

Krzysztof Piech

Grzegorz Sobiecki

Witold Srokosz

Kom pen dium Block chain

Zagadnienia prawne

Wydawnictwo
Naukowe
Helion 

Autorzy: Agnieszka Babińska, Marcin Frankowski, Arkadiusz Gajdamowicz, Katarzyna M. Gorzkowska, Michał Gromek, Daniel J. Hornung, Damian R. Jaworski, Krzysztof M. Józwiak, Marcin Kózka, Wojciech Kuliński, dr Aleksandra Ossowska, dr hab. Krzysztof Piech, dr Kamil Polak, Małgorzata Reszka, Max Richards, dr inż. Przemysław Rodwald, dr Grzegorz Sobiecki, dr hab. Witold Srokosz, dr hab. Konrad Zacharzewski.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz wydawca dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz wydawca nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Redaktor prowadzący: Natalia Hermansa

Recenzja naukowa: prof. dr hab. Włodzimierz Szpringer,
Szkoła Główna Handlowa w Warszawie

Projekt okładki: Studio Gravite/Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Grafika na okładce została wykorzystana za zgodą AdobeStock.com.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: helion@helion.pl
WWW: helion.pl (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
helion.pl/user/opinie/komb12
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-289-0664-8

Copyright © Helion S.A. 2026

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

Wstęp	11
--------------------	-----------

CZĘŚĆ I. PRZESTĘPSTWA NA RYNKU KRYPTOAKTYWÓW

ROZDZIAŁ 1. Oszustwa na rynku kryptoaktywów — ujęcie prawne	25
Wprowadzenie	25
1.1. Inwestycje na rynku kryptoaktywów	25
1.1.1. Rynek kryptoaktywów	27
1.1.2. Mechanizmy inwestowania	30
1.1.3. Cechy rynku kryptoaktywów sprzyjające popełnianiu przestępstw	33
1.2. Modus operandi sprawców przestępstw	35
1.2.1. Socjotechnika	36
1.2.2. Pump and dump	38
1.2.3. Pranie pieniędzy	40
1.3. Przegląd orzecznictwa	42
1.3.1. Kryptowaluty a pranie pieniędzy	42
1.3.2. Stałe źródło dochodu	44
Podsumowanie	44
Bibliografia	45
ROZDZIAŁ 2. Oszustwa, regulacje i entuzjaści rynku kryptoaktywów	49
Wprowadzenie	49
2.1. Metodologia badań	50
2.1.1. Analiza sentymentu na Twitterze	50
2.1.2. Dane ankietowe	52
2.1.3. Wywiady	53
2.2. Skala oszustw na rynkach kryptowalut	54
2.3. Sposoby ochrony użytkowników	59
2.4. Entuzjaści rynku kryptoaktywów	60
2.5. Regulacje rynku kryptoaktywów	63
Podsumowanie	66
Bibliografia	67
ROZDZIAŁ 3. Ryzyka prawne i technologiczne związane z ICO oraz mechanizmy ochrony inwestorów	69
Wprowadzenie	69
3.1. Specyfika ICO jako mechanizmu wysokiego ryzyka	70
3.1.1. Asymetria informacji i brak dojrzałych standardów ujawnień	70
3.1.2. Ryzyka technologiczne związane ze smart kontraktami	71
3.1.3. Ryzyka instytucjonalne i jurysdykcyjne	72
3.2. Typologia nadużyć i niepowodzeń na rynku ICO	73
3.2.1. Oszustwa inwestycyjne w emisjach ICO	73
3.2.2. Manipulacje marketingowe i informacyjne w ICO	75
3.2.3. Cyberataki i nadużycia tożsamościowe w ekosystemie ICO	76

3.3. Studia przypadków wybranych nieprawidłowości w projektach ICO	77
3.3.1. The DAO — błąd smart kontraktu i spór o zasadę „code is law”	78
3.3.2. AriseBank — przykład klasycznego oszustwa inwestycyjnego w formule ICO	79
3.3.3. Centra Tech — manipulacje marketingowe i wykorzystanie celebrytów do promocji ICO	80
3.4. Mechanizmy ograniczania ryzyka i ochrony inwestorów na rynku ICO	82
3.4.1. Due diligence projektów ICO i ocena ich wiarygodności	82
3.4.2. Audyt bezpieczeństwa smart kontraktów	83
3.4.3. Rola giełd kryptowalutowych i model IEO	83
3.4.4. Znaczenie regulacji i nadzoru na rynku ICO	83
3.5. Podsumowanie	84
Bibliografia	85
ROZDZIAŁ 4. Wash trading na rynku NFT	87
Wprowadzenie	87
4.1. Handel tokenami NFT	87
4.2. Zjawisko wash tradingu	89
4.3. Przegląd literatury	92
4.4. Opis danych i metodologia badań	95
4.4.1. Ekstrakcja danych	95
4.4.2. Modelowanie	97
4.5. Wyniki badań	99
Podsumowanie	102
Załącznik: opis zmiennych	103
Bibliografia	104
ROZDZIAŁ 5. Możliwości deanonimizacyjne w świecie kryptowalut	106
Wprowadzenie	106
5.1. Modele transakcji	106
5.2. Heurystyki grupowania adresów	110
5.2.1. Heurystyka 1. (transakcje z wieloma adresami wejściowymi)	111
5.2.2. Heurystyka 2. (identyfikacja adresu reszty)	111
5.3. Systemy deanonimizacyjne	113
5.4. Wyzwania	115
Podsumowanie	118
Bibliografia	118
ROZDZIAŁ 6. Blockchain oraz uczenie maszynowe w identyfikowaniu oszustw finansowych	120
Wprowadzenie	120
6.1. Skala oszustw finansowych	121
6.2. Informacje o projekcie badawczym	126
6.3. Rozwiązywane problemy badawcze i technologiczne	127
6.4. Wybrane wyniki prac nad doбором komponentów i algorytmów blockchajna	128
6.5. Wybrane wyniki badań nad modelami uczenia maszynowego	130
Podsumowanie	131
Bibliografia	132
ROZDZIAŁ 7. Blockchain w walce z dezinformacją i fake newsami	135
Wprowadzenie	135
7.1. W świecie postprawdy, blockchajna i sztucznej inteligencji	136
7.2. Dlaczego blockchain?	140
7.3. Rozwiązania	141

7.4. Autorstwo, integralność i historia zmian publikowanych treści	142
7.5. Weryfikowanie prawdziwości treści	144
7.6. Koncepty weryfikacji wiadomości w mediach społecznościowych	150
7.7. Wyzwania i perspektywy	153
Podsumowanie	154
Bibliografia	155
ROZDZIAŁ 8. Crowdfunding kryptowalutowy na Telegramie jako źródło finansowania najemników i zakupów broni we wschodniej Ukrainie	158
Wprowadzenie	158
8.1. Wykorzystanie kryptowalut w finansowaniu nielegalnej działalności	159
8.2. Metody pozyskiwania finansowania przez nielegalne grupy najemnicze	161
8.2.1. Synergia szyfrowanej komunikacji na Telegramie i kryptowalut w aktywności nielegalnych podmiotów	162
8.2.2. Promowanie crowdfundingu kryptowalutowego w kanałach Telegram na przykładzie grupy Rusicz	164
8.3. Finansowanie grup prorosyjskich za pomocą kryptowalut i Telegramu — analiza przypadku	165
8.3.1. Cele badania	166
8.3.2. Istniejące regulacje	167
8.3.3. Wnioski z badania	167
8.4. Wizualizacja przepływów transakcji	168
8.5. Rozbieżność między regulacjami a podejściem sektora kryptowalutowego do rosyjskich PMSC	171
8.5.1. Wpływ sankcji Unii Europejskiej na sektor kryptowalutowy	172
8.5.2. Zaostrzenie sankcji — ósmy pakiet sankcji Unii Europejskiej	172
8.6. Rekomendacje	173
8.6.1. Rola technologii blockchain w finansowaniu najemników	174
8.6.2. Możliwości przeciwdziałania nielegalnemu finansowaniu najemników	175
8.7. Wnioski	175
Podsumowanie	176
Bibliografia	177

CZĘŚĆ II. EWOLUCJA OTOCZENIA REGULACYJNEGO DLA KRYPTOAKTYWÓW W POLSCE

ROZDZIAŁ 9. Narodziny i wczesny rozwój polskiego rynku kryptoaktywów	181
Wprowadzenie	181
9.1. Krajobraz pierwszych polskich giełd kryptowalutowych	183
9.1.1. Bitomat i Mt.Gox	183
9.1.2. Międzynarodowy kontekst problemów giełd kryptowalutowych	184
9.1.3. Problemy i upadki na polskim rynku giełd	185
9.1.4. Bitcurex — od lidera do upadku	185
9.1.5. Nadpodaż giełd i presja kosztowa	186
9.1.6. Przyczyny i konsekwencje niestabilności rynku	186
9.2. Początki górnictwa cyfrowego w Polsce	187
9.3. Rozwój społeczności kryptowalutowych w Polsce	189
9.3.1. Powstanie Polskiego Stowarzyszenia Bitcoin	189
9.3.2. Pierwsze inicjatywy edukacyjne, naukowe i rozwój dialogu branżowego	190
9.3.3. Pierwsze stanowisko Ministerstwa Finansów	193

9.3.4. Minimalne standardy bezpieczeństwa — pionierska inicjatywa samoregulacyjna i dialog z instytucjami	194
9.4. Polscy kryptografowie i badacze systemów rozproszonych wobec kryptowalut i technologii blockchain	197
9.4.1. Bitcoin jako narzędzie budowy protokołów kryptograficznych	197
9.4.2. Od Proof-of-Space do SpaceMint i Chia	198
9.4.3. Bezpieczeństwo wydobywania i krytyczna analiza Bitcoina	199
9.4.4. Kryptograf jako ekspert publiczny	200
9.4.5. Kontynuacje poza pierwszym okresem rozwoju rynku	200
9.4.6. Znaczenie polskiego wkładu	201
9.5. Ewolucja i wyzwania na rynku polskich giełd kryptowalut	201
9.5.1. BitBay — wzrost lidera i pierwsze wyzwania	202
9.5.2. Bitcurex i BitMarket — dalsza działalność i jej zakończenie	203
9.5.3. Relacje z bankami — narastający problem	204
9.6. Polskie start-upy kryptowalutowe — pierwsze globalne sukcesy i inicjatywy	206
9.6.1. Golem Network — pionierskie ICO i wizja zdecentralizowanego superkomputera	206
9.6.2. InPay — prekursor płatności bitcoinowych i pionier crowdfundingu udziałowego	207
9.6.3. Coinfirm — RegTech po polsku, czyli czy możliwe jest zbudowanie mostu między blockchainem a regulacjami	208
9.7. Działania edukacyjne, infrastrukturalne i samoregulacyjne środowiska	209
Podsumowanie	210
Bibliografia	211

ROZDZIAŁ 10. Między innowacyjnością a ostrożnością —

samoregulacja i dialog branży kryptoaktywów z administracją publiczną w Polsce (2016 – 2017)	217
Wprowadzenie	217
10.1. Geneza dialogu państwo – branża kryptoaktywów	218
10.1.1. Kontekst polityki cyfryzacji państwa	218
10.1.2. Powołanie Strumienia „Blockchain i kryptowaluty”	219
10.2. Faza konstruktywnego dialogu i jego granice	223
10.2.1. Organizacja i dynamika prac Strumienia w 2017 roku	224
10.2.2. Merytoryczne kierunki prac Strumienia — przegląd projektów	225
10.2.3. Kanon dobrych praktyk — pionierski akt samoregulacji branży	230
10.3. Reakcje instytucji państwowych na rozwój rynku i inicjatywy branżowe	232
10.3.1. Ministerstwo Cyfryzacji jako katalizator dialogu z branżą oraz parasol ochronny dla wczesnych innowacji	233
10.3.2. Ministerstwo Finansów — ostrożność fiskalna, pierwsze konsultacje i sygnały systemowej regulacji	234
10.3.3. Stanowisko nadzoru finansowego	235
10.3.4. Zainteresowanie parlamentarzystów	237
10.3.5. Aktywność pozostałych instytucji i organów państwowych	239
10.4. Polski Akcelerator Technologii Blockchain — wizja, działania i upadek	241
10.4.1. Geneza, model działania i wsparcie instytucjonalne	241
10.4.2. Kluczowe projekty i inicjatywy wdrożeniowe	243
10.4.3. Kryzys finansowy i upadek akceleratora	245
10.5. Niezależna infrastruktura wsparcia ekosystemu	248
Podsumowanie	249
Bibliografia	250

ROZDZIAŁ 11. Polski rynek kryptoaktywów w przededniu MiCA — błędy regulacyjne i utracone szanse (2018 – 2024)	254
Wprowadzenie	254
11.1. Rok 2018 — konfrontacja, regulacje i samoorganizacja branży	255
11.1.1. Wczesne objęcie rynku walut wirtualnych reżimem AML/CFT — ustawa z 1 marca 2018 roku i jej konsekwencje	255
11.1.2. „Kryzys podatkowy” — spór o podatek od czynności cywilnoprawnych	257
11.1.3. Systemowa zmiana podatkowa — nowelizacja ustaw o PIT i CIT	259
11.1.4. Profesjonalizacja ekosystemu i odpowiedź branży	260
11.2. Boom na ICO i jego wpływ na polski rynek (2017 – 2018)	263
11.2.1. Polski rynek na fali globalnego fenomenu	263
11.2.2. Reakcja nadzoru — komunikat KNF w sprawie ICO	264
11.3. Konstrukcja rejestru VASP i jej skutki (2019 – 2021)	266
11.3.1. Próżnia instytucjonalna po ustawie AML z 2018 roku	266
11.3.2. Proces legislacyjny rejestru VASP — ograniczony dialog z rynkiem	268
11.3.3. Międzynarodowe doświadczenia w zakresie sandboxów regulacyjnych	271
11.3.4. Ograniczony rozwój sandboxu regulacyjnego w Polsce	272
11.4. Polska na tle wczesnych prac nad MiCA (2019 – 2024)	274
11.4.1. Impuls dla Europy — od „FinTech Action Plan” do efektu projektu Libra	274
11.4.2. Ograniczona obecność Polski w pracach przygotowawczych nad MiCA	276
11.4.3. Granice analogii PSD2 – MiCA i ryzyka przenoszenia rozwiązań	276
11.4.4. Działania na zapleczu — Polska w europejskich projektach technologicznych	279
Podsumowanie	280
Bibliografia	281
ROZDZIAŁ 12. Smart kontrakty w świetle polskiego prawa — zarys problematyki regulacyjnej	285
Wprowadzenie	285
12.1. Definicja smart kontraktów	286
12.2. Cechy smart kontraktów	289
12.3. Smart kontrakt jako umowa w rozumieniu prawa cywilnego?	292
12.4. Wykonanie smart kontraktu	299
12.5. Odpowiedzialność za błędy w kodzie	302
Podsumowanie	305
Bibliografia	307
ROZDZIAŁ 13. Zabezpieczenia majątkowe na kryptoaktywach	310
Wprowadzenie	310
13.1. Zarys instytucji zabezpieczenia majątkowego w postępowaniu karnym	311
13.2. Kryptoaktywa jako przedmiot zabezpieczenia w świetle przepisów postępowania karnego oraz rozporządzenia MiCA	314
13.3. Kluczowe problemy z realizacją zabezpieczenia majątkowego na kryptoaktywach	317
Podsumowanie	320
Bibliografia	322

ROZDZIAŁ 14. Tokeny NFT a prawo autorskie	323
Wprowadzenie	323
14.1. Charakterystyka NFT w kontekście prawa autorskiego	323
14.2. Status prawnoautorski tokenów NFT	325
14.3. Tworzenie i zawartość NFT a prawa do utworu	326
14.4. Obrót tokenami NFT a prawa autorskie	327
14.4.1. Charakter prawny transakcji NFT	329
14.4.2. Publiczne udostępnianie i dozwolony użytek	330
14.4.3. Kwestia droit de suite	331
14.5. Czy NFT stanowi nowe pole eksploatacji?	332
Podsumowanie	333
Bibliografia	334

CZĘŚĆ III. REGULACJE PRAWNE DOTYCZĄCE KRYPTOAKTYWÓW

ROZDZIAŁ 15. Czy można skutecznie sankcjonować niezmienny smart kontrakt?	
Analiza przypadku Tornado Cash	339
Wprowadzenie	339
15.1. Ramy prawne sankcji finansowych	341
15.1.1. Sankcje finansowe jako instrument polityki	341
15.1.2. OFAC — kluczowa instytucja w systemie amerykańskim	342
15.1.3. Podstawy prawne — IEEPA	344
15.1.4. Pojęcie własności w prawie sankcyjnym	345
15.1.5. Sankcje a nowe technologie	346
15.2. Tornado Cash i niezmiennosc smart kontraktów	346
15.2.1. Mechanizm działania miksera Tornado Cash	346
15.2.2. Zdecentralizowana struktura i brak podmiotu kontrolującego	347
15.2.3. Niezmiennosc — istota problemu	347
15.3. Sankcje OFAC wobec Tornado Cash (2022)	348
15.3.1. Kontekst nałożenia sankcji	348
15.3.2. Reakcja branży i organizacji pozarządowych	349
15.3.3. Problem egzekucji sankcji wobec zdecentralizowanego protokołu	350
15.4. Problem niezmienności i wyrok Fifth Circuit (2024)	351
15.4.1. Niezmiennosc jako wyzwanie dla prawa sankcyjnego	351
15.4.2. Sprawa Van Loon v. Department of the Treasury	352
15.4.3. Studium przypadku — Alexey Pertsev (Holandia, 2024)	353
15.4.4. Studium przypadku — Roman Storm (USA, 2025)	353
15.4.5. Perspektywa porównawcza — prawo publiczne a prawo karne	354
15.5. Zniesienie sankcji przez OFAC (2025)	355
15.5.1. Kontekst decyzji	355
15.5.2. Powody zniesienia sankcji	356
15.5.3. Reakcje rynku i organizacji społecznych	356
15.5.4. Znaczenie decyzji dla przyszłości sankcji wobec DeFi	356
15.6. Perspektywa prawnoporównawcza	357
15.6.1. Regulacje Unii Europejskiej — MiCA, TFR oraz pakiet AML	357
15.6.2. Wielka Brytania i podejście „common law”	360
15.6.3. Azja — przykład Singapuru i Japonii	361
15.6.4. FATF i standardy globalne	361
Podsumowanie	362
Bibliografia	363

