

Waluty wirtualne jako przedmiot przestępstwa



Adam Behan

Kraków 2022

Szczegółowy spis treści

Wykaz skrótów	13
Wprowadzenie	21
1. Problem i cel badawczy	21
2. Struktura opracowania	27

Rozdział 1. Droga do kryptowalut – rys historyczny

1.1. Protokół ślepych podpisów	33
1.2. DigiCash	36
1.3. NetCheque	40
1.4. E-Gold	40
1.4.1. Wstęp	40
1.4.2. Zabezpieczenie w złocie	41
1.4.3. Popularność e-Gold	45
1.4.3.1. Chargeback	46
1.4.3.2. High Yield Investment Program (HYIP)	49
1.4.4. Precedensowa sprawa sądowa (Stany Zjednoczone <i>versus</i> e-Gold Ltd.)	51
1.4.4.1. Zarzuty	51
1.4.4.2. <i>Memorandum opinion</i> i ukształtowanie się statusu prawnego kryptowaluty	55
1.4.4.3. <i>Plea offer</i> i wątpliwości prawne	59

Rozdział 2. Sposób funkcjonowania kryptowalut na przykładzie ekosystemów Bitcoin i Ethereum

2.1. Wstęp	65
2.1.1. Pieniądz	68

Spis treści

2.1.2.	Wartość Bitcoina	69
2.1.3.	„Bitcoin” a „bitcoin”	73
2.2.	Aspekty techniczne kryptowalut	74
2.2.1.	<i>Peer-to-peer</i> (P2P)	75
2.2.2.	Hash / funkcja skrótu	79
2.3.	Blockchain	86
2.3.1.	Rys historyczny	86
2.3.2.	Blockchain Nakamoto	90
2.3.3.	Blok Bitcoina	91
2.3.3.1.	Wstęp	91
2.3.3.2.	Wielkość bloku	92
2.3.3.3.	Nagłówek Bitcoina (Bitcoin header)	95
2.3.3.4.	Część transakcji	97
2.3.3.5.	Węzły sieci (ang. <i>nodes</i>)	105
2.3.4.	Drzewo Merkle	108
2.4.	Blockchain 2.0	111
2.4.1.	DLT (<i>distributed ledger technology</i>)	112
2.4.1.1.	Wstęp	112
2.4.1.2.	Rodzaje Blockchain	121
2.4.1.3.	Przyszłość DLT (<i>distributed ledger technology</i>)	124
2.4.2.	Smart contracts	125
2.4.2.1.	Wstęp	125
2.4.2.2.	Czym są smart contracts	126
2.4.2.3.	Smart contract a Bitcoin	129
2.4.2.4.	Ethereum	131
2.4.2.5.	Cechy smart contracts	137
2.4.2.6.	Przyszłość smart contracts	138
2.4.3.	Blockchain – pozostałe aspekty prawne	142
2.4.3.1.	Blockchain a RODO	142
2.4.3.2.	Blockchain a prawo konsumenckie	144
2.4.4.	Przyszłość blockchajna	146
2.5.	Adres Bitcoin	147
2.5.1.	Kryptografia asymetryczna	148
2.5.2.	Adresy i klucze w Bitcoinie	150
2.5.2.1.	Klucz prywatny	151
2.5.2.2.	Klucz publiczny	153
2.5.2.3.	Tworzenie adresu	162
2.5.2.4.	Portfele	165
2.5.2.5.	Podpisywanie transakcji	183
2.5.2.6.	Miksowanie transakcji	184
2.6.	Double spending	190
2.7.	Algorytmy konsensusu	192
2.7.1.	Proof of work (PoW) – dowód wykonania pracy	192
2.7.1.1.	Tworzenie bitcoinów i kopanie (ang. <i>mining</i>)	198
2.7.1.2.	Trudność i target Bitcoina (<i>Bitcoin difficulty and target</i>)	203
2.7.1.3.	Moc obliczeniowa sieci Bitcoin (ang. <i>hashrate</i>)	205
2.7.2.	Proof of Stake (PoS) i inne	207
2.8.	Forkowanie sieci (ang. <i>forking</i>)	209
2.8.1.	Priorytet „najdłuższego” łańcucha – <i>the longest chain fork (chain split)</i>	211

Spis treści

2.8.2.	<i>Soft forks</i>	218
2.8.3.	<i>Hard forks</i>	221
2.8.3.1.	Bitcoin	222
2.8.3.2.	Ethereum	226
2.8.3.3.	Niezamierzone forki	228
2.9.	Rozwój protokołu (Bitcoin Improvement Proposal)	229
2.10.	Kto kontroluje Bitcoina	234

