A. Pe termen scurt (unu până la trei ani)	1177
B. Pe termen mediu (trei până la șapte ani)	1178
C. Pe termen lung (șapte ani și mai mult)	1179
Concluzii. Soluții există, dar implementarea necesită voință (politică) și timp	1180
Bibliografie	1183