ROZDZIAŁ 16. Unijne rozporządzenie w sprawie rynków kryptoaktywów	366
Wprowadzenie	366
16.1. Podstawy unijnego prawodawstwa	366
16.2. Charakter prawny rozporządzenia UE	367
16.3. Procedura ustawodawcza	368
16.4. Zarys najistotniejszych regulacji rozporządzenia MiCA	370
16.4.1. Kontekst i motywy przyjęcia rozporządzenia	370
16.4.2. Przegląd przepisów rozporządzenia MiCA	373
16.4.3. Skutki stosowania MiCA	378
Podsumowanie	379
Bibliografia	381
ROZDZIAŁ 17. Emisja tokena będącego e-pieniędzem w prawie Unii Europejskiej ...	382
Wprowadzenie	382
17.1. Zakres zastosowania rozporządzenia MiCA w odniesieniu do EMT	385
17.2. Obowiązki emitenta EMT wynikające z rozporządzenia MiCA	386
17.2.1. Uzyskanie zezwolenia na prowadzenie działalności	387
17.2.2. Sporządzenie dokumentu informacyjnego dotyczącego kryptoaktywa	387
17.2.3. Odpowiednie formułowanie komunikatów marketingowych	388
17.2.4. Odpowiednie wykorzystywanie środków otrzymanych w zamian za EMT	388
17.2.5. Ustanowienie i utrzymywanie tzw. planu naprawy i planu wykupu	388
17.2.6. Zakaz przyznawania odsetek	389
17.2.7. Znaczące EMT	389
17.3. Relacja między rozporządzeniem MiCA a aktami normującymi świadczenie usług płatniczych z punktu widzenia emitenta EMT	391
17.4. Zasadność „rozszczepienia regulacyjnego” EMT	393
Podsumowanie	394
Bibliografia	396
ROZDZIAŁ 18. Czynności maklerskie w obrocie aktywami cyfrowymi	398
Wprowadzenie	398
18.1. Kwestie terminologiczne	399
18.2. Podstawy prawne świadczenia usług oraz podstawy wykorzystania analogii	401
18.3. Ogólne zasady świadczenia usług maklerskich w obrocie aktywami cyfrowymi	403
18.4. Podobieństwo czynności maklerskich w obrocie aktywami cyfrowymi do czynności maklerskich w obrocie instrumentami finansowymi	406
18.5. Reżim odpowiedzialności	408
Podsumowanie	409
Bibliografia	410
ROZDZIAŁ 19. Cyberbezpieczeństwo ekosystemu kryptoaktywów: zagrożenia i podatności oraz mechanizmy obronne	412
Wprowadzenie	412
19.1. Ramy koncepcyjne cyberbezpieczeństwa kryptoaktywów	413
19.1.1. Definicje podstawowych pojęć	413
19.1.2. Triada CIA w ekosystemie kryptoaktywów	413
19.1.3. Podstawowi sprawcy zagrożeń i ich motywy	415
19.1.4. Trzy wymiary cyberbezpieczeństwa blockchainów	416
19.2. Zagrożenia dla infrastruktury technologicznej blockchain	417
19.2.1. Ataki na mechanizmy konsensusu	417
19.2.2. Podatności w oprogramowaniu węzłów	418

19.2.3. Bezpieczeństwo warstwy sieciowej P2P	419
19.2.4. Podatności kryptograficzne	420
19.3. Zagrożenia związane ze smart kontraktami i zdecentralizowanymi aplikacjami	421
19.3.1. Typowe błędy i podatności w kodzie smart kontraktów	421
19.3.2. Ataki wykorzystujące logikę biznesową i mechanizmy ekonomiczne	422
19.3.3. Bezpieczeństwo mostów międzyłańcuchowych	423
19.3.4. Ryzyka na rynku NFT	424
19.3.5. Zagrożenia dla DAO	425
19.4. Zagrożenia dla platform scentralizowanych	426
19.5. Zagrożenia dla użytkowników końcowych	427
19.6. Strategie mitygacji ryzyka i środki zaradcze	430
19.7. Wyzwania	433
Podsumowanie	435
Bibliografia	437

ROZDZIAŁ 20. Regulacje Unii Europejskiej w zakresie cyberbezpieczeństwa ekosystemu kryptoaktywów	440
Wprowadzenie	440
20.1. Geneza i kontekst regulacji cyberbezpieczeństwa kryptoaktywów w UE	441
20.1.1. Geneza rozporządzenia MiCA w kontekście strategii finansów cyfrowych UE	442
20.1.2. MiCA na tle dotychczasowych ram finansowych — znaczenie dla cyberbezpieczeństwa	443
20.2. Analiza rozporządzenia MiCA pod kątem cyberbezpieczeństwa	443
20.2.1. Zakres podmiotowy MiCA w kontekście cyberbezpieczeństwa	444
20.2.2. Zakres przedmiotowy MiCA w kontekście cyberbezpieczeństwa	444
20.2.3. Status prawny i daty stosowania	445
20.2.4. Ogólne zasady i definicje związane z cyberbezpieczeństwem w rozporządzeniu MiCA	445
20.2.5. Wymogi cyberbezpieczeństwa dla emitentów (ART i EMT)	446
20.2.6. Wymogi cyberbezpieczeństwa dla dostawców usług w zakresie kryptoaktywów	448
20.3. Rozporządzenie DORA i jego implikacje dla cyberbezpieczeństwa rynku kryptoaktywów	449
20.3.1. Cel i zakres zastosowania rozporządzenia DORA	449
20.3.2. Główne filary wymogów rozporządzenia DORA	450
20.3.3. Znaczenie rozporządzenia DORA dla podmiotów rynku kryptoaktywów	451
20.4. Potencjalne implikacje dyrektywy NIS2 dla sektora kryptoaktywów	451
20.4.1. Zakres podmiotowy NIS2 a rynek kryptoaktywów	452
20.4.2. Kluczowe wymogi dyrektywy NIS2 i potencjalne nakładanie się rozporządzeń MiCA i DORA	452
20.4.3. Interakcja NIS2 z MiCA i DORA	453
20.4.4. Implikacje dla sektora kryptoaktywów	454
Podsumowanie	454
Bibliografia	456

Informacje o autorach	457
------------------------------------	------------

Skorowidz	459
------------------------	------------

Wstęp

Przedstawiamy Państwu drugi tom z serii „Kompendium blockchain”, zatytułowany *Zagadnienia prawne rynku kryptoaktywów*. Jest to wieloautorska monografia naukowa, która stanowi próbę kompleksowej analizy jednego z najbardziej dynamicznych i złożonych obszarów współczesnej gospodarki i prawa. Publikacja ukazuje się w symbolicznym momencie — w 2026 roku, gdy w pełni obowiązuje już unijne rozporządzenie w sprawie rynku kryptoaktywów (MiCA), które zmienia krajobraz technologiczno-finance w Europie. Prace nad drugim tomem trwały blisko dwa lata i wymagały wielokrotnego przeglądu każdego rozdziału, aby zapewnić najwyższą jakość merytoryczną.

Publikacja została przygotowana z myślą o szerokim i zróżnicowanym gronie odbiorców. Będzie ona cennym źródłem wiedzy dla **prawników, sędziów i prokuratorów**, którzy w swojej praktyce stykają się z nowymi formami przestępczości. Okaże się niezbędna dla **pracowników instytucji finansowych, organów nadzoru i legislatorów**, którzy muszą zrozumieć i stosować nowe ramy regulacyjne. Zainteresuje **przedsiębiorców i menedżerów** z sektora FinTech, szukających sposobów na legalne i bezpieczne prowadzenie działalności. Wreszcie, będzie stanowić kompendium wiedzy dla **środowiska akademickiego, analityków i studentów** badających skrzyżowanie prawa, finansów i technologii.

Na polskim rynku wydawniczym brakowało dotąd pozycji, która w tak holistyczny sposób podchodziłaby do zagadnień związanych z prawnymi i kryminologicznymi aspektami kryptoaktywów. Wierzymy, że książka, którą oddajemy w Państwa ręce, wypełnia tę lukę. Jej główne wyróżniki to:

- **Kompleksowość i interdyscyplinarność** — książka łączy w sobie trzy kluczowe perspektywy:
 1. **kryminologiczną**, szczegółowo opisując mechanizmy przestępstw;
 2. **historyczno-regulacyjną**, śledząc fascynującą ewolucję polskiego ekosystemu;
 3. **prawno-analityczną**, dokonując analizy najważniejszych aktów prawnych, z unijnym rozporządzeniem MiCA na czele.
- **Pionierski charakter i rzetelność** — przedstawiamy pierwsze na polskim rynku tak obszerne opracowanie, które nie opiera się na publicystycznych uproszczeniach, lecz na analizie faktów, studiach przypadków i egzegezie aktów prawnych. Zespół autorów, składający się z czołowych ekspertów i praktyków, gwarantuje wysoki poziom merytoryczny.
- **Praktyczny wymiar** — publikacja stanowi bezpośrednią odpowiedź na wyzwania związane z wejściem w życie przełomowych regulacji, a jej praktyczny wymiar, widoczny w analizie konkretnych oszustw, procesów regulacyjnych i ich konsekwencji, czyni ją użytecznym narzędziem w codziennej pracy profesjonalistów.

Należy w tym miejscu podkreślić, że poglądy i przekonania wyrażane przez autorów poszczególnych rozdziałów nie zawsze odpowiadają poglądom i przekonaniom redaktorów tomu.

Zawartość książki i wnioski z poszczególnych rozdziałów

Drugi tom trylogii podzielony jest na trzy główne części:

1. Część I (rozdziały 1. – 8.) zajmuje się kwestiami nieprawidłowości rynkowych.
2. Część II (rozdziały 9. – 14.) analizuje ewolucję otoczenia regulacyjnego dla kryptoaktywów w Polsce.
3. Część III (rozdziały 15. – 20.) jest poświęcona aktualnej prawnej regulacji kryptoaktywów.

Rozdział 1., „Oszustwa na rynku kryptoaktywów — ujęcie prawne”

W rozdziale otwierającym, autorstwa Małgorzaty Reszki, dokonano wszechstronnej analizy oszustw inwestycyjnych w ekosystemie kryptoaktywów z perspektywy prawa. Rozdział charakteryzuje specyfikę tego rynku, wskazując na jego niedojrzałość, podatność na wahania oraz niedostateczne uregulowanie jako czynniki sprzyjające działalności przestępczej. Autorka szczegółowo omawia *modus operandi* sprawców, opisując zarówno techniki socjotechniczne, wzmacniane dziś przez technologię deepfake, jak i nadużycia związane z platformami crowdfundingowymi, schematami *pump & dump* czy praniem pieniędzy. Unikalną wartością rozdziału jest oparcie analizy nie tylko na ramach teoretycznych i raportach Europolu, ale również na dogłębnym przeglądzie orzecznictwa polskich sądów, które już teraz zajmują się sprawami łączącymi obrót kryptowalutami z tradycyjną przestępczością zorganizowaną.

Kluczowym wnioskiem z lektury jest konstatacja, że polski wymiar sprawiedliwości, mimo braku dedykowanych regulacji karnych, już teraz stosuje istniejące instrumenty prawne (m.in. z Kodeksu karnego) do ścigania przestępstw związanych z kryptoaktywami. Rozdział ten w sposób plastyczny ukazuje, jak abstrakcyjne pojęcia z unijnych rozporządzeń, takich jak MiCA, znajdują swoje odbicie w konkretnych stanach faktycznych rozpatrywanych przez sądy, co stanowi pomost między teorią a praktyką i podkreśla pilną potrzebę dalszej profesjonalizacji organów ścigania.

Rozdział 2., „Oszustwa, regulacje i entuzjaści rynku kryptoaktywów”

Rozdział autorstwa Maxa Richardsa prezentuje oryginalne, empiryczne badania poświęcone trzem obszarom ekosystemu kryptoaktywów: oszustwom, regulacjom i społeczności entuzjastów. Punktem wyjścia jest wskazanie skali problemu — dane amerykańskiej Federalnej Komisji Handlu (FTC) pokazują wysoką wartość strat, a w eksploracyjnej próbie 34 respondentów 16% zadeklarowało, że zna osobę, która padła ofiarą oszustwa związanego z projektem kryptowalutowym. Cechą wyróżniającą ten rozdział jest jego unikalna metodologia, łącząca analizę sentymentu danych z platformy Twitter (obecnie X), badania ankietowe prowadzone w społecznościach Discord oraz wywiady z ekspertami. Na szczególną uwagę zasługuje studium przypadku promocji tokena Ethereum Max przez

Kim Kardashian, gdzie autor, za pomocą analizy sentymentu, mierzy wpływ mediów społecznościowych na postrzeganie projektów kryptowalutowych zarówno przed, jak i po interwencji regulatora.

Wnioski płynące z rozdziału wskazują, że media społecznościowe są głównym kanałem informacyjnym dla inwestorów, ale jednocześnie stanowią podstawowe narzędzie manipulacji i dezinformacji. Co równie istotne, autor demaskuje głęboki rozdzźwięk między idealistycznymi podstawami Bitcoina a rynkową praktyką, gdzie większość użytkowników wciąż polega na scentralizowanych podmiotach.

Rozdział 3., „Ryzyka prawne i technologiczne związane z ICO oraz mechanizmy ochrony inwestorów”

Rozdział analizuje zjawisko przestępczości związanej z emisją cyfrowych tokenów w ramach Initial Coin Offering (ICO). Marcin Frankowski omawia najczęstsze formy nadużyć towarzyszących kampaniom ICO — od oszustw inwestycyjnych i działania na szkodę inwestorów po wyłudzenia o charakterze zorganizowanym. Zostają przedstawione konkretne przykłady nielegalnych praktyk, w tym znikanie zebranych środków (tzw. *rug pull*), brak realizacji projektów oraz manipulowanie informacjami i dokumentacją. W dalszej części rozdziału zaprezentowano środki ochrony inwestorów — zarówno te wynikające z samoregulacji branży, jak i z ram prawnych oraz orzecznictwa. Autor poddaje krytycznej analizie skuteczność obecnych rozwiązań, zwracając uwagę na potrzebę dalszego rozwoju regulacji i instrumentów nadzoru. Podkreśla również rolę świadomości inwestorów oraz edukacji jako istotnego elementu prewencji.

Rozdział 4., „Wash trading na rynku NFT”

W tym rozdziale dr Kamil Polak koncentruje się na zjawisku *wash tradingu* na rynku niewymienialnych tokenów (NFT), czyli sztucznym zawyżaniu wolumenu obrotu i ceny aktywów. Autor przedstawia teoretyczne podstawy tego procederu, jego motywacje (m.in. inflacja ceny i pranie pieniędzy) oraz techniki jego realizacji, ilustrując je niezwykle obrazowymi przykładami zaczerpniętymi z narzędzi analitycznych, które pokazują sieć powiązań setek portfeli kontrolowanych przez jedną osobę. Rdzeniem rozdziału jest prezentacja autorskiej metodyki badawczej, opartej na zaawansowanych narzędziach analizy danych i uczenia maszynowego (algorytm *k*-średnich) w celu identyfikacji i kwantyfikacji tego zjawiska na platformie OpenSea.

Najważniejszym wynikiem jest zidentyfikowanie klastrów nr 5 i 7, obejmujących 2,16% badanych portfeli, jako grup potencjalnie związanych z wash tradingiem. Rozdział stanowi ciekawe studium przypadku zastosowania nowoczesnych metod kryminalistyki cyfrowej (*on-chain forensics*). Pokazuje, w jaki sposób analitycy, regulatorzy i organy ścigania mogą wykorzystywać transparentność technologii blockchain do wykrywania złożonych schematów manipulacji rynkowej.

Rozdział 5., „Możliwości deanonimizacyjne w świecie kryptowalut”

W tym rozdziale dr inż. Przemysław Rodwald w sposób przystępny i precyzyjny wprowadza czytelnika w świat deanonimizacji, czyli procesu pozwalającego na łączenie pseudonimowych adresów blockchain z realnymi podmiotami. Autor omawia podstawowe

modele transakcji w sieci Bitcoin, a następnie przechodzi do sedna zagadnienia — heurystyk, czyli metod wnioskowania pozwalających grupować adresy w klastry należące do jednego użytkownika. Co szczególnie interesujące, rozdział przedstawia konkretne przykłady i wizualizacje działania różnych systemów deanonimizacyjnych — zarówno komercyjnych, jak i darmowych — pokazując, jak ten sam adres analizowany jest przez różne platformy. Rozdział zamyka omówienie wyzwań, takich jak miksery kryptowalut, które mają na celu zwiększenie anonimowości transakcji.

Kluczowy wniosek jest dość jednoznaczny: pseudonimowość transakcji w publicznych blockchainach jest w dużej mierze iluzoryczna. Rozwój zaawansowanych narzędzi analitycznych, opartych na dobrze ugruntowanych heurystykach, pozwala z dużą skutecznością śledzić przepływ środków i identyfikować podmioty stojące za konkretnymi adresami. Dla organów ścigania jest to potężne narzędzie, ale dla użytkowników ceniących prywatność stanowi to fundamentalne wyzwanie, napędzające „wyścig zbrojeń” między technikami deanonimizacji i anonimizacji.

Rozdział 6., „Blockchain oraz uczenie maszynowe w identyfikowaniu oszustw finansowych”

Autorzy rozdziału, Wojciech Kuliński i Krzysztof Piech, przedstawiają studium przypadku implementacji zaawansowanych technologii w odpowiedzi na realne wyzwania sektora finansowego. Treść koncentruje się na wynikach projektu badawczo-rozwojowego „Open Banking Anti Fraud PSD2”, zrealizowanego przez polską spółkę FinTech — Igoria Trade. Rozdział ten stanowi unikalne spojrzenie na praktyczne aspekty łączenia technologii blockchain i uczenia maszynowego. W sposób niezwykle szczegółowy przedstawiono w nim zarówno dobór komponentów technologicznych, jak i mierzalne wyniki wydajności stworzonego systemu, zdolnego do przetwarzania milionów transakcji dziennie. Autorzy prezentują także porównanie skuteczności różnych algorytmów uczenia maszynowego w wykrywaniu anomalii.

Najważniejszy wniosek ma charakter empiryczny i praktyczny: badania potwierdziły wykonalność prototypu systemu antyfraudowego łączącego technologię blockchain i uczenie maszynowe. Uzyskane wyniki dotyczą wydajności, zdolności modeli do rozróżniania klas i audytowalności rozwiązania; nie stanowią jednak potwierdzenia skuteczności systemu w warunkach produkcyjnych ani redukcji rzeczywistych strat z oszustw.

Rozdział 7., „Blockchain w walce z dezinformacją i fake newsami”

W tym rozdziale Krzysztof M. Józwiak dokonuje szerokiego przeglądu zastosowań technologii blockchain jako narzędzia do walki z dezinformacją. Autor osadza problem w szerokim kontekście społecznym — w tzw. epoce postprawdy i ekonomii uwagi — a następnie systematycznie analizuje, w jaki sposób kluczowe cechy blockchajna mogą się stać fundamentem budowy bardziej wiarygodnego ekosystemu informacyjnego. W rozdziale przedstawiono całe spektrum istniejących i proponowanych rozwiązań: od systemów uwierzytelniania treści i ich autorstwa, przez platformy do zbiorowej weryfikacji faktów (*fact-checking*), aż po zdecentralizowane systemy medialne. Oryginalność rozdziału polega na odejściu od czysto finansowych zastosowań blockchajna i pokazaniu jego ogromnego potencjału w rozwiązywaniu jednego z ważniejszych wyzwań społecznych XXI wieku.

Głównym wnioskiem płynącym z analizy jest stwierdzenie, że technologia blockchain, zwłaszcza w połączeniu ze sztuczną inteligencją, oferuje zestaw narzędzi, które mogą pomóc w budowie „ekonomii dowodów” (*evidence economy*) jako alternatywy dla obecnej „ekonomii uwagi”.

Rozdział 8., „Crowdfunding kryptowalutowy na Telegramie jako źródło finansowania najemników i zakupów broni we wschodniej Ukrainie”

Rozdział autorstwa Michała Gromka jest unikalnym na polskim rynku i bardzo aktualnym studium przypadku, które w przystępny sposób pokazuje „ciemną stronę” wykorzystania kryptoaktywów. Autor, bazując na analizie ponad trzech tysięcy rosyjskojęzycznych kanałów na platformie Telegram, dokumentuje *modus operandi* prorosyjskich grup paramilitarnych, które wykorzystują kryptowaluty do finansowania swojej działalności. Cechą wyróżniającą rozdział jest rygorystyczna metodologia, łącząca wywiad jawnoźródłowy (OSINT) z zaawansowaną analizą danych on-chain. Czytelnik znajdzie tu fascynujące i jednocześnie niepokojące wizualizacje przepływów finansowych, które pokazują drogę środków od anonimowych darczyńców, przez portfele donacyjne, aż po największe globalne giełdy kryptowalut.

