

# ZABEZPIECZANIE KRYPTOWALUT W POSTĘPOWANIU KARNYM

Aspekty procesowe, techniczne i praktyczne

**podkom. Przemysław Szczerba**

Wydział Informatyki Śledczej CBZC

**Podkom. Przemysław Szczerba**, radca w Wydziale Informatyki Śledczej w Centralnym Biurze Zwalczania Cyberprzestępczości (CBZC) w Warszawie. Posiada ponad 14-letnie doświadczenie w służbach ścigania, specjalizując się w informatyce śledczej oraz zabezpieczaniu dowodów cyfrowych. Certyfikowany specjalista w zakresie: SEC+, CCSK, CHFI, BTL1, eCDFP. Absolwent studiów z zakresu bezpieczeństwa wewnętrznego oraz inżynier informatyki. Trener cyberbezpieczeństwa w NASK. Wielokrotnie zapraszany do wsparcia dydaktycznego w przedsięwzięciach realizowanych przez Zakład Kryminalny Centrum Szkolenia Policji w Legionowie z zakresu szeroko pojętej cyberprzestępczości, analizy kryminalnej czy kryptowalut.

**Obszary zainteresowań:** blockchain forensics, analiza kryptowalut, OSINT/SOCMINT, geolokalizacja cyfrowa, ransomware, postępowanie dowodowe w sprawach cyberprzestępczości.

Artykuł przedstawia kompleksową analizę problematyki zabezpieczania kryptowalut w polskim postępowaniu karnym. Omówiono podstawy technologiczne walut cyfrowych, w tym technologię blockchain, mechanizmy kluczy kryptograficznych oraz rodzaje portfeli. Przedstawiono podstawy prawne zabezpieczania kryptowalut, procedury stosowane przez organy ścigania oraz wytyczne Prokuratury Krajowej z 2023 r. Szczególną uwagę poświęcono wyzwaniom technicznemu i prawnym związanym z pozorną anonimowością transakcji, problemami jurysdykcyjnymi oraz przechowywaniem zabezpieczonych aktywów cyfrowych. Sformułowano rekomendacje dotyczące dobrych praktyk dla funkcjonariuszy organów ścigania i prokuratur.

## WPROWADZENIE

Dynamiczny rozwój technologii rozproszonych rejestrów, zapoczątkowany publikacją koncepcji Bitcoina przez Satoshiego Nakamoto w 2008 r., wywołał fundamentalne zmiany nie tylko w sferze finansowej, ale również w obszarze prawa karnego materialnego i procesowego<sup>1</sup>.

Kryptowaluty, początkowo postrzegane jako niszowy eksperyment technologiczny, stały się pełnoprawnym

instrumentem obrotu gospodarczego, a jednocześnie narzędziem wykorzystywanym przez sprawców przestępstw do transferu i ukrywania środków pochodzących z działalności przestępczej. Zjawisko to wymaga od organów ścigania zarówno odpowiednich kompetencji technicznych, jak i znajomości procedur prawnych właściwych dla tej specyficznej kategorii mienia.

„Informatyk śledczy powinien posiadać pełne zrozumienie technologii, na których opierają się waluty cyfrowe, gdyż tylko to pozwala na przeprowadzenie efektywnych analiz”.

P. Rodwald, *Kryptowaluty z perspektywy informatyki śledczej*, AMW, Gdynia 2021, s. 14.

Stwierdzenie to w równym stopniu dotyczy funkcjonariuszy organów ścigania i prokuratur, którzy coraz częściej stają przed koniecznością zabezpieczania aktywów cyfrowych w toku prowadzonych postępowań karnych. Brak specjalistycznej wiedzy technicznej może prowadzić nie tylko do utraty istotnych dowodów, ale również do nieodwracalnego przepadku mienia o znacznej wartości<sup>2</sup>.

Niniejszy artykuł ma na celu przedstawienie kompleksowej analizy problematyki zabezpieczania kryptowalut w polskim postępowaniu karnym, z uwzględnieniem aspektów technologicznych, prawnych i praktycznych. Opracowanie uwzględnia aktualne wytyczne Prokuratury Krajowej, literaturę specjalistyczną z zakresu informatyki śledczej oraz doświadczenia praktyczne wynikające z dotychczasowych postępowań.

## PODSTAWY TECHNOLOGICZNE KRYPTOWALUT

### Pojęcie i definicja waluty wirtualnej

Ustawodawca polski zdecydował się na wprowadzenie definicji legalnej waluty wirtualnej w art. 2 ust. 2 pkt 26 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Zgodnie z przywołaną regulacją walutą wirtualną jest cyfrowe odwzorowanie wartości, które nie stanowi prawnego środka płatniczego, pieniądza elektronicznego, instrumentu finansowego ani weksla bądź czeku, lecz jest wymieniane w obrocie

gospodarczym na prawne środki płatnicze i akceptowane jako środek wymiany<sup>3</sup>. Definicja ta, choć krytykowana w doktrynie za swoją negatywną konstrukcję, stanowi punkt wyjścia dla kwalifikacji prawnej kryptowalut w postępowaniu karnym.

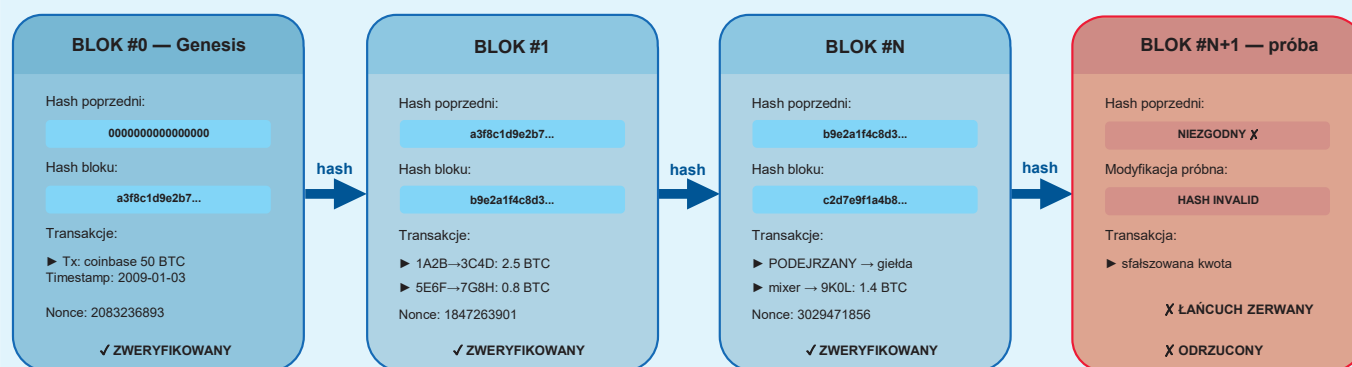
M. Wnęk, analizując naturę prawną kryptowaluty, zwraca uwagę na konieczność rozróżniania pojęciami waluty wirtualnej, waluty cyfrowej i kryptowaluty. W świetle jego analiz termin „kryptowaluta” w sposób najprecyzyjniejszy oddaje istotę omawianych aktywów, akcentując ich kryptograficzny charakter. Rozróżnienie to ma istotne znaczenie praktyczne, ponieważ zakres pojęciowy waluty wirtualnej w rozumieniu ustawowym jest szerszy niż pojęcie kryptowaluty i obejmuje również aktywa nieoparte na technologii blockchain<sup>4</sup>.

