



KORYCKI &
GRACZYK
CONSULTING
GROUP SPÓŁKA Z
OGRAŃCZONĄ
ODPOWIEDZIALNOŚĆ
CIĄ



Kryptowaluty: metody analizy i identyfikacji podejrzanych transakcji w systemie blockchain – specjalistyczna usługa szkoleniowa w zakresie bezpieczeństwa cyfrowego

Numer usługi 2025/05/08/161638/2731884

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 18 h

📅 26.07.2025 do 27.07.2025

3 000,00 PLN brutto

3 000,00 PLN netto

166,67 PLN brutto/h

166,67 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	• Specjaliści ds. bezpieczeństwa i cyberbezpieczeństwa, • Pracownicy działów AML/KYC, Compliance i audytu wewnętrznego, • Prawnicy i doradcy podatkowi zajmujący się tematyką kryptoaktywów, • Pracownicy instytucji finansowych, banków oraz fintechów, • Osoby odpowiedzialne za wdrażanie procedur zarządzania ryzykiem i regulacji, • Osoby zainteresowane tematyką cyberbezpieczeństwa w zakresie transakcji kryptowalutami.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	3
Data zakończenia rekrutacji	14-07-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	18
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Celem edukacyjnym jest wyposażenie uczestników w zaawansowaną, praktyczną wiedzę dotyczącą zarówno technicznych mechanizmów funkcjonowania kryptowalut i rozwiązań blockchain, jak i prawno-regulacyjnych wymagań związanych z tym rynkiem. Uczestnicy nauczą się ponadto identyfikować, analizować i raportować podejrzone transakcje w kontekście AML i cyberbezpieczeństwa, co ułatwi im skuteczne zabezpieczanie organizacji przed zagrożeniami i zapewnienie zgodności z obowiązującymi przepisami.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
rozróżnia kluczowe typy kryptoaktywów (kryptowaluty, tokeny użytkowe, security tokens, NFT) oraz odróżnia je od walut wirtualnych używanych np. w grach	Uczestnik rozróżnia poszczególne rodzaje kryptoaktywów	Test teoretyczny
	Uczestnik definiuje pojęcia związane z kryptoaktywami	Test teoretyczny
	Uczestnik rozróżnia podstawowe pojęcia z obszaru kryptowalut i blockchain	Test teoretyczny
definiuje podstawowe pojęcia z obszaru kryptowalut i blockchain (m.in. decentralizacja, konsensus, smart kontrakty),	Uczestnik opisuje cechy blockchain	Test teoretyczny
	Uczestnik charakteryzuje specyfikę transakcji w systemie blockchain	Test teoretyczny
charakteryzuje mechanizmy działania sieci blockchain (m.in. funkcje hashujące, rolę górników/walidatorów, model P2P) oraz specyfikę transakcji,	Uczestnik definiuje pojęcia związane z działaniem mechanizmu blockchain	Test teoretyczny
	Uczestnik charakteryzuje wymogi KYC oraz AML w kontekście przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu	Deбата swobodna
	Uczestnik uzasadnia istotę raportowania podejranych transakcji	Deбата swobodna
	Uczestnik rozróżnia najważniejsze schematy działań hakerów z wykorzystaniem kryptoaktywów	Test teoretyczny
monitoruje rynek kryptowalut i transakcje w celu identyfikacji potencjalnie podejranych schematów (darknet markets, ataki phishingowe, rug pull)	Uczestnik identyfikuje potencjalnie podejrane schematy działań w systemie blockchain	Obserwacja w warunkach symulowanych
	Uczestnik monitoruje rynek kryptowalut i transakcji w systemie blockchain	Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
planuje strategię przeciwdziałania zagrożeniom cyberbezpieczeństwa związanym z obrotem kryptowalutami (m.in. wdrażanie procedur wieloskładnikowego uwierzytelniania, audyty bezpieczeństwa)	Uczestnik projektuje strategię przeciwdziałania zagrożeniom naruszającym istotę cyberbezpieczeństwa związaną z obrotem kryptowalutami	Obserwacja w warunkach symulowanych
	Uczestnik przygotowuje procedury w zakresie zwiększenia cyberbezpieczeństwa związanego z obrotem kryptowalutami	Obserwacja w warunkach symulowanych
	Uczestnik organizuje audyty bezpieczeństwa cyfrowego	Obserwacja w warunkach symulowanych
projektuje wewnętrzne procedury i polityki AML, uwzględniające specyfikę transakcji w kryptowalutach oraz wymogi obowiązujących przepisów	Uczestnik projektuje polityki AML w celu zwiększenia bezpieczeństwa transakcji oraz zapewnienia zgodności z obowiązującymi przepisami	Obserwacja w warunkach symulowanych
organizuje proces identyfikacji ryzyka oraz wdrażania metod ograniczania nieprawidłowości i przestępstw (m.in. layering, smurfing, pranie pieniędzy przez DeFi)	Uczestnik uzasadnia istotę identyfikacji i analizy ryzyka	Debata swobodna
	Uczestnik analizuje ryzyko w celu ograniczania nieprawidłowości i przestępstw	Obserwacja w warunkach symulowanych
	Uczestnik rozróżnia rodzaje przestępstw związanych z kryptowalutami	Test teoretyczny
kontroluje zgodność przepływów kryptowalutowych z regulacjami (polskimi i międzynarodowymi) oraz wewnętrznymi standardami bezpieczeństwa	Uczestnik analizuje zgodność przepływów kryptowalutowych z regulacjami w prawie krajowym, unijnym i międzynarodowym	Obserwacja w warunkach symulowanych
	Uczestnik charakteryzuje najważniejsze przepisy związane z zasadami bezpieczeństwa cyfrowego w zakresie transakcji kryptowalutami	Debata swobodna
	Uczestnik rozróżnia podstawy prawne związane z bezpieczeństwem przepływów kryptowalutowych w zakresie prawa wewnętrznego, krajowego, unijnego i międzynarodowego	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
ocenia poziom ryzyka związanego z wykorzystaniem różnych rodzajów portfeli (hot, cold, sprzętowych) i giełd (CEX, DEX) w kontekście technicznym i prawnym	Uczestnik rozróżnia rodzaje portfeli służących do przechowywania walut cyfrowych	Test teoretyczny
	Uczestnik charakteryzuje rodzaje giełd w zakresie handlu kryptowalutami	Deбата swobodna
	Uczestnik analizuje poziom ryzyka związany z handlem kryptowalutami na giełdach kryptowalut w zakresie technicznym oraz prawnym	Obserwacja w warunkach symulowanych
nadzoruje wdrażanie procedur wewnętrznych (SOP) w firmie lub instytucji, mających na celu wykrywanie i raportowanie podejrzanych transakcji oraz utrzymanie zgodności z przepisami KYC/AML	Uczestnik uzasadnia istotę wdrożenia procedur wewnętrznych (SOP) w firmie	Deбата swobodna
	Uczestnik organizuje proces raportowania podejrzanych transakcji	Obserwacja w warunkach symulowanych
	Uczestnik nadzoruje utrzymanie zgodności z przepisami KYC/AML	Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Tak, dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Tak, dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji.