Rozdział 3. Pojęcia waluty cyfrowej, wirtualnej i kryptowaluty

3.1.	Wstęp	237
3.2.	Waluta cyfrowa	237
3.3.	Waluta wirtualna	239
3.4.	Kryptowaluta	241
3.4.1.	Wstęp	241
3.4.2.	Cechy kryptowalut	242
3.4.3.	Łatwość transferu	244
3.4.3.1.	Blokowanie działania sieci Bitcoin	245
3.4.4.	Anonimowość (pseudoanonimowość) użytkownika	249
3.4.4.1.	Możliwości deanonimizacji	260
3.4.4.2.	Bitcoin a Tor	270
3.4.4.3.	Dusting attack	271
3.4.4.4.	AEC (ang. <i>anonymity-enhanced cryptocurrency</i>)	272
3.4.5.	Wymienialność	274
3.4.6.	Wymienność / zamiennność (ang. <i>fungibility</i>)	275
3.4.7.	Nieodwracalność*	280
3.4.7.1.	DAO (<i>decentralized autonomous organization</i>)	281
3.4.7.2.	Atak 51%. Opis techniczny	284
3.4.8.	Bezpieczeństwo	293
3.4.9.	Wartość kryptowaluty	294

Rozdział 4. Regulacja walut wirtualnych przed Bitcoinem

4.1.	Wstęp	299
4.2.	Stany Zjednoczone	301
4.2.1.	Waluty wirtualne a pranie brudnych pieniędzy	303
4.2.2.	Bank Secrecy Act	304
4.2.3.	Financial Crimes Enforcement Network	304
4.2.4.	USA Patriot Act	305
4.2.5.	Know Your Customer (KYC)	312
4.2.6.	Financial Action Task Force (FATF, Grupa specjalna ds. przeciwdziałania praniu pieniędzy)	314
4.3.	Europa i wpływ FATF (Financial Action Task Force) na prawodawstwo europejskie	317
4.4.	Polska i implementacje dyrektyw AML	319

Rozdział 5. Regulacja kryptowalut w erze Bitcoina

5.1.	Wstęp	321
5.2.	Status prawny kryptowalut	322
5.2.1.	Stany Zjednoczone	322
5.2.1.1.	Poziom federalny	322
5.2.1.2.	Poziom stanowy	354
5.2.1.3.	Wybrane orzecznictwo amerykańskie dotyczące kryptowalut	357
5.2.1.3.1.	Wstęp	357
5.2.1.3.2.	Sprawa <i>United States versus Ulbricht</i> (sprawa Silk Road)	358
5.2.1.3.3.	Securities and Exchange Commission <i>versus</i> Shavers	365
5.2.1.3.4.	United States <i>versus</i> Faiella	366
5.2.1.3.5.	State of Florida <i>versus</i> Espinoza	369
5.2.1.4.	Podsumowanie	379
5.2.2.	Uregulowania wspólnotowe (Unia Europejska)	380
5.2.2.1.	Regulacje dotyczące walut wirtualnych	380
5.2.2.1.1.	Rys historyczny, dyrektywy AML I–IV	380
5.2.2.1.2.	Dyrektywy AML IV, V i VI	391
5.2.2.1.2.1.	AML IV	391
5.2.2.1.2.2.	AML V	392
5.2.2.1.2.2.1.	Uzasadnienie podjęcia prac prawodawczych nad AML V	392
5.2.2.1.2.2.2.	Przedmiot dyrektywy AML V	400
5.2.2.1.2.2.3.	Dyrektywa AML V a virtual currency (VC)	402
5.2.2.1.2.2.3.1.	Wstęp	402
5.2.2.1.2.2.3.2.	Pojęcie waluty wirtualnej (VC)	403
5.2.2.1.2.2.3.3.	Virtual currency (VC) a mienie	412
5.2.2.1.2.2.3.4.	Dyrektywa AML V a giełdy walut wirtualnych	416
5.2.2.1.2.2.3.5.	Dyrektywa AML V a dostawcy kont waluty wirtualnej	418
5.2.2.1.2.2.3.6.	Podsumowanie	420
5.2.2.1.2.3.	Dyrektywa AML VI i dalsza harmonizacja prawa Unii Europejskiej	421
5.2.2.1.2.4.	Dyrektywa 2019/713	426
5.2.2.1.2.5.	MiCA – Rozporządzenie w sprawie rynków kryptoaktywów i zmieniające dyrektywę (UE) 2019/1937	430
5.2.2.1.2.6.	Pakiet wniosków Komisji Europejskiej dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu	436
5.2.2.1.2.7.	Podsumowanie	438
5.2.2.1.3.	Waluty wirtualne a podatki	441
5.2.2.2.	Wybrane regulacje europejskie dotyczące DLT (<i>distributed ledger technology</i>)	445
5.2.3.	FATF (Financial Action Task Force) a VC (<i>virtual currency</i>)	460
5.2.3.1.	Zmiana rekomendacji 15, VA i VASP oraz Travel Rule	467
5.2.3.2.	Podsumowanie	489
5.2.4.	Polska	491
5.2.4.1.	Pojęcie waluty wirtualnej	492
5.2.4.1.1.	Prawny środek płatniczy emitowany przez NBP, zagraniczne banki centralne lub inne organy administracji publicznej	502