### Technologia blockchain i mechanizmy kryptograficzne

Funkcjonowanie kryptowalut opiera się na technologii łańcucha bloków (blockchain), która stanowi zdecentralizowany i rozproszony system rejestracji transakcji. Każdy blok zawiera kryptograficzny skrót (hash) bloku poprzedniego, co tworzy nieprzerwany łańcuch zapewniający integralność danych. Próba modyfikacji jakiegokolwiek historycznej transakcji wymagałaby zmiany wszystkich następujących bloków, co przy odpowiednio dużej sieci jest praktycznie niemożliwe<sup>5</sup>.

Zasadniczym elementem środowiska kryptowalut jest szyfrowanie asymetryczne, oparte na parze klucza publicznego i prywatnego. Klucz publiczny pełni funkcję adresu portfela – jest jawny i umożliwia otrzymywanie środków. Klucz prywatny natomiast służy do autoryzacji transakcji wychodzących i stanowi jedyny dowód dysponowania środkami zgromadzonymi pod danym adresem. Utrata klucza prywatnego oznacza bezpowrotną utratę dostępu do kryptowalut, co ma fundamentalne znaczenie dla procedur zabezpieczania – organy ścigania muszą dążyć do pozyskania tego klucza, aby efektywnie zabezpieczyć walutę cyfrową<sup>6</sup>.

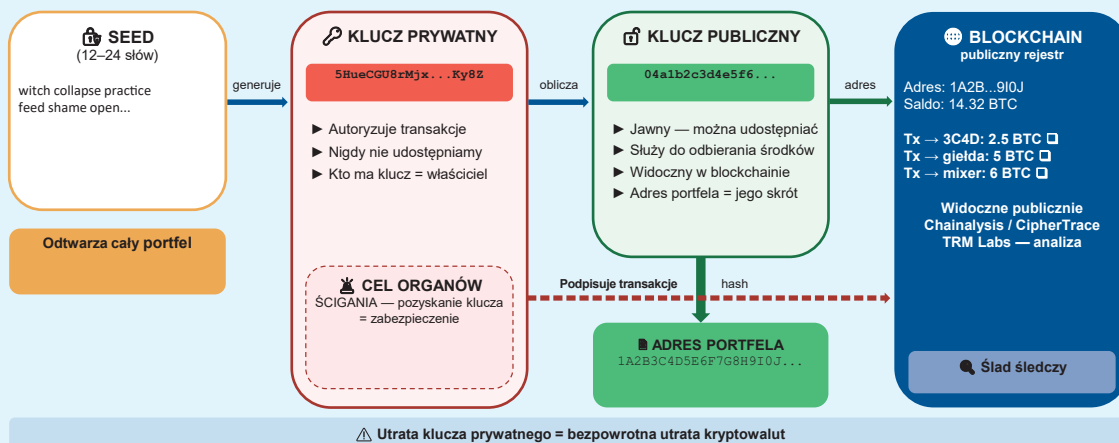
### Technologia Blockchain – struktura łańcucha bloków



⚠ Każda transakcja jest publicznie widoczna i trwale zapisana — modyfikacja historii jest praktycznie niemożliwa przy dużej sieci

Ryc. 1. Struktura łańcucha bloków — każda modyfikacja historycznych danych unieważnia kolejne bloki. Źródło: opracowanie własne.

## Kryptografia asymetryczna – klucze w ekosystemie kryptowalut



Ryc. 2. Kryptografia asymetryczna – relacja między seed, kluczem prywatnym, kluczem publicznym i adresem portfela.  
Źródło: opracowanie własne.

### ⚠️ Kluczowe pojęcie: SEED (frazja odzyskiwania)

Seed to ciąg 12–24 słów w języku angielskim, służący do odtworzenia dostępu do portfela kryptowalutowego.

Samo posiadanie seeda umożliwia odzyskanie środków – bez fizycznego dostępu do urządzenia i bez znajomości kodu PIN. Seed zapisany na kartce papieru, ujawniony podczas przeszukania, może stanowić kluczowy element umożliwiający zabezpieczenie kryptowalut. Należy traktować go z taką samą uwagą jak gotówkę lub klucz do sejfów.

Obok pary kluczy, istotnym pojęciem jest tzw. seed (ziarno), czyli ciąg od 12 do 24 słów w języku angielskim, służący do odtworzenia dostępu do portfela kryptowalutowego. Z perspektywy czynności procesowych oznacza to, że seed ujawniony podczas przeszukania – nawet zapisany odręcznie na kartce papieru – może stanowić kluczowy element umożliwiający zabezpieczenie kryptowalut<sup>7</sup>.

### Rodzaje portfeli kryptowalutowych

Blockchain pełni w ekosystemie kryptowalut rolę rozproszonego rejestru transakcji, porównywalnego funkcjonalnie z księgą wieczystą. Istotne jest, że kryptowaluty nie są fizycznie przechowywane w portfelach – portfel zawiera je-

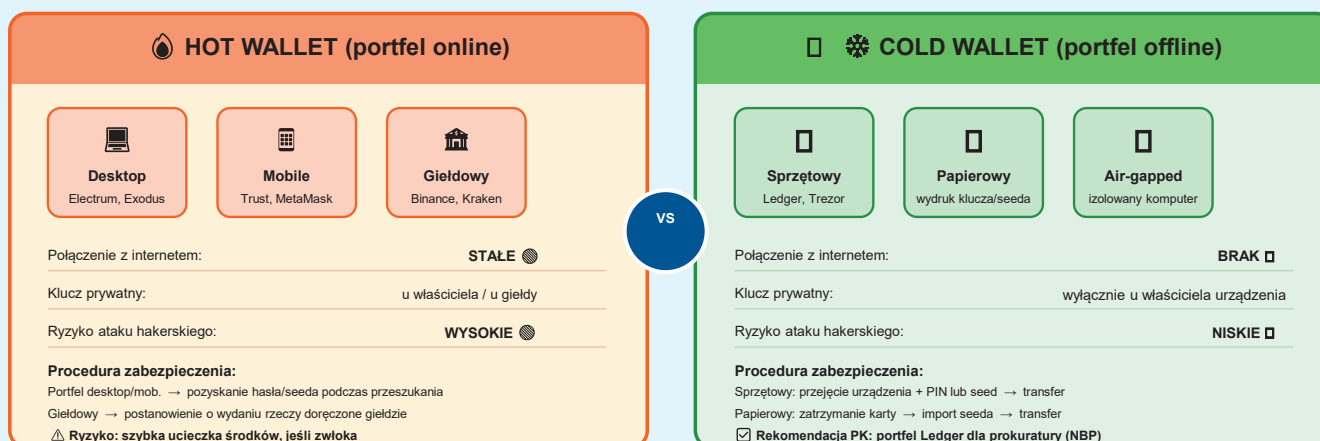
Tabela 1. Rodzaje portfeli kryptowalutowych a właściwa procedura zabezpieczenia.