Z rozdziału płynie dwojaki, lecz niezwykle istotny wniosek. Po pierwsze, pokazuje on w praktyce, jak synergia szyfrowanych komunikatorów i kryptoaktywów tworzy wysoce efektywny i trudny do zablokowania mechanizm finansowania nielegalnej działalności. Po drugie, udowadnia, że dzięki transparentności publicznych blockchainów i zaawansowanym narzędziom analitycznym możliwe jest precyzyjne śledzenie tych środków. Ujawnia to paradoks kryptowalut: choć mogą one służyć działalności przestępczej, jednocześnie dostarczają organom ścigania bezprecedensowych narzędzi do jej zwalczania.

Rozdział 9., „Narodziny i wczesny rozwój polskiego rynku kryptoaktywów”

Ten rozdział, przygotowany przez Krzysztofa Piecha, jest unikalną na polskim rynku próbą historycznej rekonstrukcji pionierskiego okresu (lata 2010 – 2016), w którym kształtował się polski ekosystem kryptoaktywów. Autor, bazując na bogatym materiale źródłowym, w tym archiwalnych postach z forów dyskusyjnych, ukazuje fenomen spontanicznego i oddolnego rozwoju rynku. Czytelnik znajdzie tu fascynującą historię pierwszych polskich giełd kryptowalut, z głośnym przypadkiem Bitomat.pl na czele, którego przejęcie przez japoński Mt.Gox wprowadziło polskiego złotego do globalnego obrotu. Niezwykle interesującym wątkiem jest również przedstawienie Polski jako jednego z wczesnych światowych centrów *miningu* za sprawą projektów takich jak Polmine oraz produkcji specjalistycznego sprzętu (ASIC), co dowodzi ogromnego potencjału technologicznego tamtego okresu.

Wnioskiem płynącym z tego rozdziału jest to, że Polska, wbrew powszechnej opinii, nie była naśladowcą, lecz jednym z globalnych liderów i pionierów wczesnej ery Bitcoinu. To w naszym kraju powstały jedne z pierwszych giełd w Europie, tu rozwijała się zaawansowana produkcja sprzętu do wydobywania i tu rodziła się jedna z najaktywniejszych społeczności na świecie. Okres ten, choć chaotyczny i naznaczony głośnymi upadkami projektów, stworzył fundamenty kapitału ludzkiego i technologicznego, które zadecydowały o dalszym, dynamicznym rozwoju całej branży.

Rozdział 10., „Między innowacyjnością a ostrożnością — samoregulacja i dialog branży kryptoaktywów z administracją publiczną w Polsce (2016 – 2017)”

Kontynuując historyczną analizę, Krzysztof Piech opisuje w tym rozdziale wyjątkowy w skali Europy okres konstruktywnego dialogu między dynamicznie rozwijającą się branżą technologii blockchain a administracją publiczną w Polsce. Autor rekonstruuje genezę i działania powołanego w 2016 roku przy Ministerstwie Cyfryzacji Strumienia „Blockchain i kryptowaluty”. Była to unikalna platforma współpracy, łącząca start-upy, globalne korporacje, środowisko akademickie i przedstawiciele rządu w celu wspólnego kształtowania ram dla nowego sektora. Na szczególną uwagę zasługuje szczegółowe przedstawienie prac nad *Kanonem dobrych praktyk* — oddolną, branżową inicjatywą samoregulacyjną, która w wielu aspektach wyprzedzała późniejsze, formalne przepisy prawa.

Z rozdziału płynie fundamentalny wniosek: lata 2016 – 2017 dowodzą, że możliwy jest model regulacji oparty na partnerskim dialogu i proaktywnej samoorganizacji branży. Polska była wówczas polem bezprecedensowego eksperymentu, gdzie środowisko, świadome ryzyk, samo podjęło się stworzenia wysokich standardów bezpieczeństwa, zyskując w części administracji publicznej (kierowanej wówczas przez Annę Streżyńską) otwarcie na innowacje partnera. Okres ten pokazuje, jak dalece branża była gotowa do wzięcia odpowiedzialności za rynek, zanim państwo zdecydowało się na jednostronne interwencje.

Rozdział 11., „Polski rynek kryptoaktywów w przededniu MiCA — błędy regulacyjne i utracone szanse (2018 – 2024)”

Rozdział 11., pióra Krzysztofa Piecha, stanowi krytyczną analizę okresu, który nastąpił po zerwaniu dialogu państwo – branża, a który autor określa mianem „ery utraconych szans”. Treść koncentruje się na serii błędnych decyzji i zaniechań regulacyjnych. Niezwykle interesującym studium przypadku jest tu tzw. kryzys podatkowy z 2018 roku, wywołany przez próbę nałożenia podatku od czynności cywilnoprawnych (PCC) na każdą transakcję kryptoaktywami, co wywołało bezprecedensowe protesty społeczne. Jednak za najdotkliwszy błąd autor uznaje sposób implementacji V dyrektywy AML i stworzenie w 2021 roku krajowego rejestru VASP. Rozdział pokazuje, jak liberalne i pozbawione realnej weryfikacji kryteria doprowadziły do zarejestrowania w Polsce podmiotów o wątpliwej reputacji, kwestionując wiarygodność polskiego nadzoru i zamieniając rejestr w tzw. tanią banderę w skali Europy.

Kluczowy wniosek z tej analizy jest niezwykle gorzki: odejście od dialogu ze środowiskiem eksperckim prowadzi do tworzenia regulacji nieefektywnych, a nawet szkodliwych. Przypadek polskiego rejestru VASP jest modelowym przykładem, jak regulacja — stworzona w oderwaniu od realiów technologicznych i biznesowych — może przynieść efekt odwrotny do zamierzonego: zamiast budować zaufanie, osłabia wiarygodność państwa. W rezultacie Polska w kluczowym momencie kształtowania się ogólnoeuropejskich ram prawnych straciła zarówno impet innowacyjny, jak i wiarygodność, a także motywację do tego, by w sposób aktywny uczestniczyć w tworzeniu MiCA dla preforsowania polskich „racji”.

Rozdział 12., „Smart kontrakty w świetle polskiego prawa — zarys problematyki regulacyjnej”

Rozdział autorstwa Agnieszki Babińskiej jest próbą osadzenia smart kontraktów — jednego z fundamentalnych narzędzi technologii blockchain — w realiach polskiego systemu prawa cywilnego. Autorka w sposób metodyczny dekonstruuje to zjawisko, wychodząc od technicznych definicji i przechodząc do kluczowego pytania: czy i w jakim zakresie smart kontrakt może być uznany za prawnie wiążącą umowę? Szczególnie cenna jest szczegółowa analiza smart kontraktu przez pryzmat podstawowych instytucji prawa zobowiązań, takich jak oświadczenie woli, forma czynności prawnych czy zasada swobody umów. Wnikliwie omówiono cechy smart kontraktów, konfrontując je z elastycznością i wymogami tradycyjnych umów.

Najważniejszy wniosek płynący z lektury tego rozdziału jest taki, że polskie prawo cywilne, dzięki swojej elastyczności, jest w stanie „pomieścić” koncepcję smart kontraktu, jednak nie bez istotnych wyzwań interpretacyjnych. Autorka dowodzi, że samo wykorzystanie kodu nie wyklucza możliwości zawarcia skutecznej umowy, ale rodzi fundamentalne pytania o wykładnię oświadczeń woli i odpowiedzialność za błędy w kodzie.

Rozdział 13., „Zabezpieczenia majątkowe na kryptoaktywach”

Rozdział przygotowany przez Damiana R. Jaworskiego to wysoce specjalistyczna i unikalna analiza z pogranicza prawa karnego, procesowego i nowych technologii. Autor stawia fundamentalne pytanie: w jaki sposób organy ścigania mogą skutecznie zabezpieczyć kryptoaktywa na poczet przyszłych kar i roszczeń? Rozdział rozpoczyna się od zarysu ogólnej instytucji zabezpieczenia majątkowego w polskim prawie, by następnie przejść do sedna problemu, czyli trudności w zastosowaniu tych tradycyjnych narzędzi do aktywów cyfrowych. Wnikliwie przeanalizowano tu kluczowe przeszkody, takie jak niemożność uznania kryptowaluty za „rzecz ruchomą” w kontekście instytucji tymczasowego zajęcia mienia oraz problemy związane z zasadą adekwatności przy aktywach o wysokiej zmienności cen.

Główny wniosek jest tyleż klarowny, ileż alarmujący: obecne ramy polskiej procedury karnej są fundamentalnie nieprzystosowane do skutecznego zabezpieczania kryptoaktywów, co tworzy poważną lukę w systemie zwalczania przestępczości gospodarczej. Rozdział dowodzi, że bez pilnych i precyzyjnych zmian legislacyjnych, które uwzględnią unikalny, cyfrowy charakter tych aktywów, działania organów ścigania pozostaną obciążone wysokim ryzykiem proceduralnym i niską efektywnością.

Rozdział 14., „Tokeny NFT a prawo autorskie”

W ostatnim rozdziale tej części książki Arkadiusz Gajdamowicz i Krzysztof Piech dokonują dogłębnej analizy skomplikowanej relacji między niewymienialnymi tokenami (NFT) a prawem autorskim. Kluczowym wyróżnikiem rozdziału jest precyzyjne oddzielenie tokena NFT jako zapisu w blockchainie od utworu cyfrowego, z którym jest on powiązany. Autorzy systematycznie dekonstruują mit, jakoby nabycie NFT było równoznaczne z nabyciem praw autorskich. Analiza obejmuje kluczowe zagadnienia, takie jak status

prawnoautorski samego tokena, kwestia tworzenia i obrotu NFT w kontekście pól eksploatacji oraz problematyka stosowania takich instytucji jak *droit de suite* czy publiczne udostępnianie w kontekście linkowania.

Wnioski z lektury są fundamentalne dla zrozumienia rynku NFT. Po pierwsze, sam token NFT co do zasady nie jest utworem w rozumieniu prawa autorskiego. Po drugie, zakup NFT nie przenosi automatycznie autorskich praw majątkowych do powiązanego z nim dzieła. I wreszcie, po trzecie, istniejące konstrukcje prawne są w większości nieadekwatne do specyfiki transakcji NFT. Rozdział jasno pokazuje, że rynek ten funkcjonuje obecnie w dużej mierze w próżni interpretacyjnej, a jego przyszła stabilność będzie zależeć od ukształtowania się nowej praktyki kontraktowej oraz ewentualnych dedykowanych rozwiązań legislacyjnych.

Rozdział 15., „Czy można skutecznie sankcjonować niezmienny smart kontrakt?”

Rozdział autorstwa Marcina Kózki analizuje jeden z najbardziej kontrowersyjnych problemów współczesnego prawa kryptoaktywów — możliwość skutecznego stosowania sankcji gospodarczych wobec zdecentralizowanych i niezmiennych smart kontraktów. Punktem wyjścia jest sprawa Tornado Cash — protokołu służącego do zwiększania prywatności transakcji w sieci Ethereum — objętego w 2022 roku sankcjami przez amerykański Office of Foreign Assets Control (OFAC). Autor szczegółowo rekonstruuje zarówno podstawy prawne decyzji administracji USA, jak i późniejsze spory sądowe, ze szczególnym uwzględnieniem przełomowego wyroku *Van Loon v. Department of the Treasury*. Na szczególną uwagę zasługuje analiza napięcia między tradycyjnymi instrumentami prawa sankcyjnego a zdecentralizowaną architekturą technologii blockchain. Rozdział został dodatkowo wzbogacony o perspektywę porównawczą obejmującą regulacje Unii Europejskiej, Wielkiej Brytanii oraz standardy FATF dotyczące przeciwdziałania praniu pieniędzy i usług związanych z kryptoaktywami.

Najważniejszy wniosek płynący z rozdziału jest taki, że tradycyjne mechanizmy sankcyjne napotykają istotne ograniczenia w zetknięciu z protokołami zdecentralizowanymi, które nie posiadają klasycznej struktury właścicielskiej ani podmiotu kontrolującego. Autor pokazuje jednak, że egzekwowanie regulacji w praktyce nie znika, lecz przesuwają się na poziom pośredników — giełd, dostawców usług w zakresie kryptoaktywów (CASP), operatorów infrastruktury oraz podmiotów objętych obowiązkami AML/CFT. Rozdział stanowi jedno z pierwszych w polskiej literaturze kompleksowych opracowań łączących problematykę sankcji gospodarczych, zdecentralizowanych finansów (DeFi) oraz ewolucji międzynarodowych regulacji rynku kryptoaktywów.

Rozdział 16., „Unijne rozporządzenie w sprawie rynków kryptoaktywów (rozporządzenie MiCA)”

W rozdziale autorstwa Daniela J. Hornunga czytelnik otrzymuje dogłębne i ustrukturyzowane wprowadzenie do najważniejszego aktu prawnego dla europejskiego rynku kryptoaktywów — rozporządzenia MiCA. Rozdział ten ma charakter fundamentalny, ponieważ nie tylko omawia przepisy, ale również, co jest jego unikalną wartością, osadza je w szerszym kontekście całego systemu prawnego Unii Europejskiej. Autor w klarowny sposób wyjaśnia różnice między prawem pierwotnym i wtórnym, tłumaczy, dlaczego MiCA, jako rozporządzenie, jest bezpośrednio stosowane we wszystkich państwach członkowskich,

a także przybliży samą procedurę ustawodawczą, która doprowadziła do jego przyjęcia. Następnie szczegółowo omawia najważniejsze regulacje zawarte w rozporządzeniu MiCA.

Najważniejszy wniosek z lektury tego rozdziału jest taki, że rozporządzenie MiCA to nie tylko zbiór technicznych przepisów, ale przede wszystkim potężny instrument legislacyjny, mający na celu stworzenie jednolitego i zharmonizowanego rynku dla całej Unii Europejskiej.

Rozdział 17., „Emisja tokena będącego e-pieniędzem w prawie Unii Europejskiej”

W tym rozdziale dr Aleksandra Ossowska dokonuje wnikliwej analizy jednego, lecz wyjątkowo złożonego typu kryptoaktywa — tokena będącego e-pieniędzem (EMT). Rozdział stanowi przykład dogłębnej analizy prawnej. Jego największą wartością jest precyzyjne ukazanie hybrydowej natury prawnej EMT, który podlega jednocześnie regulacjom z dwóch światów: nowego rozporządzenia MiCA oraz dotychczasowych dyrektyw o pieniądzu elektronicznym (EMD2) i usługach płatniczych (PSD2). Autorka analizuje, w jaki sposób te reżimy prawne nakładają się na siebie, gdzie się uzupełniają, a gdzie rodzą potencjalne konflikty i wyzwania interpretacyjne. Na szczególną uwagę zasługuje omówienie tzw. rozszczepienia regulacyjnego jako świadomej decyzji prawodawcy.

Najważniejszy wniosek płynący z rozdziału jest taki, że regulacja tokenów EMT stanowi modelowy przykład złożoności legislacyjnej w erze FinTech. Ustawodawca unijny, zamiast tworzyć prawo od nowa, zdecydował się na nałożenie nowych przepisów MiCA na już istniejącą, dojrzałą strukturę prawa dotyczącego usług płatniczych oraz regulowanego pieniądza elektronicznego. Skutkuje to powstaniem skomplikowanego, wielowarstwowego reżimu prawnego, który z jednej strony ma zapewnić wysoki poziom ochrony, a z drugiej — stawia ogromne wyzwania przed emitentami i organami nadzoru w zakresie zapewnienia pełnej zgodności i spójności. Studium przypadku EMT pokazuje, jak trudne jest proste „kopiowanie” istniejących rozwiązań do świata nowych technologii.

Rozdział 18., „Czynności maklerskie w obrocie aktywami cyfrowymi”

W rozdziale autorstwa dr. hab. Konrada Zacharzewskiego podjęto próbę nowatorskiego spojrzenia na działalność dostawców usług w zakresie kryptoaktywów (CASP) przez pryzmat dobrze ugruntowanych instytucji prawa rynku kapitałowego. Autor stawia tezę, że czynności wykonywane przez giełdy i kantory kryptoaktywowe są w istocie funkcjonalnymi odpowiednikami tradycyjnych czynności maklerskich. Cechą wyróżniającą rozdział jest zastosowanie metody prawno-porównawczej i analogii do analizy oraz interpretacji przepisów rozporządzenia MiCA. Ta perspektywa pozwala wyjaśnić naturę prawną takich usług jak przyjmowanie i przekazywanie zleceń czy zarządzanie portfelem kryptoaktywów, odwołując się do bogatej spuścizny doktryny i orzecznictwa z zakresu obrotu instrumentami finansowymi.

Kluczowy wniosek, jaki płynie z tego rozdziału, ma fundamentalne znaczenie dla praktyki: pomimo braku bezpośredniego odesłania w przepisach MiCA — w procesie ich wykładni nie tylko można, ale wręcz należy posiłkować się dorobkiem prawa rynku kapitałowego. Taka metoda interpretacyjna pozwala na wypełnienie nieuniknionych luk i niejasności w nowym akcie prawnym, zapewniając spójność systemową oraz wyższy stopień przewidywalności dla uczestników rynku. Autor argumentuje, że choć jest to regulacja dla

nowego typu aktywów, jej logika jest głęboko zakorzeniona w sprawdzonych zasadach, które od lat rządzą rynkami finansowymi.

Rozdział 19., „Cyberbezpieczeństwo ekosystemu kryptoaktywów — zagrożenia i podatności oraz mechanizmy obronne”

Rozdział przygotowany przez Krzysztofa Piecha stanowi kompleksowe i panoramiczne kompendium wiedzy na temat cyberbezpieczeństwa całego ekosystemu kryptoaktywów. Wyróżnikiem tego opracowania jest jego holistyczne i trójwymiarowe podejście. Autor nie skupia się wyłącznie na technologii blockchain, lecz analizuje zagrożenia w trzech kluczowych obszarach: bezpieczeństwa samej infrastruktury technologicznej (ataki na mechanizmy konsensusu, luki w oprogramowaniu węzłów), bezpieczeństwa aplikacji i protokołów (exploity na smart kontraktach, ataki na DeFi i mosty międzyłańcuchowe) oraz bezpieczeństwa użytkowników końcowych (phishing, malware, oszustwa inwestycyjne). Każdą z kategorii zagrożeń autor ilustruje aktualnymi przykładami, a następnie przedstawia katalog strategii mitygacji i środków zaradczych.

Z lektury płynie fundamentalny wniosek, że cyberbezpieczeństwo w świecie kryptoaktywów jest zagadnieniem wielowymiarowym, a najsłabszym ogniwem bardzo często pozostaje czynnik ludzki. Nawet najlepiej zabezpieczona infrastruktura technologiczna jest podatna na zagrożenia, jeśli jej użytkownicy nie mają odpowiedniej wiedzy i świadomości. Dlatego skuteczna ochrona ekosystemu wymaga synergii działań na wszystkich poziomach — od zabezpieczeń technicznych, przez audyty kodu i standardy branżowe, aż po masową i nieustanną edukację użytkowników.

Rozdział 20., „Regulacje Unii Europejskiej w zakresie cyberbezpieczeństwa ekosystemu kryptoaktywów”

Ostatni rozdział w tym tomie, autorstwa Katarzyny M. Gorzkowskiej i Krzysztofa Piecha, jest analitycznym zwieńczeniem całej publikacji. W sposób systemowy pokazuje, w jaki sposób Unia Europejska odpowiedziała na zagrożenia zdiagnozowane w poprzednich częściach książki. Rdzeniem rozdziału jest szczegółowa analiza trzech filarów unijnego systemu cyberbezpieczeństwa: rozporządzenia MiCA, rozporządzenia DORA oraz dyrektywy NIS2. Unikalność tego ujęcia polega na tym, że autorzy nie omawiają tych aktów w izolacji, ale pokazują, jak ich przepisy wzajemnie się przenikają, uzupełniają i tworzą spójną (choć skomplikowaną) siatkę regulacyjną. Szczegółowo omówiono m.in. zakresy podmiotowe, kluczowe obowiązki dotyczące zarządzania ryzykiem ICT, zgłaszania incydentów oraz testowania odporności.