Spis treści

5.2.4.1.2.	Międzynarodowa jednostka rozrachunkowa ustanawiana przez organizację międzynarodową i akceptowana przez poszczególne kraje należące do tej organizacji lub z nią współpracujące	503
5.2.4.1.3.	Pieniądz elektroniczny w rozumieniu ustawy z dnia 19 sierpnia 2011 roku o usługach płatniczych	504
5.2.4.1.4.	Instrument finansowy w rozumieniu ustawy z dnia 29 lipca 2005 roku o obrocie instrumentami finansowymi	506
5.2.4.1.5.	Weksel lub czek wystawiony w prawnym śródku płatniczym lub międzynarodowej jednostce rozrachunkowej	508
5.2.4.2.	Instytucje obowiążane a waluty wirtualne	509
5.2.4.3.	Wartość majątkowa i pranie brudnych pieniędzy	517
5.2.4.4.	Waluty wirtualne a prawo majątkowe	532
5.2.4.5.	Inne	542
5.2.5.	Salwador	544
5.3.	In-game currency	550
5.4.	Podsumowanie	575

Rozdział 6. Prawnkarne aspekty kryptowalut

6.1.	Wstęp	577
6.2.	Waluta wirtualna / kryptowaluta w polskim Kodeksie karnym	580
6.2.1.	Waluta wirtualna a pojęcie rzeczy	585
6.2.2.	Waluta wirtualna a pojęcie dokumentu	589
6.2.3.	Waluta wirtualna a pojęcie instrumentu finansowego	594
6.2.4.	Waluta wirtualna a kodeksowe pojęcie mienia	594
6.2.5.	Waluta wirtualna a korzyść majątkowa	598
6.2.6.	Waluta wirtualna a pojęcie informacji, systemu informatycznego i danych informatycznych	600
6.2.7.	Przepadek	609
6.3.	Wybrane typy czynów zabronionych	615
6.3.1.	„Kradzież” kryptowaluty	615
6.3.2.	Ataki na giełdy walut wirtualnych	619
6.3.2.1.	Mt. Gox	620
6.3.2.2.	Bitmarket	631
6.3.2.3.	Inne ataki na giełdy VC (<i>virtual currency</i>) – przykłady	635
6.3.2.4.	Kwalifikacja prawna na gruncie polskiego Kodeksu karnego	638
6.3.3.	Ataki na blockchain	642
6.3.3.1.	Wstęp	642
6.3.3.2.	Atak 51%	643
6.3.3.3.	Double spend	644
6.3.4.	<i>Crypto jacking</i>	649
6.3.4.1.	Web-based crypto jacking	656
6.3.5.	Atak DDoS (<i>distributed denial of service</i>)	660
6.3.6.	Przepalanie środków przez <i>transaction fee</i>	664
6.3.7.	Łamanie kluczy za pomocą komputerów kwantowych	666
6.3.8.	Pozostałe ataki	667
6.3.9.	Procesowe zabezpieczenie kryptowaluty	668

Rozdział 7. Dalszy rozwój walut wirtualnych i technologii blockchain

7.1.	Przyszłość	673
7.2.	Diem (Facebook) oraz inne rozwiązania Stablecoin	679
7.2.1.	Diem / Libra	679
7.2.2.	Inne Stablecoiny	688
7.2.3.	Regulacje prawne	692
7.3.	CBDC (Central Bank Digital Currency)	695
7.3.1.	Wstęp	695
7.3.2.	Pojęcie i rodzaje CBDC	696
7.3.2.1.	Różnice względem walut wirtualnych	704
7.3.3.	Rozwój	706
7.3.3.1.	Rys historyczny i pierwsze prace badawcze nad CBDC	706
7.3.3.2.	Sand Dollar	711
7.3.3.3.	Szwedzka e-krona	716
7.3.3.4.	Chiński juan	724
7.3.3.5.	Polska	733
7.3.3.6.	Inne państwa	735
7.3.4.	Motywacje wprowadzenia oraz potencjalnie korzyści i zagrożenia	736
7.3.4.1.	Motywy	736
7.3.4.2.	Korzyści	740
7.3.4.3.	Zagrożenia	742
7.3.4.4.	Anonimowość transakcji	745
7.3.5.	Wybrane zagadnienia prawne	747
7.3.5.1.	Wyzwania prawne, jakie stawia CBDC	747
7.3.5.2.	Status CBDC w polskim systemie prawnym i możliwość jej prawnokarnego wartościowania	751
	Podsumowanie* i postulaty <i>de lege ferenda</i>	765
	Bibliografia	773
	Schematy i rysunki	837
	Wykresy	839
	Tabele	841