| TYP PORTFELA                                   | PRZYKŁADY                                | KLUCZ PRYWATNY                                    | PROCEDURA ZABEZPIECZENIA                                                                           |
|------------------------------------------------|------------------------------------------|---------------------------------------------------|----------------------------------------------------------------------------------------------------|
| PORTFEL SPRZĘTOWY (HARDWARE WALLET)            | Ledger Nano X/S+, Trezor Model T/Safe 3  | Wyłącznie u właściciela urządzenia                | Przejęcie urządzenia + kod PIN lub seed → transfer na portfel prokuratury                          |
| PORTFEL PAPIEROWY (PAPER WALLET)               | Wydruk klucza prywatnego lub frazy seed  | Dokument papierowy w posiadaniu właściciela       | Zatrzymanie dokumentu jako dowód rzeczowy → import seeda → transfer środków                        |
| PORTFEL DESKTOPOWY / MOBILNY (SOFTWARE WALLET) | Electrum, Exodus, Trust Wallet, MetaMask | Na urządzeniu użytkownika (zaszyfrowany plik)     | Zabezpieczenie nośnika elektronicznego → pozyskanie hasła lub seeda → transfer                     |
| PORTFEL GIEŁDOWY (CUSTODIAL / EXCHANGE)        | Binance, Kraken, Zonda, Coinbase         | Giełda – użytkownik nie posiada klucza prywatnego | Postanowienie o wydaniu rzeczy doręczone giełdzie; ewentualnie MLA przy giełdach zagranicznych     |
| STABLECOIN ZE SCENTRALIZOWANYM EMITENTEM       | USDT (Tether), USDC (Circle)             | Emitent zachowuje zdolność do zamrożenia portfela | Wniosek o zamrożenie (freeze) do Tether / Circle (LEA request); uwaga: zamrażany jest cały portfel |

Objaśnienia skrótów: **MLA** (ang. *Mutual Legal Assistance*) – wzajemna pomoc prawna w sprawach karnych, formalna procedura współpracy między państwami, polegająca na wystąpieniu jednego państwa do drugiego z wnioskiem o wykonanie określonych czynności procesowych (np. przesłuchanie świadka, dostarczenie dokumentów, zajęcie majątku); **USDT (Tether)** – stablecoin (kryptowaluta powiązana z kursem dolara USD) emitowany przez Tether Operations Limited, jeden z najszerzej stosowanych stablecoinów w obrocie kryptowalutowym; **USDC (USD Coin)** – stablecoin emitowany przez Circle Internet Financial, podobnie jak USDT, utrzymuje parytet 1:1 z dolarem USD, obaj emitenci prowadzą procedury zamrażania portfeli na wniosek organów ścigania (LEA freeze request); **LEA** (ang. *Law Enforcement Agency*) – organ ścigania (policja, prokuratura lub inny właściwy organ uprawniony do ścigania przestępstw).

Źródło: opracowanie własne na podstawie wytycznych Prokuratury Krajowej z 2023 r. i literatury przedmiotu.

## Hot Wallet vs Cold Wallet – znaczenie dla postępowania karnego



Ryc. 3. Portfel online (Hot Wallet) vs portfel offline (Cold Wallet) – porównanie z perspektywy procedur zabezpieczających.  
 Źródło: opracowanie własne.

dyne klucze kryptograficzne umożliwiające dysponowanie środkami zarejestrowanymi w blockchainie. Rozróżnienie to jest kluczowe dla zrozumienia procedur zabezpieczania<sup>8</sup>. Z punktu widzenia czynności procesowych należy wyróżnić dwie zasadnicze kategorie portfeli: zewnętrzne (poza-giełdowe) oraz giełdowe. Kluczowa różnica polega na tym, że w przypadku portfeli giełdowych użytkownik nie dysponuje kluczem prywatnym – klucze te pozostają w gestii giełdy. Ma to bezpośrednie przełożenie na sposób postępowania organów ścigania.

W przypadku portfeli giełdowych zabezpieczenie kryptowalut wymaga współpracy z operatorem platformy, podczas gdy w przypadku portfela zewnętrznego niezbędne jest pozyskanie klucza prywatnego lub seeda<sup>9</sup>.

## PODSTAWY PRAWNE ZABEZPIECZANIA KRYPTOWALUT W POSTĘPOWANIU KARNYM

### Kwalifikacja prawna kryptowalut jako przedmiotu zabezpieczenia

Status prawny kryptowalut w polskim systemie prawnym budzi w dalszym ciągu kontrowersje doktrynalne. Niemniej jednak z perspektywy prawa karnego procesowego kluczo-

we znaczenie ma ustalenie, że waluta wirtualna może zostać uznana zarówno za dowód w sprawie, jak i za mienie podlegające zabezpieczeniu majątkowemu. Okoliczność, że kryptowaluty stanowią jednocześnie cyfrowe odwzorowanie wartości i posiadają określoną wartość majątkową, nie wyklucza ich traktowania jako dowodów rzeczowych<sup>10</sup>. Kodeks postępowania karnego nie zawiera szczególnych przepisów dotyczących zabezpieczania walut cyfrowych. Jak wskazuje Prokuratura Krajowa w wytycznych z 2023 r., brak jest przeciwwskazań do poszukiwania i zabezpieczania dowodów w postaci kryptowalut z wykorzystaniem ujawnionych danych dostępowych. W odniesieniu do kryptowalut zastosowanie znajdują ogólne przepisy dotyczące zatrzymania rzeczy, przeszukania oraz zabezpieczenia majątkowego, uzupełnione o specyficzne dla aktywów cyfrowych aspekty techniczne<sup>11, 12</sup>.

### Dualny charakter zabezpieczenia

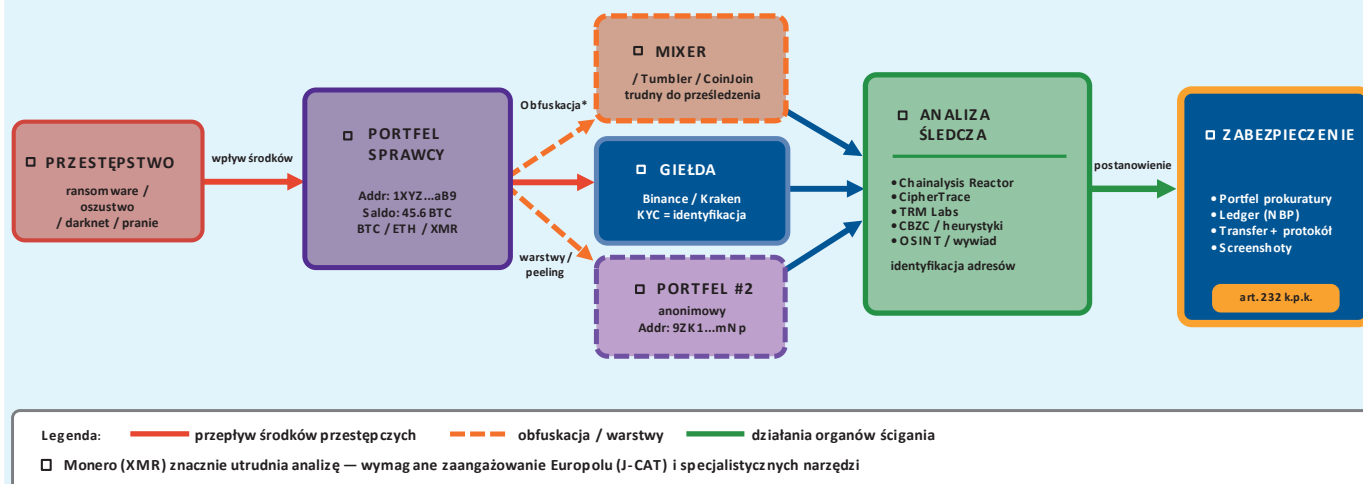
W toku prowadzonych postępowań karnych możliwe jest procedowanie w stosunku do waluty wirtualnej w dwojaki sposób. Po pierwsze, kryptowaluty mogą być zabezpieczane jako mienie podlegające zabezpieczeniu majątkowemu – w szczególności w celu orzeczenia zwrotu pokrzywdzo-