Kluczowy wniosek ma charakter strategiczny: Unia Europejska — poprzez synergiczne działanie MiCA, DORA i potencjalnie NIS2 — buduje kompleksowe regulacyjne ramy cyberbezpieczeństwa dla sektora kryptoaktywów. Celem tego podejścia jest podniesienie standardów i profesjonalizacja rynku na niespotykaną dotąd skalę, co ma zwiększyć bezpieczeństwo i zaufanie. Jednocześnie tak wysoki poziom regulacji stanowi ogromne wyzwanie implementacyjne i kosztowe, zwłaszcza dla mniejszych podmiotów, rodząc pytania o przyszłą konkurencyjność i innowacyjność europejskiego ekosystemu w skali globalnej. To właśnie znalezienie równowagi między bezpieczeństwem a wspieraniem innowacji będzie kluczowym wyzwaniem w nadchodzących latach.

Wnioski z książki

Z niniejszej książki wynikają następujące główne wnioski:

- 1. Fundamentalne napięcie między innowacją a regulacją.** Cała książka jest w istocie studium ogromnego napięcia między oddolną, dynamiczną i często chaotyczną innowacją technologiczną (charakterystyczną dla ekosystemu kryptoaktywów) a odgórną, z natury ostrożną i powolną potrzebą stabilności i bezpieczeństwa, którą reprezentują organy państwa, regulatorzy i nadzorcy. Sposób zarządzania tym konfliktem — widoczny zarówno w historycznej analizie rynku polskiego, jak i w porównaniu podejścia UE i USA — jawi się jako kluczowe wyzwanie, które decyduje o konkurencyjności i przyszłości całego sektora.
- 2. Podwójna, janusowa¹ natura transparentności blockchaina.** W wielu rozdziałach powraca wniosek, że transparentność publicznych blockchainów jest mieczem obojczy. Choć stwarza ona nowe wektory i możliwości dla działalności przestępczej, jednocześnie po raz pierwszy w historii finansów daje organom ścigania i analitykom bezprecedensowe narzędzia do publicznego śledzenia przepływów finansowych w czasie niemal rzeczywistym. To zmienia paradygmat zwalczania przestępstw gospodarczych.
- 3. Krytyczna rola dialogu i ryzyko jego zaniechania.** Historia polskiego rynku (a zwłaszcza kontrast między okresem 2016 – 2017 a latami późniejszymi) dostarcza uniwersalnej lekcji: konstruktywny i partnerski dialog między innowacyjną branżą a otwartymi na argumenty regulatorami jest warunkiem koniecznym do stworzenia zdrowego i konkurencyjnego ekosystemu. Jego zerwanie i zastąpienie jednostronnymi, niekonsultowanymi decyzjami prowadzi do tworzenia wadliwych regulacji i utraty szans gospodarczych.
- 4. Nieadekwatność tradycyjnych instrumentów prawnych.** Rozdziały poświęcone prawu autorskiemu (NFT), zabezpieczeniom majątkowym czy smart kontraktom systematycznie dowodzą, że bezpośrednie stosowanie tradycyjnych, stuletnich instytucji prawnych (jak „rzecz ruchoma”, forma pisemna, egzemplarz utworu) do zjawisk ze świata cyfrowego jest często nieadekwatne i prowadzi do powstawania luk prawnych oraz niepewności. Nowa technologia wymaga albo stworzenia dedykowanych rozwiązań, albo niezwykle świadomej i elastycznej interpretacji istniejących przepisów.
- 5. Siła i granice samoregulacji.** Polski *Kanon dobrych praktyk* z 2017 roku jest w książce przedstawiony jako studium przypadku pokazujące, że dojrzała i świadoma ryzyka branża jest w stanie sama wypracować wysokie standardy bezpieczeństwa, często bardziej rygorystyczne i lepiej dopasowane do realiów niż późniejsze regulacje państwowe. Jednocześnie historia ta pokazuje granice samoregulacji — jest ona bezsilna wobec braku dostępu podmiotów rynkowych do kluczowej infrastruktury, takiej jak rachunki bankowe.

¹ Od imienia Janusa (łac. *Ianus*) — jednego z najstarszych bóstw rzymskich, przedstawianego z dwiema twarzami zwróconymi w przeciwne strony. Określenie „janusowy” w sposób metaforyczny opisuje zjawisko, które ma dwoistą, często ambiwalentną lub sprzeczną naturę. W kontekście niniejszej książki odnosi się ono do faktu, że transparentność, będąca fundamentalną cechą publicznych blockchainów, z jednej strony stanowi potężne i bezprecedensowe narzędzie w rękach organów ścigania, regulatorów i analityków (co wykazano m.in. w rozdziałach 4., 5. i 8.), z drugiej zaś stwarza nowe wektory ataków i zagrożenia dla prywatności użytkowników.

6. Konieczność synergii prawa, edukacji i technologii. Jak refren powraca w całej książce wniosek, że ani same regulacje, ani sama technologia nie wystarczą, by zapewnić bezpieczeństwo ekosystemu. Ochrona przed oszustwami wymaga edukacji użytkowników, skuteczna walka z przestępczością zorganizowaną wymaga zaawansowanych narzędzi analitycznych, a bezpieczny rozwój rynku wymaga mądrych i proporcjonalnych ram prawnych. Jedynie synergia tych trzech filarów może przynieść trwałe rezultaty, o ile dołączy do tego element skutecznego stosowania prawa z poszanowaniem praworządności, tj. w polskich warunkach — sprawne postępowania przygotowawcze i sądowe.

7. Paradoks centralizacji w zdecentralizowanym świecie. Mimo że decentralizacja jest fundamentalną ideą stojącą za kryptoaktywami, z wielu rozdziałów wyłania się obraz postępującej centralizacji — zarówno na poziomie rynkowym (dominacja dużych giełd i platform), jak i regulacyjnym (wprowadzenie przez MiCA reżimu licencyjnego wzorowanego na tradycyjnych finansach). Tendencja ta, choć zrozumiała z perspektywy bezpieczeństwa, stanowi jedno z największych zagrożeń dla pierwotnej wizji i innowacyjnego potencjału technologii blockchain.

Głównym wnioskiem z niniejszej książki jest to, że znajdujemy się w środku fundamentalnego starcia dwóch paradygmatów:

1. oddolnej, zdecentralizowanej, przełomowej innowacji technologicznej z jednej strony oraz
2. odgórnego, scentralizowanego, tradycyjnego porządku prawnego i finansowego z drugiej.

Przyszłość i globalna konkurencyjność ekosystemu kryptoaktywów — zarówno w Polsce, jak i w Europie — będzie zależeć nie od tego, który z tych paradygmatów zwycięży, lecz od tego, czy decydenci i uczestnicy rynku potrafią znaleźć między nimi mądry, dynamiczny kompromis. Niniejsza książka jest w istocie przewodnikiem po ryzykach, szansach i narzędziach, które mogą w tym procesie pomóc.

Warszawa, czerwiec 2026 r.

Krzysztof Piech, Grzegorz Sobiecki, Witold Srokosz

ROZDZIAŁ 11.

Polski rynek kryptoaktywów w przededniu MiCA — błędy regulacyjne i utracone szanse (2018 – 2024)

Wprowadzenie

Na początku 2018 roku relacje między polskim rynkiem kryptoaktywów a administracją publiczną weszły w fazę wyraźnie bardziej ostrożnościową. Nie oznaczało to próżni regulacyjnej: obowiązywały już przepisy ogólne (w tym podatkowe i karne), a w marcu 2018 roku wprowadzono do polskiego porządku prawnego definicję „waluty wirtualnej” w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Zmienił się jednak sposób kształtowania polityki publicznej wobec tego rynku: częściej dominowały działania reaktywne (interpretacyjne i nadzorcze), a rzadziej narzędzia redukujące niepewność regulacyjną i wspierające testowanie nowych modeli biznesowych.

W niniejszym rozdziale analizowane są lata 2018 – 2024 jako okres poprzedzający rozpoczęcie stosowania rozporządzenia MiCA, gdy polski rynek kryptoaktywów przechodził od fazy szybkiego wzrostu (w tym boomu na ICO) do fazy narastającej regulacji oraz rosnącej presji instytucjonalnej. Teza rozdziału jest następująca: kluczowe instrumenty publiczne w Polsce były projektowane i wdrażane w sposób, który nie odpowiadał specyfice obrotu kryptoaktywami. Skutkiem były rozwiązania o ograniczonej jakości (w sensie spójności, proporcjonalności i przewidywalności), a także koszty i utracone korzyści po stronie rynku — w szczególności w obszarze innowacji, napływu kapitału w okresie boomu na ICO oraz zdolności do budowy wiarygodnych relacji z sektorem bankowym.

Pierwszym punktem zwrotnym była sprawa podatku od czynności cywilnoprawnych (PCC) w 2018 roku, kiedy komunikat Ministerstwa Finansów — wprowadzający opodatkowanie każdej transakcji w wysokości 1% jej wartości — uruchomił silną mobilizację społeczną i branżową, a następnie doprowadził do czasowego zaniechania poboru PCC oraz późniejszych zmian ustawowych. Drugim wątkiem była konstrukcja rejestru VASP, wprowadzona w 2021 roku jako narzędzie realizacji wymogu rejestracji w reżimie AML/CFT. Model wpisu przy formalnych i relatywnie łagodnych kryteriach *ex ante* nie dostarczał jednak selekcji merytorycznej ani mechanizmów budowy zaufania, a w praktyce generował napięcia w relacjach z bankami i ryzyka reputacyjne. Trzecim wątkiem była niejednoznaczna pozycja Polski w pracach przygotowawczych nad MiCA: przy ograniczonej widoczności doświadczeń krajowych w procesie unijnym równolegle realizowano działania technologiczne w inicjatywach europejskich, co pokazuje rozdzielenie ścieżki technologicznej i regulacyjnej.

Celem rozdziału jest możliwie precyzyjne odtworzenie sekwencji zdarzeń i mechanizmów instytucjonalnych, które doprowadziły do wskazanych rezultatów. Analiza ma charakter krytyczny, ale opiera się na rozróżnieniu pomiędzy faktami (daty aktów, konstrukcja instrumentów, przebieg działań instytucji) a interpretacją (ocena proporcjonalności i skutków). W tym sensie rozdział stanowi zarówno opis kluczowych epizodów w historii polskiego rynku kryptoaktywów, jak i studium ograniczeń polityki publicznej wobec innowacji finansowych w okresie poprzedzającym MiCA.

11.1. Rok 2018 — konfrontacja, regulacje i samoorganizacja branży

Rok 2018 stanowił cezurę w relacjach państwa z rynkiem kryptoaktywów, przynosząc zakończenie okresu intensywnej współpracy rządu i branży oraz zapoczątkowując okres jednostronnych interwencji regulacyjnych. Był to czas pełen sprzeczności: z jednej strony państwo wprowadziło pierwsze „twarde” regulacje, z drugiej — wywołało „kryzys podatkowy”, który ujawnił niezrozumienie specyfiki rynku. Równolegle, w odpowiedzi na globalny boom ICO i rosnącą presję, branża podjęła próbę profesjonalizacji, tworząc nowe struktury instytucjonalne.

11.1.1. Wczesne objęcie rynku walut wirtualnych reżimem AML/CFT — ustawa z 1 marca 2018 roku i jej konsekwencje

Pierwszym aktem prawnym, który w sposób bezpośredni i kompleksowy objął polski sektor walut wirtualnych, była ustawa z dnia 1 marca 2018 roku o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu¹ (dalej: AML). Jej wejście w życie 13 lipca 2018 roku (kwartał po ogłoszeniu) stanowiło fundamentalną zmianę, kończąc okres funkcjonowania branży w „szarej strefie” regulacyjnej i formalnie włączając ją do systemu finansowego państwa.

Ustawa ta — jeszcze przed przyjęciem AMLD5 — wprowadziła do polskiego porządku prawnego rozwiązania zbieżne z kierunkiem późniejszych zmian unijnych, obejmując część rynku walut wirtualnych reżimem AML/CFT. Ustawa wprowadziła do polskiego porządku prawnego kilka kluczowych elementów.

Po pierwsze, ustawa AML wprowadziła do polskiego porządku prawnego definicję **waluty wirtualnej** (art. 2 ust. 2 pkt 26) jako cyfrowego odwzorowania wartości, które **nie jest** emitowane ani gwarantowane przez bank centralny lub organ publiczny, **nie ma** statusu prawnego środka płatniczego, lecz jest akceptowane jako środek wymiany i może być przechowywane oraz przenoszone elektronicznie. Była to pierwsza w polskim prawie definicja o tak szerokim, funkcjonalnym ujęciu, potrzebna m.in. do zbudowania reżimu AML wobec podmiotów rynku kryptoaktywów. Jednocześnie definicja ta była projektowana przede wszystkim pod potrzeby regulacyjne (AML), a nie pod porządkowanie zjawiska od strony technologicznej: nie odwołuje się do cech technicznych, takich jak

¹ Ustawa z 1 marca 2018 roku o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. 2018 poz. 723).

decentralizacja czy mechanizm konsensusu, lecz operuje kryteriami funkcjonalnymi („akceptowane jako środek wymiany”). W konsekwencji ustawowy język zaczął „się rozjeżdżać” z językiem praktyki rynkowej: w tekście ustawy nie użyto popularnych w obiegu terminów („kryptowaluta” czy ewentualnie „waluta cyfrowa”), a posłużono się pojęciem przyjętym na poziomie prawa unijnego (tj. waluta wirtualna), które w polskim (czy europejskim) dyskursie branżowym w tamtym okresie nie było standardem. Warto także odnotować, że definicja zawiera **konkretne wyłączenia** (m.in. dla niektórych instrumentów płatniczych oraz jednostek rozliczeniowych stosowanych w ramach gier lub systemów o ograniczonym zastosowaniu), co pokazuje, że jej zakres wyznaczono przez cele funkcjonalne, a nie przez klasyfikację technologiczną aktywów.

Po drugie i najważniejsze, ustawa wprost zaliczyła **„podmioty prowadzące działalność w zakresie wymiany pomiędzy walutami wirtualnymi”** do katalogu **„instytucji obowiązanych”** (art. 2 ust. 1 pkt 12)². Oznaczało to, że od 13 lipca 2018 roku giełdy, kantory online oraz operatorzy portfeli zostali zobowiązani do stosowania pełnego reżimu AML/CFT, w tym do identyfikacji klientów (KYC), analizy ryzyka transakcji oraz raportowania podejrzanych aktywności (SAR) do Generalnego Inspektora Informacji Finansowej (GIIF).

Po trzecie, zdefiniowano, że środki utrzymywane na giełdach kryptowalutowych są przechowywane na „rachunkach” podobnych do rachunków bankowych oraz innych, analogicznych instrumentów³. Należy jednak podkreślić, że wejście w życie tych przepisów nie odbywało się w próżni. Polska branża w ramach zainicjowanego rok wcześniej *Kanonu dobrych praktyk* dobrowolnie zobowiązała się do stosowania standardów KYC i AML, zanim jeszcze stało się to wymogiem ustawowym. Był to dowód na dojrzałość sektora, który rozumiejąc ryzyka, wyprzedził działania legislatora. Mimo to ten akt proaktywnej samoregulacji nie został w pełni wykorzystany w dalszym dialogu, a ustawa była pierwszym przykładem regulacji narzucanej rynkowi, a nie współtworzonej z nim, co stało się charakterystyczne dla dalszych działań państwa w tym obszarze.

Warto również umieścić polskie działania w kontekście europejskim. Dyrektywa (UE) 2018/843 (AMLD5)⁴, przyjęta 30 maja 2018 roku, wymagała transpozycji do 10 stycznia 2020 roku. Polska na mocy ustawy z 1 marca 2018 roku już od 13 lipca 2018 objęła istotną część podmiotów z obszaru walut wirtualnych reżimem AML/CFT, co — na tle wielu państw UE, które wprowadzały porównywalne obowiązki bliżej terminu transpozycji — plasowało Polskę w grupie wczesnych implementatorów obowiązków AML. Wcześniej podobne przepisy wprowadziły jedynie Włochy, Estonia i Gibraltar. Większość państw UE, w tym Niemcy, Francja czy Holandia, dokonała transpozycji dyrektywy dopiero w 2020 roku, a część z nich uczyniła to z opóźnieniem, za co Komisja Europejska wszczynała

² Zaliczono do nich: „podmioty prowadzące działalność gospodarczą polegającą na świadczeniu usług w zakresie: a) wymiany pomiędzy walutami wirtualnymi i środkami płatniczymi, b) wymiany pomiędzy walutami wirtualnymi, c) pośrednictwa w wymianie, o której mowa w lit. a lub b, d) prowadzenia rachunków, o których mowa w ust. 2 pkt 17 lit. e”.

³ Zgodnie z art. 2 ust. 2 pkt. 17 ustawy przez rachunek rozumiano: „e) prowadzony w formie elektronicznej zbiór danych identyfikacyjnych zapewniających osobom uprawnionym możliwość korzystania z jednostek walut wirtualnych, w tym przeprowadzania transakcji ich wymiany”.

⁴ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z 30 maja 2018 roku zmieniająca dyrektywę 2015/849 (Dz.U. UE L 156/43).

postępowania naruszeniowe⁵. Warto odnieść tę sytuację do późniejszych regulacji dotyczących rynku kryptoaktywów, w przypadku których Polska należała do państw najpóźniej wdrażających odpowiednie przepisy w Unii Europejskiej.

Polska w latach 2018 – 2021 stopniowo rozszerzała reżim AML na podmioty związane z „walutami wirtualnymi”, przy czym kluczowy element infrastrukturalny w postaci **rejestru działalności w zakresie walut wirtualnych** wprowadzono dopiero nowelizacją z 30 marca 2021 roku, a obowiązek wpisu zaczął funkcjonować od 31 października 2021 roku.

Wdrożenie tych regulacji miało dla polskiego rynku dwojakie skutki. Z jednej strony znacząco podniosło koszty operacyjne (ang. *compliance-cost*), zmuszając firmy do inwestycji w nowe procedury i personel. Część najmniejszych podmiotów, nie mogąc sprostać nowym obciążeniom, wycofała się z rynku lub przeniosła działalność do jurysdykcji oferujących bardziej elastyczne rozwiązania. Z drugiej strony dla podmiotów, które pozostały w kraju, formalizacja statusu prawnego poprawiła ich wiarygodność w oczach banków i partnerów zagranicznych. Brak centralnego rejestru VASP, który wprowadzono dopiero nowelizacją z marca 2021 roku⁶, wciąż stanowił jednak istotną barierę instytucjonalną. Należy przypomnieć, że branża utworzyła rejestr zweryfikowanych, działających na rynku podmiotów, zobowiązujących się samodzielnie do ostrzejszych regulacji niż obowiązujące prawnie, i przekazała ten rejestr do Ministerstwa Cyfryzacji pod koniec 2017 roku. Jednak w dalszych pracach nad rejestrem VASP nie wykorzystano tego dorobku, co miało swoje konsekwencje — nawet międzynarodowe.