Tabela 2. Dualny charakter zabezpieczenia kryptowalut w postępowaniu karnym.

| KRYTERIUM         | DOWÓD RZECZOWY                                                                                                  | ZABEZPIECZENIE MAJĄTKOWE                                                  |
|-------------------|-----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| CEL PROCESOWY     | Wykazanie okoliczności faktycznych przestępstwa                                                                 | Orzeczenie przepadku lub zwrot korzyści pokrzywdzonemu                    |
| PODSTAWA PRAWNA   | Art. 217 k.p.k., art. 228–236 k.p.k.                                                                            | Art. 291–296 k.p.k., art. 232 § 1 k.p.k.                                  |
| FORMA ORZECZENIA  | Protokół zatrzymania rzeczy + postanowienie o uznaniu za dowód                                                  | Postanowienie o zabezpieczeniu majątkowym lub tymczasowym zajęciu mienia  |
| ORGAN EGZEKUCYJNY | Prokurator / sąd                                                                                                | Komornik lub naczelnik urzędu skarbowego (sprzedaż – art. 232 § 1 k.p.k.) |
| KUMULACJA         | Te same jednostki kryptowaluty mogą być jednocześnie dowodem rzeczowym i przedmiotem zabezpieczenia majątkowego |                                                                           |

Źródło: opracowanie własne na podstawie k.p.k. i Wytycznych PK 2023.

### Mapa przepływu środków – od przestępstwa do zabezpieczenia



Ryc. 4. Mapa przepływu środków od przestępstwa do zabezpieczenia przez organy ścigania. Źródło: opracowanie własne.

\* Obfuskacja (ang. obfuscation) – technika zaciemniania kodu lub danych cyfrowych, polegająca na takim przekształceniu programu lub informacji, że ich zrozumienie i analiza przez człowieka lub narzędzia są znacznie utrudnione, przy jednoczesnym zachowaniu ich pełnej funkcjonalności. Stosowana m.in. przez twórców złośliwego oprogramowania (malware) w celu ukrycia sposobu działania kodu przed analizą śledczą i narzędziami antywirusowymi.

nemu bądź przepadku. Po drugie, ujawnione jednostki cyfrowe mogą stanowić dowód rzeczowy. Nie wyklucza to sytuacji, w której te same jednostki cyfrowe będą jednocześnie dowodem rzeczowym i przedmiotem zabezpieczenia majątkowego<sup>13</sup>.

Priorytetowym celem każdego postępowania przygotowawczego powinno być dążenie do wyrównania szkody wyrządzonej pokrzywdzonemu, w tym w drodze odzyskania utraconych środków. Ma to szczególne znaczenie w sprawach z zakresu cyberprzestępczości, gdzie jedyną drogą wyrównania szkody może okazać się właśnie zabezpieczenie i zwrot zajętych wartości majątkowych<sup>14</sup>.

## PROCEDURY I METODY ZABEZPIECZANIA KRYPTOWALUT

### Czynności przygotowawcze i profilowanie majątkowe

Zgodnie z art. 217 § 1 k.p.k. rzeczy mogące stanowić dowód w sprawie lub podlegające zajęciu powinny być wydane na żądanie sądu lub prokuratora. Jedną z pierwszych czynności, w toku której może dojść do ujawnienia posiadania kryptowalut przez sprawcę, jest czynność przeszukania<sup>15</sup>. Etap profilowania majątkowego stanowi kluczowy element przygotowania do czynności zabezpieczających. Metodyka zabezpieczeń majątkowych Prokuratury Krajowej szczegółowo opisuje czynności poprzedzające zajęcie walut cyfrowych, obejmujące m.in. analizę rachunków bankowych pod kątem transakcji z giełdami kryptowalut, weryfikację źródeł otwartych (OSINT), a także ustalenia operacyjne dotyczące sposobu przechowywania aktywów cyfrowych. Podczas przeszukania należy zwracać szczególną uwagę na wszelkie zapiski mogące stanowić adresy kluczy, hasła, loginy, kody autoryzacyjne, portfele papierowe i sprzętowe oraz na nośniki elektroniczne<sup>16</sup>.

### Algorytm postępowania przy zabezpieczaniu kryptowalut

Tabela 3 oraz rysunek 4 prezentują schemat decyzyjny dla funkcjonariuszy organów ścigania i prokuratorów w zależności od rodzaju portfela i stopnia współpracy ze strony podejrzanego.

### Zabezpieczanie kryptowalut na portfelu giełdowym

Odrębne zagadnienie stanowi sytuacja, gdy ustalono, że ujawniony adres publiczny stanowi portfel giełdowy. W przypadku dobrowolnego wydania loginów i haseł należy postępować analogicznie jak w przypadku portfela zewnętrznego. Natomiast w sytuacji braku ujawnienia kodów dostępowych niezbędne będzie wydanie postanowienia o żądaniu wydania rzeczy, doręczonego bezpośrednio giełdzie<sup>17</sup>.

Możliwe jest również dokonanie blokady konta na giełdzie lub wstrzymania transakcji na podstawie art. 86 ust. 10 ustawy o przeciwdziałaniu praniu pieniędzy, ponieważ rachunek w rozumieniu tej ustawy obejmuje również prowadzony w formie elektronicznej zbiór danych identyfikacyjnych zapewniających możliwość korzystania z jednostek walut wirtualnych<sup>18</sup>.

### Przechowywanie i sprzedaż zabezpieczonych kryptowalut

Kwestia przechowywania zabezpieczonych kryptowalut została szczegółowo uregulowana w Wytycznych PK 2023. Rekomendowaną formą przechowywania jest portfel zewnętrzny – papierowy lub sprzętowy marki Ledger. Konfiguracja portfela sprzętowego powinna zostać przeprowadzona komisyjnie, przy udziale kierownika jednostki, wyznaczonego administratora portfela oraz – w razie potrzeby – specjalisty. Ustanowiony kod PIN oraz wygenerowany seed należy zapisać na odrębnych kartkach, bez sporządzania kopii,

Tabela 3. Algorytm postępowania przy zabezpieczeniu kryptowalut – schemat decyzyjny.