11.1.2. „Kryzys podatkowy” — spór o podatek od czynności cywilnoprawnych

O ile ustawa AML, mimo nałożenia nowych obowiązków, była przez branżę postrzegana jako nieuchronny krok w stronę profesjonalizacji, o tyle działania Ministerstwa Finansów z wiosny 2018 roku doprowadziły do otwartej konfrontacji i jednego z największych kryzysów w relacjach państwo – rynek w historii polskiej branży kryptoaktywów. Epizod ten stanowi studium przypadku regulacji tworzonej w oderwaniu od specyfiki technologicznej, realiów biznesowych i bez konsultacji ze środowiskiem eksperckim.

⁵ Na podstawie własnej analizy aktów prawnych: Włochy, *Decreto Legislativo 25 maggio 2017, n. 90 — Attuazione della direttiva (UE) 2015/849... e attuazione del regolamento (UE) n. 2015/847... (17G00104)*, Gazzetta Ufficiale Serie Generale n. 140 del 19.06.2017 (Suppl. Ordinario n. 28), <https://www.gazzettaufficiale.it/eli/id/2017/06/19/17G00104/sg>; Estonia, *Money Laundering and Terrorist Financing Prevention Act* (passed 26.10.2017; in force from 27.11.2017), Riigi Teataja (ELI), <https://www.riigiteataja.ee/en/eli/517112017003/consolide>; Gibraltar, *Proceeds of Crime Act 2015 (Amendment) Regulations 2017*, Second Supplement to the Gibraltar Gazette No. 4375 (26.06.2017), Legal Notice No. 119 of 2017, tekst w suplemencie (PDF), <https://www.gibraltarlaws.gov.gi/legislations/proceeds-of-crime-act-2015-amendment-regulations-2017-4140/download>; Komisja Europejska, *February infringements package: key decisions*, INF_20_202, 11.02.2020, Press corner, https://ec.europa.eu/commission/presscorner/detail/en/inf_20_202.

⁶ Ustawa z 30 marca 2021 roku o zmianie ustawy AML oraz niektórych innych ustaw (Dz.U. 2021 poz. 815).

Iskrą zapalną stało się opublikowanie **4 kwietnia 2018 roku komunikatu Krajowej Informacji Skarbowej *Skutki podatkowe obrotu kryptowalutami w PIT, VAT i PCC***⁷. W części dotyczącej podatku od czynności cywilnoprawnych (PCC) wskazano, że umowy sprzedaży i zamiany „waluty wirtualnej” podlegają PCC według stawki 1% wartości rynkowej, przy czym podstawą opodatkowania jest wartość każdej czynności, a nie wynik ekonomiczny z obrotu⁸. W praktyce — przy wysokiej częstotliwości transakcji na giełdach — taka wykładnia przepisów PCC (oparta na opodatkowaniu każdej czynności cywilnoprawnej od jej wartości) mogła prowadzić do obowiązku składania bardzo dużej liczby deklaracji PCC-3 oraz do narastania zobowiązań podatkowych nieproporcjonalnych do realnej dochodowości handlu. W publicznych wyliczeniach wskazywałem, że przy obrocie rządu 10 tysięcy złotych dziennie i przy wielokrotnych transakcjach (kupno/sprzedaż) w ciągu dnia hipotetyczna suma PCC, liczona jako 1% od wartości każdej czynności, mogłaby w skali roku przekraczać kilkaset tysięcy złotych⁹, co w praktyce czyniłoby legalny obrót operacyjnie niewykonalnym.

Reakcja rynku była natychmiastowa i gwałtowna. Pojawiały się również doniesienia medialne o silnych reakcjach emocjonalnych części drobnych inwestorów na ryzyko powstania zaległości podatkowych¹⁰.

12 kwietnia 2018 roku odbyło się **otwarte spotkanie Parlamentarnego Zespołu ds. Kryptowalut**, zorganizowane przez posłów Wojciecha Murdzka, Jakuba Kuleszę i Jacka Wilka. Nagranie wideo dokumentuje wystąpienia akademików i przedsiębiorców krytykujących opodatkowanie PCC oraz proponujących moratorium podatkowe dla innowacji¹¹. Ministerstwo Finansów nie zmieniło wówczas publicznie komunikowanego stanowiska.

Gniew społeczny, podsycany brakiem jakiegokolwiek próby dialogu ze strony resortu, skanalizował się w postaci **demonstracji zorganizowanej 20 kwietnia 2018 roku pod**

⁷ Warto wyjaśnić kulisy tego zdarzenia. Kilkanaście dni wcześniej z inicjatywy posła Wojciecha Murdzka odbyło się na terenie Sejmu robocze spotkanie parlamentarzystów i wiceministra finansów z przedstawicielami branży, podczas którego uzgodniono, że środowisko — w osobie mecenasa Marceliny Szwed — przygotuje projekt „zdraworozsądkowych” zmian w ustawach podatkowych. Niestety, z przyczyn zdrowotnych autorki projekt ten trafił do resortu z kilkudniowym opóźnieniem w stosunku do uzgodnień. Jak się okazało, ministerstwo zaczęło samodzielnie pracować nad własnymi regulacjami, co otworzyło drogę do opracowania „konkurencyjnej” wersji przepisów w Ministerstwie Finansów — bez konsultacji z rynkiem. Z nieoficjalnych doniesień wynika, że projekt ten w ministerstwie opracowywał student-stażysta...

⁸ Krajowa Informacja Skarbowa, *Skutki podatkowe obrotu kryptowalutami w PIT, VAT i PCC*, komunikat z 4 kwietnia 2018 roku, https://www.kis.gov.pl/wiadomosci/aktualnosci/-/asset_publisher/JSs9/content/id/7793320.

⁹ M. Ratajczak, *Inwestujący w kryptowaluty wyjdą na ulice i będą protestować. „Niektórzy mają myśli samobójcze”*, Money.pl, 9 kwietnia 2018, <https://www.money.pl/podatki/wiadomosci/arttykul/inwestujacy-w-kryptowaluty-wyjda-na-ulice-i,197,0,2402757.html>.

¹⁰ Media branżowe pisały o „podatkowym absurdzie”, a portal Bezprawnik alarmował, że część drobnych inwestorów, przerażona wizją astronomicznego długu podatkowego, deklarowała myśli samobójcze. T. Laba, *Handlujący kryptowalutami mają myśli samobójcze. Wszystkiemu winny ostatni komunikat Ministerstwa Finansów*, Bezprawnik, 10 kwietnia 2018, <https://bezprawnik.pl/handel-kryptowalutami/>.

¹¹ Parlamentarny Zespół ds. Kryptowalut, *Nagranie posiedzenia otwartego z 12 kwietnia 2018*, Sejm RP (YouTube, kanał Cyfrowa Ekonomia), <https://www.youtube.com/watch?v=Gd71pGCVONw>.

siedzibą Ministerstwa Finansów przez społeczność inwestorów skupioną wokół Trading Jam Session (z udziałem m.in. Sławomira Mentzena) pod hasłem „Chcemy płacić proste podatki od kryptowalut”¹². Media odnotowały, że demonstrowało wtedy ok. 300 osób. Była to największa dotąd (i na przestrzeni kolejnych kilku lat) demonstracja środowiska kryptowalutowego w Polsce, skierowana wyłącznie przeciwko ministerstwu.

Dopiero presja społeczna i medialna — w tym protesty środowiska — doprowadziła do rewizji podejścia resortu. Delegacja branży, w której uczestniczył także autor niniejszego opracowania, została zaproszona na rozmowy¹³, po których powołano międzyresortową grupę roboczą. Jej prace doprowadziły do szybkiej interwencji wykonawczej: 11 lipca 2018 roku ogłoszono rozporządzenie ministra finansów w sprawie zaniechania poboru PCC od umów sprzedaży lub zamiany waluty wirtualnej (Dz.U. 2018 poz. 1346), obowiązujące dla czynności dokonanych od 13 lipca 2018 roku¹⁴. Rozporządzenie było następnie przedłużane aż do czasu, gdy nowelizacja ustawy o podatku od czynności cywilnoprawnych w 2019 roku trwale wyłączyła obrót walutami wirtualnymi spod PCC. Należy jednak podkreślić, że rozwiązanie z 2018 roku nie usuwało automatycznie ryzyk dotyczących czynności dokonanych przed datą wejścia w życie zaniechania poboru — w tym sensie problem został rozwiązany przede wszystkim „na przyszłość”, a nie w pełni wstecznie.

Epizod ten jest niezwykle istotny, gdyż pokazuje bezpośrednie skutki marginalizacji dialogu ze środowiskiem eksperckim po 2017 roku. Podejście to, niezależnie od intencji projektodawców, generowało obowiązki sprawozdawczo-podatkowe niewspółmierne do charakteru obrotu giełdowego (wielość czynności, PCC liczony od wartości każdej transakcji), co czyniło masowy, detaliczny handel operacyjnie nieobsługiwalnym. Odejście od tej praktyki nastąpiło najpierw w formie czasowego zaniechania poboru PCC (2018), a następnie poprzez ustawowe wyłączenie obrotu walutami wirtualnymi spod PCC (2019). Przyczyną jednak nie były merytoryczne konsultacje przed zmianami dotyczącymi PCC, lecz dopiero masowe protesty i naciski opinii publicznej.

11.1.3. Systemowa zmiana podatkowa — nowelizacja ustaw o PIT i CIT

Protesty związane z praktycznymi skutkami PCC unaocznily administracji, że opodatkowanie obrotu walutami wirtualnymi wymaga rozwiązań systemowych, a nie jedynie doraźnych interwencji wykonawczych. Jednym z efektów prac międzyresortowej grupy roboczej była ustawa z 23 października 2018 roku o zmianie ustawy o podatku dochodowym od osób fizycznych, ustawy o podatku dochodowym od osób prawnych, ustawy

¹² D. Haczyk, *Nie trzeba płacić PCC — miłośnicy kryptowalut protestowali przed MF*, CyfrowaEkonomia.pl, 21 kwietnia 2018, <https://cyfrowaekonomia.pl/proste-podatki-od-kryptowalut/>.

¹³ W jego trakcie okazało się m.in., że resort dysponuje jedynie prasowymi doniesieniami o rzekomym „praniu pieniędzy w kryptowalutach”, natomiast nie zna wyników kontroli podlegającej mu administracji skarbowej, które potwierdzały marginalną skalę nadużyć (poniżej 1% wszystkich takich przypadków).

¹⁴ Rozporządzenie Ministra Finansów z 11 lipca 2018 roku w sprawie zaniechania poboru podatku od czynności cywilnoprawnych od umowy sprzedaży lub zamiany waluty wirtualnej, Dz.U. 2018 poz. 1346, <https://dziennikustaw.gov.pl/DU/2018/1346>.

Ordynacja podatkowa oraz niektórych innych ustaw (Dz.U. 2018 poz. 2193)¹⁵, która weszła w życie 1 stycznia 2019 roku i ukształtowała podstawowe ramy opodatkowania klasycznych transakcji na walutach wirtualnych. Lista skutków:

1. Wprowadzono definicję „waluty wirtualnej” na potrzeby PIT i CIT, przyjmując brzmienie zasadniczo spójne z definicją z ustawy AML (2018).
2. Doprecyzowano kwalifikację przychodów z odpłatnego zbycia walut wirtualnych:
 - o dla osób fizycznych — do przychodów z kapitałów pieniężnych (art. 17 ust. 1 pkt 11 ustawy o PIT),
 - o dla podmiotów gospodarczych — do przychodów z zysków kapitałowych (art. 7b ust. 1 pkt 6 lit. f ustawy o CIT).
3. Dla osób fizycznych zastosowano stawkę 19%. W CIT dochody z odpłatnego zbycia walut wirtualnych podlegają opodatkowaniu według stawki 19% (art. 22d ust. 1 ustawy o CIT).
4. Wprowadzono zasady rozpoznawania kosztów nabycia walut wirtualnych: wydatki na nabycie mogą być rozliczane w roku odpłatnego zbycia, a w razie braku sprzedaży — przenoszone na lata następne (akumulacja kosztów do momentu realizacji).
5. Wprowadzono zakaz kompensowania strat z odpłatnego zbycia walut wirtualnych z dochodami z innych źródeł kapitałowych (ang. *ring-fencing*), co branża krytykowała jako odstępstwo od zasady neutralności podatkowej i nierówne traktowanie części dochodów kapitałowych.

Nowelizacja zwiększyła pewność prawną dla klasycznych transakcji sprzedaży i zamiany walut wirtualnych, lecz nie obejmowała nowych zjawisk, które zaczęły nabierać znaczenia w kolejnych latach (np. *staking*, *yield-farming*, NFT), co w praktyce prowadziło do wysypu interpretacji indywidualnych oraz presji na dalsze dostosowania systemu.

Z perspektywy techniki legislacyjnej i funkcjonalności systemu podatkowego przyjęcie definicji projektowanej dla celów AML jako definicji podatkowej stanowiło rozwiązanie pragmatyczne, ale obarczone istotnym kosztem: definicja *compliance* nie jest zaprojektowana do rozróżniania zdarzeń podatkowych i w sposób naturalny nie „widzi” szeregu nowych modeli ekonomicznych. To ryzyko materializowało się w kolejnych latach w postaci rozbieżnych interpretacji i sporów o kwalifikację nowych form uzyskiwania przychodów.

11.1.4. Profesjonalizacja ekosystemu i odpowiedź branży

Rok 2018, naznaczony pierwszymi twardymi regulacjami i konfrontacją z aparatem państwa, stał się jednocześnie katalizatorem profesjonalizacji polskiego ekosystemu blockchainowego. W odpowiedzi na rosnącą presję i potrzebę posiadania silnego, merytorycznego głosu w dialogu z administracją branża zaczęła się intensywnie organizować, tworząc nowe, formalne struktury reprezentacji.

Kluczową inicjatywą w tym procesie było powołanie **Izby Gospodarczej Blockchain i Nowych Technologii (IGBiNT)**, która została formalnie zarejestrowana 27 sierpnia

¹⁵ Ustawa z 23 października 2018 roku o zmianie ustawy o podatku dochodowym od osób fizycznych, ustawy o podatku dochodowym od osób prawnych, ustawy Ordynacja podatkowa oraz niektórych innych ustaw, Dz.U. 2018 poz. 2193, <https://www.dziennikustaw.gov.pl/D2018000219301.pdf>.

2018 roku. Według komunikatów Izby była to pierwsza tego typu inicjatywa w Europie oraz jedna z pierwszych na świecie, dedykowana wyłącznie rynkowi DLT i kryptoaktywów. Pomysł narodził się w 2017 roku bezpośrednio za sprawą Piotra Bienia, związanego wówczas z giełdą Binance, choć idee w tym zakresie pojawiały się już wcześniej — zgłaszał je Sławomir Cieśliński¹⁶. W prace organizacyjne zaangażowali się też m.in. Robert Wojciechowski (późniejszy prezes Izby), Filip Pawczyński (prezes PSB) i Jakub Mościcki (członek zarządu fundacji Trading Jam Session).

Izba do swojego powołania — ze względu na ogólnopolski zakres działania — wymagała co najmniej 100 założycieli (art. 7 ustawy o izbach gospodarczych); w praktyce pozyskano ok. 150 członków-założycieli. Zrzeszała ona zarówno czołowe firmy z sektora (oraz jeden bank), jak i drobne biznesy.

Jeszcze w 2018 roku Zarząd Izby opublikował na swojej stronie internetowej **listę postulatów**. Dokument ten zawierał m.in.:

- trwałe zwolnienie obrotu walutami wirtualnymi z PCC,
- uproszczone zasady PIT/CIT dla krypto,
- gwarancję dostępu do rachunku bankowego dla legalnie działających podmiotów,
- utworzenie państwowego sandboxu regulacyjnego¹⁷.

Nie udało się zidentyfikować publicznie dostępnych śladów formalnego przedłożenia tego dokumentu w trybach legislacyjno-konsultacyjnych (np. pismo, stanowisko w konsultacjach itp.) ani jego bezpośredniego odzwierciedlenia w dokumentach rządowych.

Unikalną w skali świata inicjatywą Izby (według informacji pochodzących od niej: pierwszą taką w Europie i drugą na świecie) było powołanie 8 listopada 2018 roku stałego Sądu Polubownego ds. Blockchain. Była to odpowiedź na problem braku wyspecjalizowanych kadr w sądownictwie powszechnym, które często nie były w stanie zrozumieć technicznej specyfiki sporów w tej branży, a także przewlekłość postępowań gospodarczych w polskich sądach¹⁸. W skład kolegium arbitrów pod kierownictwem dr. hab. Konrada Zacharzewskiego weszli czołowi eksperci prawni i technologiczni (w tym autor).

Powstanie IGBiNT nie było jedynym przejawem dojrzewania rynku. W tym okresie zarejestrowano (31 października 2018 roku) w Poznaniu **Stowarzyszenie Blockchain Polska** (prezes Marcin Rzetecki)¹⁹, co świadczyło o szerszej (niż tylko PSB) potrzebie samoorganizacji w różnych częściach środowiska. Wcześniej (8 grudnia 2017 roku) w Łodzi

¹⁶ Jak czytamy na stronie internetowej Izby: „W dniu 26 kwietnia podobna inicjatywa została ogłoszona przez giełdę kryptowalut w Japonii. (...) Po raz pierwszy publicznie pomysł powstania izby gospodarczej był przedstawiony przez Sławomira Cieślińskiego na pierwszych spotkaniach Strumienia »Blockchain i kryptowaluty« prowadzonego przez Ministerstwo Cyfryzacji jeszcze w 2016. Szerokiej publice pomysł powołania bytu godnego reprezentowania środowiska w rozmowach z rządem został przywołany przez minister Annę Streżyńską w dniu 23 lutego 2018 na premierze filmu pod tytułem *Krypto* w Warszawskim kinie LUNA”. Por. *Czym jest IGBiNT?*, Izba Gospodarcza Blockchain i Nowych Technologii, <https://igbint.pl/izba/>.

¹⁷ Postulaty Izby, Izba Gospodarcza Blockchain i Nowych Technologii, <https://igbint.pl/izba/>.

¹⁸ *Pierwszy w Europie sąd arbitrażowy do spraw blockchain powstał w Polsce*, Dobra Marka, <https://dobramarka.eu/index.php/artykuly/106-komunikaty-pr/279-pierwszy-w-europie-sad-arbitrazowy-do-spraw-blockchain-powstal-w-polsce>.

¹⁹ Polish Blockchain Association, <https://blockchain-polska.org/>.

zarejestrowano fundację „Blockchain Development Foundation” (pod kierownictwem Kamila Gancarza)²⁰. Nieco później w Krakowie zarejestrowana (7 stycznia 2019 roku) została fundacja „Freelancer Startup Blockchain”, a w Warszawie zarejestrowano (15 lutego 2019 roku) fundację „Blockchain Hub Warsaw”²¹.

Istotną rolę w dalszym ciągu odgrywały niezależne platformy wymiany wiedzy, takie jak najstarszy w Europie tego typu (organizowany od 2014 roku) cykl konferencji **Digital Money & Blockchain Forum** koordynowany przez Sławomira Cieślińskiego (początkowo wraz z dr. Michałem Polasikiem z UMK w Toruniu, następnie z autorem), które stanowiły neutralny grunt do dyskusji dla całego ekosystemu. Mimo corocznie ponawianych zaproszeń na tych konferencjach nigdy nie było przedstawicieli KNF (byli obecni m.in. rzecznik finansowy, przedstawiciele banków, KIR, innych instytucji, naukowcy, biznesmani i prawnicy).

Napływ kapitału zagranicznego na polski rynek przyspieszył rozwój krajowego sektora blockchain: powstały nowe, dobrze płatne miejsca pracy dla programistów i specjalistów RegTech, a czołowe uczelnie włączyły się w proces edukacyjny. W październiku 2018 roku **Szkoła Główna Handlowa** w Warszawie uruchomiła pierwsze w Polsce kompleksowe (ponad 200 godzin dydaktycznych, w tym podstawy kryptografii, tokenizacja modeli biznesowych oraz ramy prawne i podatkowe) **studia podyplomowe** „Blockchain: Biznes, Prawo, Technologia” (ich kierownikiem został dr Grzegorz Sobiecki z Katedry Systemu Finansowego). Jest to pierwsza w Polsce kompleksowa oferta edukacyjna w tym zakresie, skierowana do menedżerów, prawników i specjalistów finansowych. Wykładowcami są zarówno naukowcy, jak i praktycy, m.in. z sektora bankowego i firm technologicznych²².

Jeszcze w 2017 roku **Uczelnia Łazarskiego**, za sprawą utworzonego w grudniu 2016 roku Centrum Technologii Blockchain, rozpoczęła organizację seminariów i konferencji poświęconych blockchainowi i kryptoaktywowi, np. „Bitcoin waluta przyszłości” (16 grudnia 2016 roku) oraz „Prawne uregulowania technologii blockchain” (25 maja 2017 roku)²³. W 2018 roku zorganizowano takie wydarzenia jak „Warsaw Legal Hackers: Blockchain, prawo i prawnicy” (17 stycznia 2018 roku, Łazarski) oraz „Initial Coin Offering — prawny punkt widzenia” (8 marca 2018 roku, Łazarski), wspierające edukację w zakresie regulacji kryptowalut²⁴. W październiku 2017 roku na tej uczelni uruchomiono pierwszy w Polsce pełnowymiarowy wykład akademicki pt. „Blockchain i kryptowaluty”. Centrum pełniło rolę think tanku i partnera merytorycznego konferencji, wspierając samoregulację branży, m.in. poprzez współpracę z Polskim Stowarzyszeniem Bitcoin i Izbą.

Inicjatywy te dowodzą, że mimo niesprzyjającego klimatu politycznego polski ekosystem DLT w 2018 roku wykazywał dużą odporność i zdolność do dalszego oddolnego rozwoju.

²⁰ Blockchain Development Foundation, <https://blockchaindev.eu/>.

²¹ Brak informacji o ich działalności, w tym brak działających stron internetowych (<http://bhwarsaw.org/>).

²² SGH, Studia podyplomowe Blockchain: Biznes, Prawo, Technologia, <https://www.sgh.waw.pl/studia-podyplomowe-i-mba/transformatcja-cyfrowa/studia-podyplomowe-blockchain-biznes-prawo-technologia>.

²³ Centrum Technologii Blockchain, Uczelnia Łazarskiego, <https://www.lazarski.pl/pl/uczelnia/wydz-ekonomii-i-zarzadzania/instituty/centrum-technologii-blockchain/>.

²⁴ Ibidem.

11.2. Boom na ICO i jego wpływ na polski rynek (2017 – 2018)

Poniżej opisane zostaną bardzo ekscytujące i dynamiczne wydarzenia boomu na ICO, który miał miejsce głównie w 2017 roku, z pewnymi jeszcze reminiscencjami w 2018 roku.

11.2.1. Polski rynek na fali globalnego fenomenu

Lata 2017 – 2018 przyniosły gwałtowny wzrost liczby emisji Initial Coin Offering (ICO) na świecie. Była to nowatorska metoda pozyskiwania kapitału przez start-upy technologiczne poprzez emisję dedykowanych tokenów. Według raportu Fabric Ventures & Token-Data w samym tylko 2017 roku projekty na całym świecie pozyskały w ten sposób około 5,6 miliarda dolarów, przy 435 udanych sprzedażach i średnim wpływie 12,7 miliona dolarów na projekt²⁵. Ta globalna fala dotarła również do Polski, trafiając na podatny grunt — rynek charakteryzujący się rosnącym zainteresowaniem kryptowalutami, co potwierdzały szacowane wolumeny obrotu na krajowych giełdach, oraz obecnością utalentowanych zespołów deweloperskich.

Choć pod względem wartości pozyskanego kapitału Polska pozostawała daleko za liderami z USA czy Szwajcarii, to wytworzyła grupę innowacyjnych projektów, które z sukcesem konkurowały o globalny kapitał. Charakterystyczną cechą polskich emisji było częste wykorzystywanie spółek rejestrowanych w jurysdykcjach postrzeganych jako bardziej przyjazne cyfrowym finansom, w szczególności w Szwajcarii (tzw. Crypto Valley w kantonie Zug), w Estonii oraz w Gibraltarze. Pozwalało to łączyć lokalny potencjał technologiczny z międzynarodową bazą inwestorów. Szczyc rynku euforii przypadł na czwarty kwartał 2017 roku, gdy wiele projektów pozyskiwało znaczne środki, opierając swoją wiarygodność niemal wyłącznie na obietnicach zawartych w dokumencie typu „biała księga” (*white paper*).

Najgłośniejszym i pionierskim sukcesem polskiego środowiska był projekt **Golem**. Jego ICO, przeprowadzone jeszcze 11 listopada 2016 roku, stanowiło zapowiedź nadchodzącego boomu. Zespół sprzedał swoje tokeny za 820 000 ETH, pozyskując w zaledwie 29 minut równowartość ok. 8,6 miliona dolarów. Wartość tej puli przy kursie ETH z lipca 2025 roku (tj. ok. 3000 dolarów)²⁶ wynosiłaby ok. 2,5 miliarda dolarów, co pokazuje skalę finansowania w kategoriach dzisiejszych cen kryptoaktywów. W kolejnych latach część środków pozostawała w portfelach powiązanych z projektem, co było przedmiotem zainteresowania oraz analiz społeczności i mediów branżowych²⁷.

²⁵ O. Williams-Grut, *Only 48% of ICOs were successful last year — but startups still managed to raise \$5.6 billion*, Business Insider, 31 stycznia 2018, <https://www.businessinsider.com/how-much-raised-icos-2017-tokendata-2017-2018-1>.

²⁶ Kurs ETH 30 maja 2025: 2653 dolarów, *CoinMarketCap — Ethereum live price*, <https://coinmarketcap.com/currencies/ethereum/>.

²⁷ Media branżowe szacowały, że projekt dysponuje jeszcze 120 tysiącami ETH. J. Leech, *Golem sends over \$100 million worth of ETH to exchanges in the past month*, The Block, 30 czerwca 2024, <https://www.theblock.co/post/303905/golem-sends-over-100-million-worth-of-eth-to-exchanges-in-the-past-month>. Jednakże na adresie smart kontraktu ICO widać jedynie 10,3 tysiąca ETH: pod adresem ICO projektu Golem (0x7da82C7AB4771FF031B66538D2FB9B0B047F6CF9,

Sukces Golema był dowodem, że polskie zespoły są w stanie tworzyć technologie o globalnym potencjale i skutecznie pozyskiwać na nie finansowanie w nowej, zdecentralizowanej formule.

W ślad za Golemem poszły kolejne projekty. Drugi co do wartości był token **indaHash (IDH)**, którego sprzedaż główna zakończyła się 20 grudnia 2017 roku wpływem 37,2 miliona dolarów²⁸. **Coinfirm** z tokenem **AMLT** zebrał w publicznej ofercie ponad 11 tysięcy ETH (ok. 9 milionów dolarów według cen z grudnia 2017 roku) na rozwój narzędzi AML/RegTech dla rynku kryptoaktywów²⁹. W tym samym roku polskie zespoły uruchomiły także emisje **AdShares (ADS)**, **Userfeeds**, **Neufund (NEU)** czy projekt **Billon**.

Autor — na podstawie największych emisji i przybliżonych kursów w okresie pozyskania kapitału — szacuje łączne wpływy polskich (lub powiązanych z polskimi zespołami) projektów ICO na 300 – 350 milionów dolarów, z czego ponad 70% przypadło na pięć największych emisji; szacunek ten ma charakter przybliżony i zależy od przyjętych kursów oraz kwalifikacji, które emisje zaliczyć do tej grupy.

W większości kapitał ten pochodził z zagranicy, a nie od polskich inwestorów. Oznaczałoby to, że polskie projekty mogły „ściągnąć” do naszego kraju kapitał rzędu od setek milionów do ok. 1 miliarda złotych (w zależności od przyjętego kursu). To byłoby uznane za sukces polskiej sceny start-upowej; temat ten miał jednak ograniczoną obecność w mediach głównego nurtu w porównaniu z mediami branżowymi.

Jednocześnie polski rynek nie uniknął negatywnych konsekwencji globalnej mody na ICO. Badania przeprowadzone przez Bloomberg i Boston College wykazały, że ok. 56% światowych ICO z 2017 roku przestało działać w ciągu czterech miesięcy od emisji³⁰. Podobny los spotkał wiele polskich projektów — większość lokalnych tokenów notowanych na giełdach odnotowała od 2018 roku głębokie spadki cen (często przekraczające 80% swojej wartości). Pokazało to inwestorom ogromne ryzyko niedojrzałego finansowania i braku fundamentów biznesowych wielu przedsięwzięć.

Mimo tych napięć okres boomu ICO odegrał ważną rolę w budowaniu kompetencji biznesowych polskich start-upów, w nabywaniu umiejętności przyciągania zagranicznych inwestorów oraz w pokazaniu, że (nieliczne) polskie zespoły potrafią konkurować na globalnym rynku Web3.

11.2.2. Reakcja nadzoru — komunikat KNF w sprawie ICO

Globalny boom na emisje tokenów i związane z nim ryzyka dla inwestorów detalicznych skłoniły polski nadzór finansowy do zajęcia stanowiska. Okres względnej swobody regulacyjnej w zakresie ICO uległ istotnej zmianie wraz z publikacją przez Urząd Komisji

oznaczony w Etherscanie jako *Golem: Multisig*) 30 maja 2025 było 10 284,34 ETH, tj. przy kursie 2636 dol./ETH odpowiadało to ok. 27,1 miliona dolarów.

²⁸ indaHash (IDH), ICO profile, ICODrops, aktualizacja 19 kwietnia 2024, <https://icodrops.com/indahash/>.

²⁹ WookieeCookie, *AMLT by Coinfirm — The Token of Compliance*, Medium, 10 stycznia 2018, <https://medium.com/@wookieecookie/amlt-by-coinfirm-the-token-of-compliance-f0f79931a725>.

³⁰ O. Kharif, *Half of ICOs die within four months*, Bloomberg, 9 lipca 2018, <https://www.bloomberg.com/news/articles/2018-07-09/half-of-icos-die-within-four-months-after-token-sales-finalized>.

Nadzoru Finansowego komunikatu z 24 października 2018 roku (ICO/ITO), wydanego już w schyłkowej fazie boomu na ICO. Dokument ten — po raz pierwszy w całości poświęcony emisjom tokenów — nie stanowił źródła prawa ani formalnie wiążącej wykładni, lecz pełnił funkcję *soft law*: porządkował sposób postrzegania ICO przez nadzór, sygnalizował kwalifikacje prawne w zależności od konstrukcji emisji (np. instrumenty finansowe, usługi płatnicze czy działalność objętą obowiązkami informacyjnymi) oraz wyznaczał oczekiwania nadzorcze wobec podmiotów działających na rynku regulowanym³¹. W praktyce komunikat ten stał się istotnym punktem odniesienia dla uczestników rynku, ponieważ wpływał na ocenę ryzyk regulacyjnych w relacjach z UKNF.

W komunikacie UKNF z 24 października 2018 roku urząd po raz pierwszy wyraźnie zasygnalizował, że tokeny stosowane w ramach ofert (ICO) mogą — w zależności od nadawanej im funkcji ekonomicznej — podlegać reżimowi:

- ustawy z 29 lipca 2005 roku o ofercie publicznej (Dz.U. 2023 poz. 993),
- ustawy z 29 lipca 2005 roku o obrocie instrumentami finansowymi (Dz.U. 2023 poz. 1467),

w brzmieniu tych ustaw obowiązującym w 2018 roku.

Urząd nie wprowadził zakazu emisji tokenów, lecz podkreślił, że ich kwalifikacja prawna wymaga każdorazowo indywidualnej analizy konstrukcji praw i obowiązków związanych z danym tokenem — w szczególności tego, czy przyznaje on uprawnienia ekonomiczne porównywalne z instrumentami finansowymi, takimi jak akcje lub obligacje. Jednocześnie UKNF nie zaproponował jednolitej metodyki ani zestawu kryteriów oceny tokenów. Dla porównania: w niektórych jurysdykcjach rynek posługuje się względnie stabilnymi standardami wypracowanymi w orzecznictwie (np. test Howeya w USA), choć ich kontekst prawny jest odmienny. Organ ograniczył się do opisowego wskazania możliwych kwalifikacji prawnych, pozostawiając w znacznym stopniu ocenę podejściu *case-by-case* w praktyce nadzorczej.

Komisja podkreśliła, że w zależności od wyniku takiej analizy organizatorzy emisji mogą potrzebować zezwolenia lub wpisu właściwego dla działalności zarządzającego alternatywnym funduszem inwestycyjnym (ZAFI/ZASI), zależnie od konstrukcji przedsięwzięcia. Jednocześnie ostrzegła inwestorów przed ryzykiem utraty całości środków, manipulacją kursami na nieuregulowanych platformach oraz brakiem dostępu do rzetelnych informacji o projekcie.

Ponadto UKNF stanowczo ostrzegł inwestorów przed kluczowymi ryzykami, w tym:

- możliwością utraty całości zainwestowanych środków,
- manipulacją cenami na nieregulowanych platformach obrotu,
- brakiem rzetelnych i zweryfikowanych informacji o projekcie (*white paper*, zespół, model biznesowy),
- wysoką zmiennością cen kryptoaktywów,
- ryzykiem kradzieży środków w wyniku ataków hakerskich,

³¹ Komisja Nadzoru Finansowego, *Komunikat UKNF w sprawie oferowania niektórych produktów i świadczenia niektórych usług na rynku finansowym z wykorzystaniem emisji tzw. kryptowalut lub tokenów (ICO/ITO)*, 24 października 2018, s. 2 – 4, https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_ICO_24_10_2018_62921.pdf.

- a także brakiem systemów ochrony inwestorów i ryzykiem wykorzystania ICO do działań przestępczych.

Reakcja branży była ambiwalentna. Z jednej strony niektórzy podkreślali, że KNF nie zdecydowała się na całkowity zakaz, lecz wybrała „ścieżkę dojrzałej regulacji”, opartą na indywidualnej analizie i istniejących przepisach³². Z drugiej strony konsekwencją komunikatu był znaczący wzrost kosztów prawnych związanych z przygotowaniem emisji³³. W praktyce komunikat zwiększył koszty obsługi prawnej emisji i — według relacji uczestników rynku — skłaniał część projektów do lokowania struktur sprzedaży poza Polską (m.in. w jurysdykcjach postrzeganych jako bardziej przewidywalne, np. Litwa czy Estonia). Jednocześnie w części projektów widać było profesjonalizację dokumentacji: częściej pojawiały się opinie prawne, elementy modelu finansowego oraz audyty smart kontraktów.

11.3. Konstrukcja rejestru VASP i jej skutki (2019 – 2021)

Poniżej zostanie opisane wprowadzenie drugiego rejestru firm kryptowalutowych w Polsce (pierwszy — środowiskowy — powstał przy Ministerstwie Cyfryzacji w 2017 roku).

11.3.1. Próżnia instytucjonalna po ustawie AML z 2018 roku

Ustawa z 1 marca 2018 roku o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu (AML) wprowadziła do polskiego systemu pojęcie „waluty wirtualnej” oraz zaliczyła giełdy, kantory i operatorów portfeli do katalogu „instytucji obowiązanych” (art. 2 ust. 1 pkt 12)³⁴. Od 13 lipca 2018 roku podmioty te musiały stosować środki bezpieczeństwa finansowego (ang. *know your customer*, KYC; *customer due diligence*, CDD), prowadzić analizę ryzyka oraz realizować obowiązki informacyjne wobec GIIF, w tym dotyczące transakcji podejrzanych oraz transakcji ponadprogowych (próg 15 000 euro). Ustawa nie przewidywała jednak żadnej licencji ani publicznego rejestru, który potwierdzałby spełnienie nowych obowiązków. Formalny wykaz VASP pojawił się dopiero nowelą ustawy AML z 30 marca 2021 roku (art. 129m – 129z), której przepisy weszły w życie 31 października 2021 roku³⁵. W dalszej części „rejestr VASP” oznacza polski rejestr działalności w zakresie walut wirtualnych (ustawa AML, nowelizacja z 30 marca 2021 roku).

Zmiany te były również konsekwencją tego, że polska ustawa z 2018 roku wyprzedziła termin implementacji dyrektywy 2018/843/UE (AMLD5). Dyrektywa — obowiązująca

³² K. Piech, *KNF nie straszy, lecz edukuje. Dokument o ICO to krok w dobrym kierunku*, wywiad dla FinTech.pl, 26 października 2018, <https://fintech.pl/knf-ico-krok-w-dobrym-kierunku-dr-krzysztof-piech/>.

³³ Kancelarie, które dotąd wyceniały obsługę ICO na ok. 50 – 70 tysięcy złotych, po tym komunikacie żądały nawet 200 tysięcy złotych, tłumacząc to koniecznością pełnego badania kwalifikacji prawnej tokena.

³⁴ Ustawa z dnia 1 marca 2018 roku o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dz.U. 2018 poz. 723, <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180000723>.

³⁵ Ustawa z dnia 30 marca 2021 roku o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw, Dz.U. 2021 poz. 815, <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20210000815>.

od 9 lipca 2018 roku, z terminem transpozycji do 10 stycznia 2020 roku — wymagała, aby państwa członkowskie objęły dostawców usług wymiany między walutami wirtualnymi a fiducyjnymi oraz dostawców portfeli powierniczych reżimem AML/CFT, a także zapewniły mechanizm ich rejestracji (art. 47 dyrektywy 2015/849 w brzmieniu nadanym AMLD5). Polska już w 2018 roku objęła część podmiotów VASP reżimem AML/CFT, co okazało się zbieżne z kierunkiem przyjętym następnie w AMLD5. Jednocześnie mechanizm rejestracji VASP wprowadzono dopiero nowelizacją z 30 marca 2021 roku (Dz.U. 2021 poz. 815, wejście w życie 31 października 2021 roku), wprowadzając do ustawy rozdział 11B „Rejestr działalności w zakresie walut wirtualnych”. Powstała więc **ponad trzyletnia** (od lipca 2018 do października 2021 roku) **prawna „próżnia” instytucjonalna** (w postaci braku publicznego instrumentu potwierdzającego status podmiotów), mimo istnienia obowiązków AML.

Z jednej strony — poprzez włączenie podmiotów z branży walut wirtualnych do katalogu „instytucji obowiązanych” — państwo po raz pierwszy nałożyło na nie twarde obowiązki prawne. Z drugiej strony ustawa nie wprowadziła żadnego mechanizmu, który pozwoliłby tym podmiotom na formalne potwierdzenie swojego nowego statusu. W praktyce oznaczało to, że giełda lub kantor kryptowalutowy stawały się podmiotem zobowiązanym do stosowania skomplikowanych procedur AML/KYC, ale nie otrzymywały w zamian żadnej licencji, zezwolenia ani nawet wpisu do publicznego rejestru. Stworzyło to stan prawnej próżni: firma była regulowana, ale nie mogła w żaden sposób udowodnić tego faktu swoim kontrahentom, w szczególności bankom.

W efekcie giełdy mogły okazać bankowi tylko własne procedury AML (które przez banki mogły być kwestionowane), bez publicznie dostępnego, państwowego dowodu „statusu regulowanego”. Banki natomiast, obawiając się odpowiedzialności, utrzymały politykę „deriskingu” — masowego wypowiadania rachunków firmom branży kryptowalutowej. Skargi branży zostały odnotowane przez Rzecznika Praw Obywatelskich i UOKiK, lecz oba urzędy stwierdziły, że bank ma prawo odmówić obsługi, kierując się własną oceną ryzyka AML³⁶. Wobec braku rejestru cała branża wciąż była postrzegana jako jednolity sektor wysokiego ryzyka. Utrwaliło to praktykę zamykania rachunków.