| SYTUACJA FAKTYCZNA                                                                 | WŁAŚCIWY TRYB POSTĘPOWANIA                                                          | KLUCZOWE CZYNNOŚCI I UWAGI PRAKTYCZNE                                                                           |
|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| WŁAŚCICIEL DOBROWOLNIE WYDAJE HASŁA / SEED                                         | Dobrowolne wydanie rzeczy (art. 293 § 6 k.p.k.)                                     | Logowanie do portfela; natychmiastowy transfer na portfel prokuratury; protokół + screenshoty z każdego etapu   |
| KLUCZ PRYWATNY LUB SEED UJAWNIONY PODCZAS PRZESZUKANIA (BRAK DOBROWOLNEGO WYDANIA) | Zatrzymanie rzeczy; logowanie i transfer bez odrębnych czynności egzekucyjnych      | Udział specjalisty CBZC obligatoryjny; dokumentacja każdego kroku; transfer bez zbędnej zwłoki                  |
| BRAK KLUCZY – PORTFEL ZEWNĘTRZNY, SEED NIEZNANY                                    | Eksperyment procesowy z biegłym lub tymczasowe zajęcie mienia (art. 295 § 1 k.p.k.) | Priorytet szybkości: współsprawcy z seedem mogą wyprowadzić środki; następcze postanowienie zatwierdzające      |
| PORTFEL GIEŁDOWY – POLSKA GIEŁDA                                                   | Postanowienie o wydaniu rzeczy doręczone giełdzie (art. 217 § 1 k.p.k.)             | Możliwa blokada na podstawie art. 86 ust. 10 ustawy AML; szybka reakcja polskich podmiotów                      |
| PORTFEL GIEŁDOWY – GIEŁDA ZAGRANICZNA                                              | Kontakt bezpośredni (LEA e-mail); przy odmowie – MLA lub Europol (J-CAT)            | Dobrowolna współpraca = dowód wydany dobrowolnie; brak konieczności MPP; dowody dopuszczalne                    |
| STABLECOIN USDT/USDC – PORTFEL ZIDENTYFIKOWANY                                     | Wniosek LEA o freeze do Tether Operations Limited / Circle Internet Financial       | Zamrażany jest cały portfel – konieczne uwzględnienie środków osób trzecich; procedura następczego odblokowania |

Objaśnienia skrótów: **J-CAT** (ang. *Joint Cybercrime Action Taskforce*) – wspólna inicjatywa operacyjna Europolu skupiająca specjalistów ds. cyberprzestępczości z państw UE oraz krajów partnerskich, powołana do koordynacji działań przeciwko zagrożeniom cybernetycznym o zasięgu transgranicznym; **MPP** (postanowienie o przymusowym przekazaniu) – czynność procesowa zobowiązująca podmiot (np. operatora giełdy kryptowalut) do przymusowego udostępnienia określonych danych lub aktywów na podstawie postanowienia organu procesowego. Źródło: opracowanie własne na podstawie Wytycznych PK 2023 i k.p.k.

a następnie zdeponować wraz z urządzeniem w Narodowym Banku Polskim jako depozyt wartościowy. Ochrona klucza prywatnego stanowi fundamentalny element bezpieczeństwa zabezpieczonych środków<sup>19, 20, 21</sup>.

Co do zasady zaleca się niezwłoczną sprzedaż zabezpieczonych walut cyfrowych na podstawie art. 232 § 1 k.p.k., mając na uwadze niestabilność rynkowej wartości kryptowalut – różnica wartości mienia podlegającego zwrotowi mogłaby stanowić przedmiot roszczeń osoby uprawnionej. Sprzedaży dokonuje organ egzekucyjny – komornik lub naczelnik urzędu skarbowego – nie zaś prokurator<sup>22, 23</sup>.

## WYZWANIA TECHNICZNE I PRAWNE

### Problem anonimowości i identyfikacji posiadaczy

Pozorna anonimowość posiadaczy kryptowalut stanowi jedno z kluczowych wyzwań dla organów ścigania. Zakup jednostek waluty cyfrowej przez sprawcę często stanowi element procedury prania brudnych pieniędzy. W praktyce jednak transakcje w sieci Bitcoin są pseudoanonimowe, nie zaś całkowicie anonimowe – każda transakcja jest publicznie widoczna w blockchainie, a zaawansowane narzędzia analityczne umożliwiają identyfikację użytkowników<sup>24</sup>.

Zastosowanie heurystyk (uproszczonych metod wnioskowania) w pracy informatyka śledczego umożliwia klasyfikowanie adresów kryptowalutowych i wiązanie ich z konkretnymi podmiotami. Połączenie tych metod z platformami analitycznymi, takimi jak Chainalysis Reactor, CipherTrace lub TRM Labs, pozwala na skuteczne śledzenie przepływów środków w sieciach kryptowalutowych<sup>25</sup>.

### Uwaga praktyczna: kryptowaluty prywatności

**Monero (XMR), Zcash (ZEC) oraz Dash w trybie PrivateSend oferują zaawansowane mechanizmy prywatności (ring signatures, zk-SNARKs, CoinJoin), które w istotny sposób utrudniają śledzenie przepływów środków. W przypadku spraw z udziałem tych walut należy w trybie priorytetowym zaangażować Europol (J-CAT) oraz rozważyć użycie specjalistycznych narzędzi. Klasyczne heurystyki analityczne mogą okazać się niewystarczające.**

### Problemy jurysdykcyjne i współpraca międzynarodowa

Zdecentralizowany charakter blockchain powoduje istotne trudności w ustaleniu właściwości miejscowej organów ścigania. Transakcje kryptowalutowe mogą obejmować podmioty z różnych krajów, a giełdy kryptowalut często są zarejestrowane w jurysdykcjach oferujących korzystne regulacje prawne.

Istotnym przykładem współpracy międzynarodowej jest procedura współpracy z emitentami stablecoinów. Tether Operations Limited, emitent najpopularniejszego stablecoina USDT, dysponuje możliwością zamrożenia portfela zawierającego środki będące przedmiotem postępowania. Należy jednak pamiętać, że Tether zamraża całe portfele, nie zaś poszczególne tokeny<sup>26</sup>.

Na poziomie Unii Europejskiej kluczowe znaczenie ma dyrektywa 2014/42/UE w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa, a także

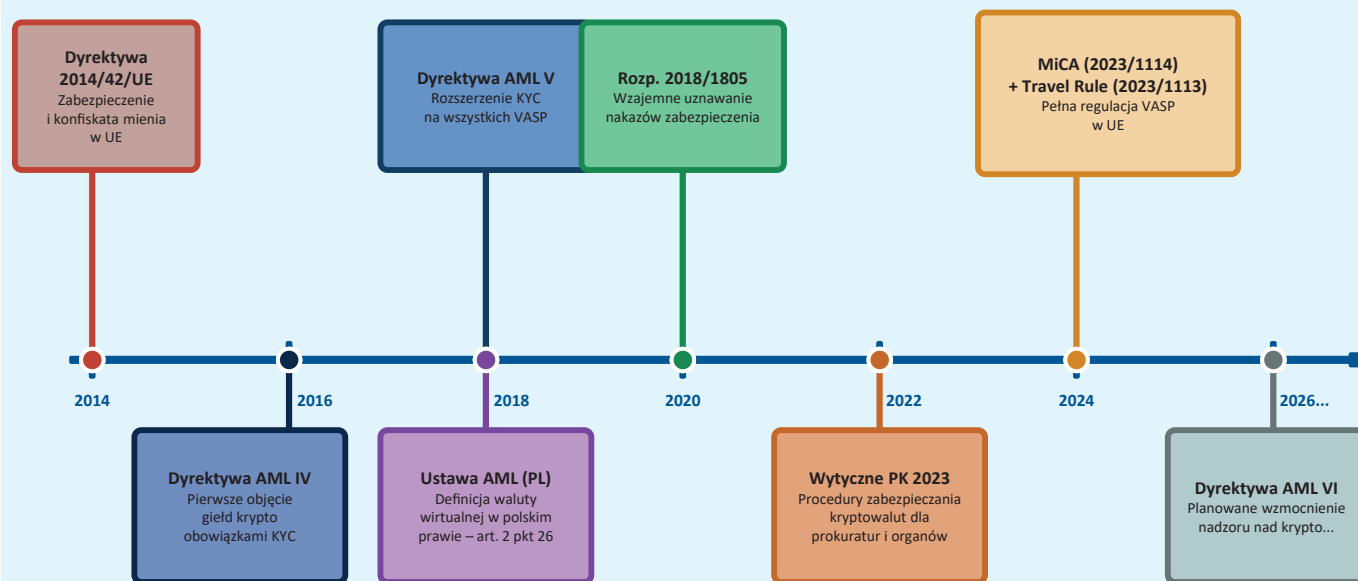
Tabela 4. Kluczowe regulacje Unii Europejskiej – znaczenie dla organów ścigania.

| AKT PRAWNY / INSTRUMENT                            | DATA WEJŚCIA W ŻYCIE | ZNACZENIE DLA ZABEZPIECZANIA KRYPTOWALUT PRZEZ ORGANY ŚCIGANIA                                                              |
|----------------------------------------------------|----------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Dyrektywa 2014/42/UE (konfiskata i zabezpieczenie) | 2014                 | Ramy prawne zabezpieczania i konfiskaty mienia w UE; zastosowanie wprost do kryptowalut jako mienia                         |
| Dyrektywa AML IV (2015/849) i AML V (2018/843)     | 2015 / 2018          | Objęcie giełd kryptowalut obowiązkami KYC/AML; rejestracja VASP; ułatwienie identyfikacji posiadaczy                        |
| Ustawa z 1.03.2018 r. (PL) — implementacja AML IV  | 2018                 | Definicja legalna waluty wirtualnej (art. 2 ust. 2 pkt 26); podstawa kwalifikacji prawnej kryptowalut w RP                  |
| Rozporządzenie (UE) 2018/1805 (wzajemne uznawanie) | 2020                 | Wzajemne uznawanie nakazów zabezpieczenia i konfiskaty między państwami UE; stosowalne do kryptowalut                       |
| Rozporządzenie MiCA — 2023/1114                    | 2024–2025            | Regulacja emitentów kryptoaktywów; obowiązek posiadania licencji VASP; wzmocnienie nadzoru i transparentności rynku         |
| Travel Rule — rozporządzenie 2023/1113             | 2024                 | Obowiązek przekazywania danych o stronach transakcji powyżej 1000 EUR; kluczowy instrument trace'owania (śledzenia) środków |

Objaśnienia skrótów: **KYC** (ang. *Know Your Customer*) – procedura weryfikacji tożsamości klientów, obowiązkowa dla podmiotów świadczących usługi finansowe i kryptowalutowe na mocy przepisów AML; **AML** (ang. *Anti-Money Laundering*) – przepisy i procedury dotyczące przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu; **VASP** (ang. *Virtual Asset Service Provider*) – dostawca usług w zakresie aktywów wirtualnych; definicja wprowadzona przez FATF (Financial Action Task Force) i transponowana do prawa UE dyrektywami AML IV i V, obejmuje giełdy kryptowalut, portfele powiernicze i inne podmioty świadczące usługi związane z kryptoaktywami; **MiCA** (ang. *Markets in Crypto-Assets Regulation*) – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów, kompleksowe ramy prawne UE regulujące emisję i obrót kryptoaktywami, w tym obowiązek uzyskania licencji przez dostawców usług w zakresie kryptoaktywów; **dyrektywa AML IV** – dyrektywa 2015/849/UE w sprawie zapobiegania praniu pieniędzy; **dyrektywa AML V** – dyrektywa 2018/843/UE rozszerzająca obowiązki KYC na giełdy kryptowalut i dostawców portfeli; **Travel Rule** – rozporządzenie 2023/1113 nakładające obowiązek przekazywania danych identyfikacyjnych stron transakcji kryptowalutowych powyżej 1000 EUR.

Źródło: opracowanie własne na podstawie aktów prawa UE.

### Regulacje Unii Europejskiej – oś czasu (perspektywa organów ścigania)



Ryc. 5. Regulacje UE w zakresie kryptowalut – oś czasu z perspektywy organów ścigania. Źródło: opracowanie własne.

## KRYPTOWALUTY – PROCEDURY I METODY ZABEZPIECZANIA

rozporządzenie 2023/1113 (Travel Rule), nakładające na dostawców usług kryptoaktywów obowiązek gromadzenia i przekazywania informacji o stronach transakcji<sup>27, 28</sup>.

## DOBRE PRAKTYKI I REKOMENDACJE

Na podstawie analizy wytycznych Prokuratury Krajowej, literatury specjalistycznej oraz doświadczeń praktycznych sformułowano listę kontrolną dla funkcjonariuszy organów ścigania i prokuratur (tabela 5).

Tabela 5. Lista kontrolna – dobre praktyki przy zabezpieczaniu kryptowalut w postępowaniu karnym.

| Lp. | ZALECANA CZYNNOŚĆ / DOBRA PRAKTYKA                                                                                                          |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | Przed czynnością – zapewnij udział specjalisty CBZC lub biegłego z zakresu kryptowalut i blockchain                                         |
| 2.  | Przeprowadź profilowanie majątkowe: analiza rachunków bankowych, transakcji z giełdami krypto, OSINT, wywiad operacyjny                     |
| 3.  | Podczas przeszukania – poszukuj: fraz seed (kartek, notatników, zdjęć), portfeli sprzętowych, nośników elektronicznych, arkuszy z kluczami  |
| 4.  | Sporządź protokół zatrzymania rzeczy z dokładnymi adresami publicznymi i liczbą jednostek na każdym adresie                                 |
| 5.  | Dokumentuj każdy etap screenshotami: logowanie do portfela, saldo przed transferem, szczegóły transakcji, saldo po transferze               |
| 6.  | Wykonaj natychmiastowy transfer na portfel prokuratury – nie zwlekaj (ryzyko wyprowadzenia środków przez współsprawcę dysponującego seedem) |
| 7.  | Portfel prokuratury – skonfiguruj komisyjnie; PIN i seed na odrębnych kartkach bez kopii; zdeponuj w NBP jako depozyt wartościowy           |
| 8.  | Nie upubliczniaj adresu publicznego portfela prokuratury – wyłącznie na potrzeby konkretnych czynności procesowych                          |
| 9.  | Przy odmowie wydania przez giełdę zagraniczną – kieruj żądanie przez Europol (J-CAT) lub w drodze międzynarodowej pomocy prawnej (MLA)      |
| 10. | Rozważ niezwłoczną sprzedaż na podstawie art. 232 § 1 k.p.k. (niestabilność wartości rynkowej kryptowalut; ryzyko roszczeń)                 |
| 11. | Przy USDT/USDC – złóż wniosek LEA o freeze do Tether / Circle; uwzględnij środki osób trzecich w portfelu; zaplanuj procedurę odblokowania  |
| 12. | Kryptowaluty prywatności (Monero XMR, Zcash ZEC) – zaangażuj Europol/J-CAT; klasyczne narzędzia analityczne mogą być niewystarczające       |

Źródło: opracowanie własne na podstawie Wytycznych PK 2023, Metodyki zabezpieczeń majątkowych PK (2018) i doświadczeń praktycznych autora.