UKNF zwrócił uwagę na te same ryzyka w *Komunikacie w sprawie funkcjonowania giełd i kantorów kryptowalut* z 6 czerwca 2018 roku (ryzyko utraty środków, manipulacje cenowe, brak rzetelnej informacji)³⁷. Komunikat pozostał aktualny aż do publikacji szerszego *Stanowiska UKNF w sprawie wydawania i obrotu kryptoaktywami* (10 grudnia 2020 roku)³⁸. Również później KNF ostrzegał przed kryptoaktywami w komunikacie z listopada 2024 roku pt. *Kryptoaktywa — czy wiążą się z wyższym ryzykiem*, gdzie ponownie ostrzegł przed

³⁶ D. Słomski, *UOKiK i RPO nie pomogą bitcoinowcom. Konta mogą być zamykane*, Money.pl, 27 września 2018, <https://www.money.pl/banki/wiadomosci/arttykul/banki-kryptowaluty-zamykanie-rachunkow,18,0,2417170.html>.

³⁷ Komisja Nadzoru Finansowego, *Komunikat w sprawie funkcjonowania giełd i kantorów kryptowalut*, 6 czerwca 2018, https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_ws_funkcjonowania_gield_i_kantorow_kryptowalut_61993.pdf.

³⁸ *Stanowisko UKNF w sprawie wydawania i obrotu kryptoaktywami*, KNF, 10 grudnia 2020, https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_ws_wydawania_i_obrotu_kryptoaktywami_71794.pdf.

brakiem gwarancji i możliwością utraty całych środków, manipulacją cenami na nieregulowanych platformach oraz deficytem rzetelnych informacji projektowych³⁹.

Ostatecznie nowela AML z 30 marca 2021 roku (Dz.U. 2021 poz. 815), wdrażając w całości AMLD5, utworzyła rejestr działalności w zakresie walut wirtualnych (art. 129m – 129z), który zaczął działać 31 października 2021 roku. Dopiero odtąd podmioty krypto mogły się posługiwać oficjalnym wpisem, a banki — weryfikować ich status regulowany w publicznym rejestrze IAS w Katowicach. Jednak nieuzyskanie wpisu w rejestrze VASP nie zakończyło problemów z bankami — nadal stosowały zasady podwyższonego ryzyka, a wiele z nich odmawiało otwierania rachunków bankowych firmom z tej branży.

11.3.2. Proces legislacyjny rejestru VASP — ograniczony dialog z rynkiem

Proces legislacyjny, który miał na celu wypełnienie trzyletniej „próżni” prawnej, stanowi studium przypadku, w jaki sposób odejście od dialogu z ekspertami prowadzi do tworzenia regulacji nieefektywnych dla rynku i szkodliwych dla reputacji państwa. Prace nad stworzeniem rejestru VASP rozpoczęły się formalnie **4 marca 2020 roku**, kiedy to na wniosek Ministerstwa Finansów w Rządowym Centrum Legislacji opublikowano projekt nowelizacji ustawy AML (sygn. UD172)⁴⁰. Miał on na celu m.in. stworzenie rejestru VASP (właściwie „rejestru w zakresie walut wirtualnych”).

W procesie konsultacji społecznych wzięło udział dziewięć podmiotów, przy czym wśród nich zabrakło kluczowych organizacji reprezentujących rynek walut wirtualnych (w szczególności Izby Gospodarczej Blockchain i Nowych Technologii, powołanej do reprezentowania interesów tego sektora — właśnie w tego typu procesach legislacyjnych).

Jedyną poprawkę odnoszącą się do walut wirtualnych zgłosiła Polska Izba Informatyki i Telekomunikacji. Postulowała ona, by rozdzielenie rozdziału 11a tworzącego rejestr (VASP) na dwa odrębne segmenty — osobno dla działalności dotyczącej spółek lub trustów oraz osobno dla działalności w zakresie walut wirtualnych⁴¹. Była to więc poprawka o charakterze porządkowym. Nie została jednak przyjęta, co z perspektywy czasu można ocenić krytycznie, ponieważ rozwiązania dotyczące „spółek lub trustów” zostały w znacznej mierze skopiowane do regulacji dotyczących walut wirtualnych. Przyjęto tym samym założenie, że oba sektory są wystarczająco podobne pod względem konstrukcji obowiązków AML, co okazało się nietrafione. W efekcie do rynku usług związanych z walutami wirtualnymi przeniesiono rozwiązania projektowane pierwotnie dla innego segmentu działalności regulowanej. Nie udało się jednocześnie zidentyfikować formalnych stanowisk ani uwag zgłoszonych w toku konsultacji przez podmioty reprezentujące rynek walut wirtualnych (w tym IGBiNT). Taka bierność pozostawała w wyraźnym kontraście

³⁹ Komisja Nadzoru Finansowego, *Kryptoaktywa — czy wiążą się z wyższym ryzykiem*, https://www.knf.gov.pl/dla_ryнку/kryptoaktywa_czy_wiaza_sie_z_wyzszym_ryzykiem.

⁴⁰ Projekt ustawy o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw, <https://legislacja.rcl.gov.pl/projekt/12330901/>.

⁴¹ *Stanowisko Polskiej Izby Informatyki i Telekomunikacji [PIIT] w przedmiocie projektu ustawy o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu i niektórych innych ustaw*, 7 marca 2020, <https://legislacja.rcl.gov.pl/docs/2/12330901/12666701/12666704/dokument446902.pdf>.

do wcześniejszego zaangażowania środowiska w prace nad *Kanonem dobrych praktyk* (w latach 2016 – 2017).

Nowelizacja ustawy z 30 marca 2021 roku⁴² wprowadziła **rejestr działalności w zakresie walut wirtualnych**, którego prowadzenie powierzono Dyrektorowi Izby Administracji Skarbowej w Katowicach. Od 31 października 2021 roku uzyskanie wpisu do tego rejestru stało się warunkiem legalnego wykonywania działalności wskazanej w art. 129m ustawy⁴³. Rejestr oparto na bardzo liberalnym modelu regulacyjnym — wpis następował przede wszystkim na podstawie oświadczeń i dokumentów formalnych, bez uprzedniej weryfikacji *ex ante*. W rezultacie Polska znalazła się w gronie państw UE o jednej z najwyższych liczb zarejestrowanych podmiotów VASP; więcej podmiotów zarejestrowano jedynie w Czechach. W celu uzyskania wpisu podmiot — w tym również osoba fizyczna — zobowiązany był do złożenia:

- formularza z danymi identyfikacyjnymi podmiotu (dla osoby prawnej m.in. KRS/NIP, a dla osoby fizycznej m.in. dane identyfikacyjne właściwe dla tej formy prowadzenia działalności),
- informacji o rodzaju świadczonych usług (z zamkniętej listy),
- oświadczenia o niekaralności (art. 129p),
- oświadczenia o posiadaniu wiedzy lub doświadczenia związanego z działalnością w zakresie walut wirtualnych (art. 129o).

Wiedza i doświadczenie mogą być udokumentowane poprzez:

1. ukończenie szkolenia lub kursu obejmujących prawne lub praktyczne zagadnienia związane z działalnością w zakresie walut wirtualnych
2. lub wykonywanie, przez okres co najmniej roku, czynności związanych z działalnością w zakresie walut wirtualnych — potwierdzone odpowiednimi dokumentami.

Ustawa nie precyzowała minimalnego standardu jakości, zakresu ani długości szkolenia, co w praktyce osłabiało funkcję selekcyjną tego kryterium.

Mechanizm wpisu nie przewidywał uprzedniej weryfikacji *ex ante* w formie audytu wdrożenia procedur AML/KYC ani oceny merytorycznej deklarowanej „wiedzy i doświadczenia”; w praktyce wpis następował po spełnieniu wymogów formalnych. Oświadczenie składano pod rygorem odpowiedzialności karnej, poprzez zamieszczenie klauzuli: „Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia”. Jednocześnie sankcje administracyjne ze strony organu rejestrowego przewidziano wyłącznie na wypadek niedopełnienia obowiązku uzyskania wpisu do rejestru (art. 129q). Innymi słowy, stworzono lukę, przez którą każdy podmiot — przy minimalnym nakładzie pracy i kosztów — mógł uzyskać wpis do rejestru, ponieważ procedura miała charakter formalny (po spełnieniu wymogów dokumentowych i uiszczeniu opłaty skarbowej wynoszącej 616 złotych), bez uprzedniej oceny merytorycznej.

Porównanie tego mechanizmu z samoregulacyjnym *Kanonem dobrych praktyk* z 2017 roku demaskuje regres, jaki dokonał się w podejściu do standardów rynkowych. *Kanon*,

⁴² Ustawa z 30 marca 2021 roku o zmianie ustawy AML oraz niektórych innych ustaw (Dz.U. 2021 poz. 815).

⁴³ Krajowa Administracja Skarbowa, *Od 31 października 2021 r. zacznie obowiązywać rejestr działalności w zakresie walut wirtualnych*, komunikat z 29 października 2021.

wypracowany przez branżę, był znacznie bardziej rygorystyczny niż późniejsza ustawa. Wymagał od sygnatariuszy m.in. publicznego udostępnienia polityki AML/KYC, obowiązku segregacji środków klientów, posiadania planów awaryjnych i cyklicznych raportów transparentności — elementów, których ustawa o rejestrze VASP w ogóle nie przewidywała.

Rejestr VASP spełniał jedynie minimalny wymóg AMLD5 — był w praktyce narzędziem informacyjnym, a nie weryfikacyjnym. Tymczasem *Kanon dobrych praktyk* wyprzedzał ustawę o cztery lata, ustanawiając standardy bezpieczeństwa, przejrzystości i ładu korporacyjnego, bardziej zbliżone do podejść opartych na selekcji i weryfikacji *ex ante* (model licencyjny), znanych z części jurysdykcji.

Luźna konstrukcja prawna rejestru pozwoliła na masowy napływ wpisów bez selekcji merytorycznej (podczas gdy model samoregulacyjny Strumienia eliminował podmioty niespełniające kryteriów już na etapie zgłoszenia). W praktyce liberalna konstrukcja rejestru spowodowała napływ dużej liczby wpisów, z których część okazywała się nieaktywna lub trudna do zweryfikowania operacyjnie. Do końca 2023 roku w rejestrze znalazło się 1100 podmiotów, zaś na koniec 2024 roku było ich (po odjęciu wykreślonych) 1394⁴⁴. Jak wykazały późniejsze analizy, duża część z nich nie prowadziła faktycznej działalności; było też wielu cudzoziemców. Polski rejestr VASP, w pewnych kręgach rynkowych znany jako „regulatory badge” (tzw. **flaga wygody**)⁴⁵, był wykorzystywany marketingowo do sugerowania statusu „regulowanego podmiotu w UE”, mimo że był to jedynie rejestr informacyjny, a nie reżim licencyjny⁴⁶.

Ministerstwo — widząc, że **duża część wpisów do rejestru okazała się „martwa”** (do końca 2024 roku wykreślono 447 podmiotów) lub dotyczyła projektów o wątpliwej reputacji — zdecydowało się w 2024 roku zaangażować **GIIF**. Kontrole te miały pełną podstawę prawną w art. 130 ustawy AML (dającą organowi prawo do kontrolowania wszystkich instytucji obowiązanych), lecz **nie rozwiązały problemu „listy-widmo”**: procedura wykreślania nieaktywnych lub ryzykownych podmiotów okazała się nieprecyzyjna (choć dokonano wykreślenia ok. czterystu podmiotów), a sam rejestr nadal nie zapewniał bankom i konsumentom rzetelnej informacji o faktycznym poziomie zgodności danego VASP z wymogami AML/KYC.

⁴⁴ IAS, *Rejestr działalności w zakresie walut wirtualnych*, Izba Administracji Skarbowej w Katowicach, https://www.slaskie.kas.gov.pl/izba-administracji-skarbowej-w-katowicach/zalatwanie-spraw/rejestr-dzialalnosci-w-zakresie-walut-wirtualnych/-/asset_publisher/R7YI/content/rejestr-dzialalnosci-w-zakresie-walut-wirtualnych.

⁴⁵ Termin „flaga wygody” (ang. *flag of convenience*, w polskiej terminologii morskiej także „tania bandera”) jest analogią do praktyki rejestrowania statków w krajach o liberalnych przepisach i niskim poziomie nadzoru w celu uniknięcia bardziej rygorystycznych wymogów państwa macierzystego właściciela. W tym kontekście oznacza wykorzystanie polskiego rejestru VASP do uzyskania statusu regulowanego podmiotu w UE przy minimalnych kosztach i bez realnej weryfikacji. Zjawisko to jest formą **arbitrażu regulacyjnego**.

⁴⁶ Z informacji uzyskanych przez autora od pracowników Ministerstwa Finansów wynika, że prowadziło to do interwencji ze strony zagranicznych regulatorów i rządów (np. Francji) w polskim Ministerstwie Finansów. Z bezpośrednich rozmów autora z przedstawicielami Izby Skarbowej w Katowicach, dokonującymi rejestracji podmiotów, można było się dowiedzieć, że byli oni świadomi problemu, lecz nie dysponowali narzędziami pozwalającymi — zgodnie z prawem — odmawiać rejestracji lub skuteczniej weryfikować procedury.

Dla porównania, podobny pomysł co w Polsce (tj. możliwość rejestrowania osób fizycznych) wprowadzono w Czechach, gdzie w rejestrze VASP znalazło się nawet ponad 9000 podmiotów. Duża liczba była również na Litwie — ok. 400, oraz w Bułgarii — ok. 200. W pozostałych krajach UE liczba ta wahała się w granicach od bliskiej zera (Belgia) do ok. 100 (Francja) i 150 (Włochy); z serwisu TheBanks.eu wynikałoby, że ok. ¼ europejskich VASP jest zarejestrowana w Polsce (tymczasem Austria — 9 firm, Cypr — 16, Dania — 17, Estonia — 42, Francja — 89, Niemcy — 23, Grecja — 7, Malta — 31)⁴⁷. Porównania międzynarodowe wymagają jednak ostrożności, ponieważ państwa stosowały odmienne definicje VASP i różne modele (rejestr informacyjny vs licencja). Widzimy, że w niektórych krajach (szczególnie w Polsce i w Czechach) nie potrafiono poradzić sobie z problemem. W praktyce prowadziło to do modelu, w którym rejestr spełniał funkcję głównie formalno-informacyjną, nie odpowiadając na oczekiwania rynku w zakresie weryfikacji i zaufania (zwłaszcza w relacji z bankami).

W praktyce widać, że podejście przyjęte w *Kanonie dobrych praktyk* z 2017 roku pozostawało skutecznym narzędziem, wymagającym przed wpisem realnej, środowiskowej weryfikacji reputacji i procedur bezpieczeństwa, podczas gdy rejestr państwowy — mimo formalnych kontroli — funkcjonował głównie jako „wirtualny” zbiór oświadczeń.

11.3.3. Międzynarodowe doświadczenia w zakresie sandboxów regulacyjnych

Postulat stworzenia w Polsce „piaskownicy regulacyjnej” był jednym z kluczowych i najczęściej powtarzanych wniosków z prac Strumienia „Blockchain/DLT i waluty cyfrowe” w 2017 roku. Idea sandboxów jest oparta na myśli przewodniej, że „prawo podąża za rozwojem technologii”. Miała na celu stworzenie kontrolowanego środowiska do testowania innowacyjnych usług finansowych pod nadzorem regulatora w warunkach podwyższonej pewności regulacyjnej (w ramach uzgodnionego planu testów i przy aktywnym dialogu z nadzorem), bez naruszania obowiązujących przepisów. Mimo poparcia tej inicjatywy przez Komitet Sterujący programu „Od papierowej do cyfrowej Polski” (decyzja z 12 grudnia 2016 roku) i formalnego przejęcia jej przez KNF w Polsce nie uruchomiono sandboxu regulacyjnego rozumianego jako program umożliwiający kontrolowane testy na realnych klientach (ang. *live testing*) w uzgodnionych warunkach, w skali i formule oczekiwanej przez branżę.

Aby zrozumieć skalę różnicy między podejściem przyjętym w Polsce a modelami wdrażanymi w innych jurysdykcjach, należy najpierw pokazać modele piaskownic regulacyjnych, które w latach 2016 – 2017 wdrażano w innych, wiodących jurysdykcjach FinTech⁴⁸.

Brytyjski Financial Conduct Authority (FCA) należał do pionierów tego podejścia w Europie, otwierając nabór do programu sandbox w 2016 roku. Jego model opierał się na **selekcji kohortowej** — firmy aplikowały w określonych oknach czasowych, a tylko te najbardziej innowacyjne i przynoszące korzyść konsumentom były dopuszczane do testów.

⁴⁷ *List of Virtual Assets Service Providers*, TheBanks.eu, <https://thebanks.eu/list-of-vasps>.

⁴⁸ Przygotowano na podstawie wewnętrznych dokumentów analitycznych Strumienia „Blockchain/DLT i waluty cyfrowe” z 2017 roku.