Szczególne znaczenie ma udział specjalisty z zakresu informatyki lub kryptowalut przy każdej czynności zabezpieczającej. Brak specjalistycznej wiedzy technicznej może prowadzić do błędów skutkujących nieodwracalną utratą

środków – np. przesłaniem kryptowaluty na nieprawidłowy adres. Współpraca z Centralnym Biurem Zwalczenia Cyberprzestępczości stanowi w tym zakresie optymalne rozwiązanie<sup>29, 30</sup>.

## PRZESTĘPCZOŚĆ Z WYKORZYSTANIEM KRYPTOWALUT I PRAKTYKA ORZECZNICZA

Kryptowaluty są wykorzystywane w wielu przestępstwach, wśród których dominują: pranie brudnych pieniędzy, oszustwa inwestycyjne, działalność na rynkach darknetowych oraz wymuszenia z użyciem oprogramowania ransomware. A. Błażowska szczegółowo analizuje penalizację prania i fałszowania kryptowalut na gruncie art. 299 i art. 310 Kodeksu karnego, wskazując na rosnącą skalę tego zjawiska<sup>31, 32</sup>.

Polskie orzecznictwo w zakresie kryptowalut jest wciąż stosunkowo skromne, choć systematycznie się rozwija. Kluczowe znaczenie mają rozstrzygnięcia dotyczące kwalifikacji prawnej kryptowalut jako mienia w rozumieniu prawa karnego oraz dopuszczalności ich zabezpieczenia majątkowego. Praktyka prokuratorska, ukształtowana wytycznymi Prokuratury Krajowej, potwierdza możliwość traktowania walut cyfrowych zarówno jako dowodów rzeczowych, jak i przedmiotu zabezpieczenia majątkowego.

**„Sprawy z udziałem kryptowalut wymagają od organów ścigania zdolności do śledzenia środków na poziomie transakcji blockchain, identyfikacji podmiotów powiązanych z adresami portfeli oraz współpracy z dostawcami usług kryptoaktywów. Brak którejkolwiek z tych zdolności praktycznie eliminuje szansę skutecznego zabezpieczenia środków”.**

**A. Błażowska, Kryptowaluty w polskim prawie karnym, C.H. Beck, Warszawa 2024, s. 91.**

Na arenie międzynarodowej warto odnotować precedensowe działania amerykańskich organów ścigania, które wielokrotnie dokonywały zabezpieczenia kryptowalut o wartości setek milionów dolarów w sprawach związanych z działalnością darknetową i praniem pieniędzy. Doświadczenia te stanowią cenne źródło praktycznej wiedzy dla polskich organów ścigania<sup>33</sup>.

## PODSUMOWANIE

Zabezpieczanie kryptowalut w postępowaniu karnym stanowi jedno z najbardziej dynamicznie rozwijających się zagadnień na styku prawa karnego procesowego i technologii informatycznych. Przeprowadzona analiza prowadzi do kilku kluczowych wniosków.

Po pierwsze, polski system prawny – pomimo braku przepisów szczególnych dedykowanych walutom cyfrowym – zapewnia odpowiednią podstawę prawną do ich zabezpieczania w toku postępowania karnego. Przepisy k.p.k. dotyczące zatrzymania rzeczy, przeszukania i zabezpieczenia

majątkowego znajdują pełne zastosowanie do kryptowalut, co potwierdziły Wytyczne Prokuratury Krajowej z 2023 r. Po drugie, kluczowym wyzwaniem pozostaje aspekt techniczny zabezpieczania. Skuteczność czynności zależy od umiejętności pozyskania kluczy prywatnych, seedów lub danych logowania, a także od szybkości działania – zwłoka może prowadzić do nieodwracalnej utraty środków. Nieodzowny jest udział specjalistów z zakresu informatyki śledczej w każdej czynności związanej z zabezpieczaniem walut cyfrowych.

Po trzecie, współpraca międzynarodowa – zarówno na poziomie instytucjonalnym (Europol, Eurojust), jak i bezpośrednim (giełdy, emitenci stablecoinów) – stanowi niezbędny element skutecznego zabezpieczania kryptowalut w sprawach o charakterze transgranicznym. Rozwój unijnych regulacji, w tym rozporządzenia MiCA i Travel Rule, powinien w nadchodzących latach ułatwić współdziałanie organów ścigania państw członkowskich.

Po czwarte, należy podkreślić pilną potrzebę systematycznego szkolenia funkcjonariuszy organów ścigania i prokuratur w zakresie technologii blockchain i kryptowalut. Dynamiczny rozwój tej technologii wymaga stałego aktualizowania kompetencji, a dotychczasowe doświadczenia wskazują, że braki wiedzy technicznej stanowią główną barierę skutecznego zabezpieczania walut cyfrowych w toku postępowań karnych.

<sup>1</sup> S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, <https://bitcoin.org/bitcoin.pdf> [dostęp: 20.01.2025 r.].

<sup>2</sup> P. Rodwald, *Kryptowaluty z perspektywy informatyki śledczej*, Wydawnictwo Akademickie AMW, Gdynia 2021, s. 14–15.

<sup>3</sup> Art. 2 ust. 2 pkt 26 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2025 r. poz. 644, z późn. zm.), dalej: ustawa AML.

<sup>4</sup> M. Wnęk, *Natura prawna kryptowaluty*, Wydawnictwo C.H. Beck, Warszawa 2023, s. 12–15.

<sup>5</sup> P. Rodwald, *Kryptowaluty z perspektywy informatyki śledczej*, s. 17–18.

<sup>6</sup> S. Bala, T. Kopyściański, W. Srokosz, *Kryptowaluty jako elektroniczne instrumenty płatnicze bez emitenta. Aspekty informatyczne, ekonomiczne i prawne*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2016, s. 52.

<sup>7</sup> P. Rodwald, *Kryptowaluty z perspektywy informatyki śledczej*, s. 36–38.

<sup>8</sup> Tamże, s. 46–60.

<sup>9</sup> A. Błażowska, *Kryptowaluty w polskim prawie karnym*, Wydawnictwo C.H. Beck, Warszawa 2024, s. 43–45.

<sup>10</sup> M. Wnęk, *Natura prawna kryptowaluty*, s. 45–48. Zob. też K. Zacharzewski, *Bitcoin jako przedmiot stosunków prawa prywatnego*, „Monitor Prawniczy” 2014, nr 21, s. 1132–1141.

<sup>11</sup> Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2025 r. poz. 46, z późn. zm.), dalej: k.p.k.

<sup>12</sup> Pismo Departamentu do Spraw Cyberprzestępczości i Informatyzacji Prokuratury Krajowej z 2023 r., sygn. 1001-12.024.4.2023, dalej: Wytyczne PK 2023.

<sup>13</sup> Wytyczne PK 2023, s. 2.

<sup>14</sup> Prokuratura Krajowa, *Metodyka zabezpieczeń majątkowych*, Warszawa 2018, s. 290–291.

<sup>15</sup> Art. 217 § 1 k.p.k.

<sup>16</sup> Prokuratura Krajowa, *Metodyka zabezpieczeń majątkowych*, s. 293–296.