Skorowidz

A

- algorytm Proof-of-Authority, PoA, 128
 - algorytmy wykrywania anomalii, 130, 131
 - AML, Anti-Money Laundering, 124, 163, 357
 - analiza
 - automatyczna
 - dynamiczna, DAST, 431
 - statyczna, SAST, 431
 - Bitcoina, 199
 - sentymentu, 50, 57
 - anonimowość
 - stosowanie mikserów kryptowalutowych, 115
 - ANSACheck, 143
 - aplikacja BlockProof, 143
 - atak, 76, 413
 - 51%, 417
 - BGP Hijacking, 420
 - DDoS, 413
 - DNS hijacking, 76
 - DoS, 419
 - Dusting Attack, 430
 - Grinding Attack, 418
 - Long Range Attack, 418
 - Partitioning Attack, 420
 - SIM swapping, 429
 - SQL Injection, 427
 - Sybil, 419
 - typu Eclipse, 419
 - XSS, Cross-Site Scripting, 427
 - ataki
 - na „gorące portfele”, hot wallets, 426
 - na „zimne portfele”, cold wallets, 426
 - na mechanizmy komunikacji międzyłańcuchowej, 424
 - konsensusu, 417
 - Proof-of-Stake, 418
 - na system zarządzania, 426
 - na zabezpieczenia do kont, 429
 - phishingowe, 412
 - phishingowe z użyciem AI, 434
 - większościowe w PoS, 418
 - z wykorzystaniem infostealerów, 429
 - keyloggerów, 429
 - logiki ekonomicznej protokołu, 423
 - pożyczek błyskawicznych, flash loans, 423
 - trojanów, 429
 - audyt bezpieczeństwa smart kontraktów, 83
- ## B
- badacze systemów rozproszonych, 197
 - badanie rynku kryptowalut
 - analiza sentymentu, 50
 - dane ankietowe, 52
 - wywiady, 53
 - bezpieczeństwo funkcjonowania ekosystemu i aplikacji, 417
 - infrastruktury technologicznej, 417
 - mostów międzyłańcuchowych, 423
 - użytkownika i jego aktywów, 417
 - warstwy sieciowej P2P, 419
 - wydobycia, 199
 - BitBay, 202
 - bitcoiny, 26
 - Bitcurex, 203
 - BitMarket, 203
 - blockchain
 - bezpieczeństwo danych osobowych, 126
 - bezpieczeństwo transakcji, 126
 - dobór komponentów i algorytmów, 128
 - finansowanie najemników, 174
 - multimediów, multimedia blockchain, 143
 - ograniczanie fake newsów, 141
 - przeciwdziałanie dezinformacji, 140–153
 - reakcje instytucji państwowych, 233–240
 - uwierzytelnianie autentyczności multimediów, 142
 - wdrożenia, 127
 - błędy
 - API, 426
 - aplikacji webowych, 426

błędy

- autoryzacji, 427
- implementacyjne, 418, 420
- w logice walidacji zdarzeń, 424
- w smart kontraktach, 78, 421, 436
- w walidacji bloków, 419
- w walidacji transakcji, 419

bounty campaigns, 74, 75

C

- cenzurowanie transakcji, 418
- CFD, contract for difference, 30
- CFT, Counter-Terrorist Financing, 163
- Chia, 198
- Coinfirm, 208
- crowdfunding
 - kryptowalutowy, 158
 - udziałowy, 207
- CTB, Centrum Technologii Blockchain, 248
- cyberatak, 413 *Patrz* atak cyberbezpieczeństwo, 412, 413
 - blockchainów, 416
 - i odporność operacyjna, ICT, 440–456
 - sprawcy zagrożeń, 415
 - triada CIA, 413
 - w UE
 - analiza rozporządzenia MiCA, 443
 - geneza i kontekst regulacji, 441
 - implikacje dyrektywy NIS2, 451
 - rozporządzenie DORA, 449
- czynności maklerskie
 - w obrocie aktywami cyfrowymi, 406
 - w obrocie instrumentami finansowymi, 399, 406
 - w prawie polskim, 399

D

- DAO, 425
 - zagrożenia, 425
- deanonimizacja użytkowników kryptowalut
 - heurystyki, 110
 - modele transakcji, 106
 - systemy
 - deanonimizacyjne, 113
 - wyzwania, 115
- deepfaki, 138
 - ograniczanie, 142
 - wykrywanie, 143
- DeFi, zdecentralizowane finanse, 339, 356, 415, 421
- dezinformacja, 136, 137, 154
- dialog z administracją publiczną, 223
- DORA, 441, 449
 - główny cel, 449
 - wymogi
 - rozporządzenia, 450
 - zakres zastosowania, 449
 - znaczenie, 451
- dostawcy usług powierniczych, custodians, 426
- dostępność, availability, 414
 - sieci blockchain, 414
 - środków dla użytkownika, 415
 - usług powiązanych, 415
- dowody o zerowej wiedzy, 414
- dowód
 - posiadania środków, PoF, 167
 - źródła majątku, PoW, 167
- due diligence projektów ICO, 82
- dźwignia finansowa, 30

E

- efekt FOMO, 74
- ekonomia
 - dowodów, evidence economy, 141
 - uwagi, 138, 141

- emisja tokenów, 83
- EMT, 382
 - obowiązki emitenta, 386–391
 - rozszczerzenie regulacyjne, 393
 - w świetle MiCA, 385, 391
- exit scam, 74
- exploit, 413

F

- fact-checking, 139
- fake
 - newsy, 138
 - ograniczanie, 141
 - rozpowszechnianie, 138
 - śledzenie źródła, 146
 - partnerships, 75
- fałszywe
 - airdrops, scam airdrops, 429
 - ICO/IDO/airdrops, 429
 - oferty, fake bids/offers, 425
 - portfele, 429
- FATF, Financial Action Task Force, 361, 363
- finansowanie
 - grup prorosyjskich, 165
 - najemników, 158, 161, 171, 174
 - nielegalnej działalności, 159
 - nielegalnych podmiotów, 162
 - z wykorzystaniem Telegramu, 162, 165
 - za pomocą kryptowalut, 162, 165
- firma
 - Coinfirm, 208
 - InPay, 207
- flash loans, 423
- FOMO, fear of missing out, 74

G

- giełda CEX, centralized exchanges, 426
- giełdy kryptowalutowe, 30
- BitBay, 202

Bitcurex, 203
 BitMarket, 203
 emisja tokenów, 83
 manipulacje pump
 and dump, 38, 55
 mechanizmy
 zabezpieczeń, 31
 międzynarodowy
 kontekst problemów,
 184
 nadpodaż, 186
 presja kosztowa, 186
 problemy i upadki, 185
 relacje z bankami, 204
 rodzaje ryzyk, 29
 transakcje, 41
 w Polsce, 183–187
 zasady działania, 30
 GNT, Golem Network
 Token, 206
 górnictwo cyfrowe, 187

H

handel
 kryptoaktywami, 30
 kryptowalutami, 31
 tokenami NFT, 87

I

ICO, Initial Coin Offerings,
 69–85
 asymetria informacji, 70
 boom w 2017 roku, 263
 cyberataki, 76
 due diligence, 82
 manipulacje
 marketingowe, 75
 informacyjne, 75
 nadużycia
 tożsamościowe, 76
 niedojrzałe standardy
 ujawnień, 70
 ocena wiarygodności
 projektu, 82
 ochrona inwestorów, 82
 ograniczanie ryzyk, 82
 oszustwa inwestycyjne
 w emisjach, 73
 regulacje i nadzór, 83
 ryzyka
 dla inwestorów, 70

instytucjonalne
 i jurysdykcyjne, 72
 technologiczne, 71
 studium przypadku
 AriseBank, 79
 Centra Tech, 80
 the DAO, 78
 wykorzystanie
 celebrytów
 do promocji, 80
 identyfikowanie oszustw
 finansowych, 120
 IEO, Initial Exchange
 Offering, 83
 Igoria Trade S.A.
 bezpieczeństwo danych
 i transakcji, 126
 incydent, 413
 InPay, 207
 inwestowanie
 na giełdach
 kryptowalut, 30
 na rynku
 kryptoaktywów, 25
 w sektor
 technologiczny, 30
 inżynieria społeczna, 428

K

klucz prywatny, 414
 kompromitacja
 operatorów mostu, 424
 walidatorów, 424
 kradzież
 danych, 413, 428
 środków, 37
 poprzez aplikacje, 429
 poprzez utratę
 dostępu, 430
 przez nieuczciwych
 pracowników, 427
 typu rug pulls, 429
 z portfeli platformy,
 426
 z pul płynnościowych,
 415
 tożsamości, 37, 73, 426
 kryptoaktywa, 29
 w Polsce, 181–216
 kryptografia
 postkwantowa, PQC, 421
 kryptografowie, 197

L

luka w kodzie
 inteligentnego
 kontraktu, 413
 portfela, 413

M

malware, 412, 416
 manipulacje
 marketingowe, 80
 marketingowe w ICO, 75
 na rynku NFT, 87–105
 mechanizmy zarządzania,
 governance, 423
 media społecznościowe
 rozpowszechnianie fake
 newsów, 138
 sprawdzanie
 wiadomości, 150
 metody
 pozyskiwania
 finansowania, 161
 sprawdzania faktów,
 139
 MEV, Maximal Extractable
 Value, 416
 MiCA, Markets in
 Crypto-Assets Regulation,
 274–280, 314, 357,
 366–381, 385, 441
 a usługi płatnicze, 391
 cyberbezpieczeństwo
 wymogi dla
 dostawców usług,
 448
 wymogi dla
 emitentów, 446
 zakres podmiotowy,
 444
 zakres przedmiotowy,
 444
 zasady i definicje, 445
 obowiązki emitenta
 EMT, 385–391
 regulacje dotyczące usług
 maklerskich, 398
 mikser Tornado Cash, 346
 miksery kryptowalutowe,
 mixers, 115
 międzyblockchainowe,
 116

miksery kryptowalutowe,
mixers
scentralizowane, 115
zdecentralizowane, 116

N

nadużycia tożsamościowe,
76

narzędzia

do deanonimizacji, 114
do śledzenia
przepływów, 434
obrony, 434

NFT, non-fungible token,
87–105, 421

a prawo autorskie,
323–335

badania

algorytmy uczenia
maszynowego, 95
analiza transakcji, 95
ekstrakcja danych, 95
metoda NFTDisk, 94
metodologia, 95
metody statystyczne,
95

metody

wykorzystujące
grafy, 94

modelowanie, 97

opis zmiennych, 103
wyniki, 99

charakter prawny
transakcji, 329

handel tokenami, 87
kwestia droit de suite,
331

obróć tokenami a prawa
autorskie, 327

poła eksploatacji, 332
publiczne

udostępnianie, 330
status prawnoautorski
tokenów, 325

tworzenie i zawartość,
326

zjawisko wash tradingu,
89

nielegalne grupy
najemnicze, 161

NIS2, 441

implikacje, 454

interakcja z MiCA
i DORA, 453
wymogi dyrektywy, 452
zakres podmiotowy,
452

NPP, News Provenance
Project, 143

O

ocena wiarygodności
projektu, 82
ochrona inwestorów, 59, 82
orzecznictwo, 42
oszustwa

finansowe

identyfikacja, 120
najczęściej spotykane
typy, 122
największe
zagrożenia, 121

inwestycyjne, 79, 429
w emisjach ICO, 73

na rynkach
kryptoaktywów, 25
kryptowalut, 54

oszustwo

fałszywe ICO/IDO, 429
pig butchering, 430

P

P2P, Peer-to-Peer, 419

phishing, 37, 122, 428
inwestycyjny, 76

piramida finansowa, 429

platformy scentralizowane
zagrożenia, 426

PoA, Proof of Authority,
128

podatności

kryptograficzne, 420
w kodzie smart
kontraktów, 421
w oprogramowaniu
węzłów, 418
w smart kontraktach
mostu, 424

podatność, 413

podpisy pierścieniowe,
ring signatures, 414

podwójne wydatkowanie
środków, 418

PoF, Proof of Funds, 167

Polski Akcelerator

Technologii Blockchain,
PATB, 241

inicjatywy

wdrożeniowe, 243

model działania, 241

projekty, 243

upadek, 245

postprawda, 136

potwierdzenie źródła
pochodzenia środków,
PSOF, 167

poufność, confidentiality,
413

PoW, Proof of Wealth, 167

pranie pieniędzy, 40, 42,
124, 434

prawa do utworu, 326

prawo autorskie, 323–335
pretexting, 37

probabilistyczna finalizacja
transakcji, 418

Proof-of-Space, 198

Proof-of-Stake, 418

protokoły

DeFi, 423

konsensusu, 431

kryptograficzne, 197

protokoł Tornado Cash, 339
przeciwdziałanie

dezinformacji

sprawdzanie faktów,
139

system DeHiDe, 147

system FiDisD, 148

użycie technologii

blockchain, 140

weryfikowanie

prawdziwości treści,
144–150

fake newsom, 146

finansowaniu

najemników, 171, 175

finansowaniu

terroryzmu, CFT, 163

praniu pieniędzy, AML,
124, 163, 357

PSB, Polskie Stowarzyszenie

Bitcoin, 189, 194

pseudonimowość, 106, 163

pump and dump, 38, 55, 75

R

reakcje instytucji
 państwowych, 233–240
 rejestr VASP, 266
 proces legislacyjny, 268
 rodzaje przestępstw, 35
 rynek ICO, 69–85
 rynek kryptoaktywów, 27
 inwestycje, 25
 konsekwencje
 niestabilności, 186
 modus operandi
 przestępców, 35
 oszustwa, 25
 popełnianie
 przestępstw, 33
 przyczyny
 niestabilności, 186
 reakcje instytucji
 państwowych,
 233–240
 regulacje
 AML, 357
 MiCA, 314, 357,
 366–381, 385, 441
 podejście „common
 law”, 360
 TFR, 357
 w Azji, 361
 ryzyko inwestycyjne, 28
 w Polsce, 254
 boom na ICO, 263
 rejestr VASP, 266
 w roku 2018,
 255–262
 w UE
 charakter prawny
 rozporządzenia, 367
 cyberbezpieczeństwo,
 440–456
 emisja tokena,
 382–397
 MiCA (2019 – 2024),
 274–280
 prawo pierwotne
 i wtórne, 366
 procedura
 ustawodawcza, 368
 rynek kryptowalut
 entuzjaści, 60
 ochrona użytkowników,
 59

oszustwa, 54
 regulacje, 63
 rynek NFT, 87–105,
 323–335, 424
 fałszywe oferty, fake
 bids/offers, 425
 usunięcie metadanych,
 425
 wash trading, 425
 wyłudzanie dostępu
 do portfela, 425
 złośliwe transakcje, 425
 ryzyko, 413
 instytucjonalne
 i jurysdykcyjne, 72
 inwestycyjne, 28
 ograniczenie, 30
 kontrahenta, 427
 na rynku NFT, 424
 SPoF, 433
 strategię mitygacji, 430
 związane z architekturą
 mostu, 424

S

samoorganizacja, 255
 samoregulacja, 217
 sandboxy regulacyjne, 271
 rozwój w Polsce, 272
 sankcje finansowe
 a nowe technologie, 346
 akt prawny IEEPA, 344
 instytucja OFAC, 342
 jako instrument
 polityki, 341
 pojęcie własności, 345
 scamy, scams, 429
 schemat
 Ponziego, 429
 pump and dump, 430
 smart kontrakty
 audyt bezpieczeństwa, 83
 błędy, 421
 arytmetyczne,
 Integer Overflow/
 Underflow, 422
 w kontroli dostępu,
 Access Control
 Vulnerabilities, 422
 cechy, 289
 definicja, 286
 exploity, 436
 generowanie
 zagrożeń, 71
 jako umowa, 292
 niewłaściwa obsługa
 standardów tokenów,
 422
 niezmiennosć,
 immutability, 346,
 351–354
 odpowiedzialność za
 błędy w kodzie, 302
 podatności, 421
 podatności mostu, 424
 ponowne wejście,
 reentrancy, 422
 skuteczność
 sankcjonowania, 339
 w Polsce, 285–309
 wykonanie, 299
 socjotechnika, 36
 SpaceMint, 198
 SPoF, Single Point
 of Failure, 434
 społeczności
 kryptowalutowe
 w Polsce, 189–196
 spójność, integrity, 414
 łańcucha bloków, 414
 smart kontraktów, 414
 stanu systemu, 414
 sprawcy zagrożeń, 415
 sprawdzanie faktów,
 fact-checking
 algorytmy AI, 139
 Community Notes, 139
 Demagog, 139
 Fact Protocol, 144
 metody statystyczne, 139
 narzędzie ClaimBuster,
 139
 PolitiFact, 139
 Wikitribune, 139
 zbiorowa weryfikacja,
 crowdsourced
 fact-checking, 139
 Srebrny Marian, 200
 stablecoin, 30, 434
 start-upy kryptowalutowe,
 206
 strategiczne
 wstrzymywanie, 418

Strumień „Blockchain i kryptowaluty”
 kanon dobrych praktyk, 230
 kierunki prac, 225
 organizacja prac, 224
 utworzenie, 219
 system przeciwdziałania praniu pieniędzy, AML, 124, 163, 357

T

Telegram, 160
 crowdfunding
 kryptowalutowy, 162, 164
 TFR, Transfer of Funds Regulation, 357
 token
 „darmowy”, 429
 bezwartościowy, 429
 NFT, 425
 nieistniejący, 429
 zarządzania,
 governance token, 425
 tokeny
 będące e-pieniędzem, EMT, 382
 NFT, 87, 323–335
 powiązane z aktywami, ART, 382
 użytkowe, 382
 Tornado Cash, 339–365
 brak podmiotu kontrolującego, 347
 działanie miksera, 346
 niezmiennosc smart kontraktów, 347, 351–354
 sankcje OFAC, 348
 kontekst, 348
 problem egzekucji, 350
 reakcja branży, 349
 zdecentralizowana struktura, 347
 zniesienie sankcji przez OFAC
 kontekst decyzji, 355

powody, 356
 reakcje rynku, 356
 znaczenie decyzji, 356
 transakcje
 wizualizacja przepływów, 168
 triada CIA
 dostępność, availability, 414
 poufność, confidentiality, 413
 spójność, integrity, 414

U

uczenie maszynowe
 wyniki badań, 130
 ujawnianie bloków, selfish mining, 418
 upadek giełdy FTX, 25
 usługi
 maklerskie
 ogólne zasady świadczenia, 403
 w zakresie kryptoaktywów, 399
 podstawy prawne, 401
 utrata dostępu do środków, 430
 użytkownik
 zagrożenia, 427

V

vishing, 37

W

waluty fiducjarne, fiat money, 49
 wash trading, 89, 92, 425
 weryfikowanie prawdziwości treści, 144–150
 wiadomości w mediach społecznościowych, 150
 węzły Sybil, 419

Z

zabezpieczenia majątkowe na kryptoaktywach, 310–322
 kluczowe problemy, 317
 rozporządzenie MiCA, 314
 w postępowaniu karnym, 311
 zagrożenia
 dla DAO, 425
 dla infrastruktury technologicznej blockchain, 417
 dla platform scentralizowanych, 426
 dla użytkowników końcowych, 427
 sprawcy
 grupy wspierane przez rządy, 415
 hakywiści, 416
 insiderzy, 416
 mniej zaawansowani atakujący, 416
 script kiddies, 416
 traderzy, 416
 zorganizowane grupy cyberprzestępcze, 415
 związane
 ze smart kontraktami, 71, 421
 ze zdecentralizowanymi aplikacjami, 421
 zagrożenie, 413
 zasady świadczenia usług maklerskich, 403

PROGRAM PARTNERSKI

— GRUPY HELION —



1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA
Helion 

Technologia blockchain z niszowego eksperymentu w ciągu kilkunastu lat stała się elementem współczesnej gospodarki cyfrowej. Jej rosnące znaczenie ujawniło nowe zagrożenia: oszustwa, piramidy finansowe i cyberataki. W odpowiedzi powstały regulacje, które miały uporządkować nowe modele biznesowe i rodzaje aktywów, zapewnić konsumentom lepszą ochronę i ograniczyć niepewność prawną firm. Jednocześnie coraz wyraźniej widać potrzebę rzetelnego spojrzenia na funkcjonowanie „gospodarki on-chain” w praktyce — w rzeczywistym świecie prawa, rynku i regulacji.

Kompendium Blockchain to seria, która porządkuje wiedzę o tej technologii z perspektywy ekonomii, finansów, prawa i praktyki rynku. Ten tom koncentruje się na prawnych i kryminologicznych aspektach kryptoaktywów, wypełniając lukę pomiędzy publicystyką a wąsko wyspecjalizowanymi komentarzami prawniczymi.

Autorzy, łącząc solidny warsztat naukowy z analizą realnych zjawisk i przypadków, omawiają między innymi:

- funkcjonowanie rynku kryptoaktywów i charakterystyczne dla niego mechanizmy
- specyfikę innowacji i nowych modeli finansowania, takich jak crowdfunding kryptowalutowy
- rozwój polskiego ekosystemu — od pierwszych podmiotów i prób samoregulacji po działania instytucji publicznych
- proces dojrzewania regulacji: wprowadzanie unijnych rozporządzeń, regulacje AML, status e-pieniądza i zmiany w krajowych przepisach
- wymagania dotyczące bezpieczeństwa i odporności infrastruktury opartej na blockchainie

Książka jest przeznaczona dla praktyków rynku finansowego, prawników, regulatorów, specjalistów *compliance* i AML, a także badaczy i ekspertów zajmujących się nowymi technologiami. Stanowi uporządkowane kompendium wiedzy dla wszystkich, którzy chcą lepiej rozumieć współczesny ekosystem kryptoaktywów i kierunki jego regulacyjnej ewolucji.

Wydawnictwo Naukowe Helion	KOD KORZYŚCI Sięgnij po więcej! ▶ 
 helion.pl	ISBN 978-83-289-0664-8
 HELION S.A. ul. Kościuszki 1c 44-100 Gliwice tel.: 32 230 98 63 helion@helion.pl	 9 788328 906648
Cena: 149,00 zł	

Blockchain