<sup>17</sup> Wytyczne PK 2023, s. 8–9.

<sup>18</sup> Art. 86 ust. 10 ustawy AML.

<sup>19</sup> Wytyczne PK 2023, s. 14–16.

<sup>20</sup> Tamże, s. 17–19.

<sup>21</sup> Prokuratura Krajowa, *Metodyka zabezpieczeń majątkowych*, s. 301.

<sup>22</sup> Art. 232 § 1 k.p.k.

<sup>23</sup> Wytyczne PK 2023, s. 12–14.

<sup>24</sup> A. Błażowska, *Kryptowaluty w polskim prawie karnym*, s. 71–93.

<sup>25</sup> P. Rodwald, *Kryptowaluty z perspektywy informatyki śledczej*, s. 11–12.

<sup>26</sup> Informacja uzyskana od Tether Operations Limited w ramach bezpośredniej współpracy z polskimi organami ścigania, 2024.

<sup>27</sup> Dyrektywa Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej (Dz. Urz. UE L 127 z 29.4.2014, s. 39).

<sup>28</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów (Travel Rule) (Dz. Urz. UE L 150 z 9.6.2023, s. 1).

<sup>29</sup> P. Opitek, *Kryptowaluty jako przedmiot zabezpieczenia i poręczenia majątkowego*, „Prokuratura i Prawo” 2017, nr 6, s. 45–62.

<sup>30</sup> Wytyczne PK 2023, s. 17–19.

<sup>31</sup> P. Rodwald, *Kryptowaluty z perspektywy informatyki śledczej*, s. 79–92.

<sup>32</sup> A. Błażowska, *Kryptowaluty w polskim prawie karnym*, s. 84–87. Zob. też art. 299 i art. 310 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2025 r. poz. 383, z późn. zm.).

<sup>33</sup> Prokuratura Krajowa, *Metodyka zabezpieczeń majątkowych*, s. 307–311.

## Bibliografia

### Literatura

Bala S., Kopyściański T., Srokosz W., *Kryptowaluty jako elektroniczne instrumenty płatnicze bez emitenta. Aspekty informatyczne, ekonomiczne i prawne*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2016.

Błażowska A., *Kryptowaluty w polskim prawie karnym*, Wydawnictwo C.H. Beck, Warszawa 2024.

Castronova E., *Synthetic Worlds: The Business and Culture of Online Games*, University of Chicago Press, Chicago 2005.

- Kędzierska A., Korus K., *Kryptowaluty. Regulacje prawne i aspekty podatkowe*, Wolters Kluwer, Warszawa 2022.
- Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008 [dokument elektroniczny – zob. netografia].
- Opitek P., *Kryptowaluty jako przedmiot zabezpieczenia i poręczenia majątkowego*, „Prokuratura i Prawo” 2017, nr 6, s. 45–62.
- Rodwald P., *Kryptowaluty z perspektywy informatyki śledczej*, Wydawnictwo Akademickie AMW, Gdynia 2021.
- Srokosz W., *Definicja waluty wirtualnej – aspekty prawne*, Wrocławskie Studia Erazmianskie 2019, t. XIII, s. 229–244.
- Wnęk M., *Natura prawna kryptowaluty*, Wydawnictwo C.H. Beck, Warszawa 2023.
- Zacharzewski K., *Bitcoin jako przedmiot stosunków prawa prywatnego*, „Monitor Prawniczy” 2014, nr 21, s. 1132–1141.

### Akty prawne

- Dyrektywa Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej (Dz. Urz. UE L 127 z 29.4.2014, s. 39).
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu (AML IV) (Dz. Urz. UE L 141 z 5.6.2015, s. 73).
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę 2015/849 (AML V) (Dz. Urz. UE L 156 z 19.6.2018, s. 43).
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1805 z dnia 14 listopada 2018 r. w sprawie wzajemnego uznawania nakazów zabezpieczenia i nakazów konfiskaty (Dz. Urz. UE L 303 z 28.11.2018, s. 1).
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów (Travel Rule) (Dz. Urz. UE L 150 z 9.6.2023, s. 1).
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów (MiCA) (Dz. Urz. UE L 150 z 9.6.2023, s. 40).
- Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2025 r. poz. 383, z późn. zm.).
- Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2025 r. poz. 46, z późn. zm.).
- Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2025 r. poz. 644, z późn. zm.).

### Dokumenty urzędowe i wytyczne

- Pismo Departamentu do Spraw Cyberprzestępczości i Informatyzacji Prokuratury Krajowej z 2023 r., sygn. 1001-12.024.4.2023 (Wytyczne PK 2023).

- Prokuratura Krajowa, *Metodyka zabezpieczeń majątkowych*, Warszawa 2018.
- Wytyczne Departamentu do Spraw Przestępczości Gospodarczej Prokuratury Krajowej z dnia 20 marca 2020 r., sygn. PK VII PG 025.11.2017.
- Europol, *Cryptocurrency: Tracing the Evolution of Criminal Finances*, EC3 Report, The Hague 2022.
- Financial Action Task Force (FATF), *Virtual Assets and Virtual Asset Service Providers – Updated Guidance*, FATF, Paris 2021.

### Netografia

- Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, <https://bitcoin.org/bitcoin.pdf> [dostęp: 20.01.2025 r.].
- Chainalysis Inc., *The 2024 Crypto Crime Report*, <https://www.chainalysis.com/blog/crypto-crime-report-2024/> [dostęp: 20.01.2025 r.].
- Europol, *IOCTA 2023 – Internet Organised Crime Threat Assessment*, <https://www.europol.europa.eu/publications-events/main-reports/iocta-report> [dostęp: 20.01.2025 r.].
- Tether Operations Limited, *Law Enforcement Guide*, <https://tether.to/en/transparency/#reports> [dostęp: 20.01.2025 r.].
- Prokuratura Krajowa, *Informacje dla organów ścigania*, <https://pk.gov.pl> [dostęp: 20.01.2025 r.].
- CBZC – Centralne Biuro Zwalczania Cyberprzestępczości, *Informacja o działalności*, <https://www.policja.pl/pol/cbzc> [dostęp: 20.01.2025 r.].

**Słowa kluczowe:** kryptowaluty, blockchain, zabezpieczenie majątkowe, postępowanie karne, dowód rzeczowy, informatyka śledcza, klucz prywatny, Prokuratura Krajowa, CBZC, VASP.

### Summary

#### *Securing Cryptocurrencies in Criminal Proceedings. Procedural, Technical and Practical Aspects*

The article presents a comprehensive analysis of the issues related to securing cryptocurrencies in Polish criminal proceedings. The technological foundations of digital currencies are discussed, including blockchain technology, cryptographic key mechanisms and types of wallets. The legal basis for securing cryptocurrencies, procedures applied by law enforcement agencies, and the 2023 guidelines of the National Public Prosecutor's Office are presented. Particular attention is paid to the technical and legal challenges associated with the pseudo-anonymity of transactions, jurisdictional problems, and the storage of secured digital assets. Recommendations of best practices for law enforcement officers and prosecution services are formulated.

**Keywords:** cryptocurrencies, blockchain, asset freezing, criminal proceedings, physical evidence, digital forensics, private key, National Prosecutor's Office, CBZC, VASP.

*Tłumaczenie: Autor*