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Tak, dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

Dzień 1 – podstawowe, techniczne i prawne aspekty kryptowalut w zakresie cyberbezpieczeństwa (9 godzin lekcyjnych + 75 minut przerw w ciągu dnia)

8:00 – 9:00 – Moduł 1: Wprowadzenie do szkolenia i świata kryptowalut

- Omówienie programu szkolenia i głównych zagadnień.
- Przedstawienie historii i ewolucji kryptowalut.
- Przedstawienie podstawowych pojęć takich jak kryptowaluta, kryptoaktywa, blockchain, smart kontrakty.
- Różnica pomiędzy kryptowalutami a walutami wirtualnymi (np. w grach, systemach lojalnościowych).

9:00 – 9:15 – przerwa

9:15 – 11:00 – Moduł 2: Aspekty techniczne obrotu kryptoaktywami i walutami wirtualnymi – część I

- Mechanizmy działania blockchain
- Zasada decentralizacji i model P2P (peer-to-peer).
- Bloki, łańcuch bloków i funkcje hashujące (SHA-256, in.).
- Rola górników (mining) i walidatorów (staking w sieciach PoS).
- Rodzaje kryptowalut i kryptoaktywów
- Bitcoin (BTC) – mechanizmy i ograniczenia techniczne.
- Ethereum (ETH), tokeny ERC-20, NFT.
- Altcoiny, stablecoiny, tokeny użytkowe i security tokens.
- Portfele (wallets) i klucze kryptograficzne
- Rodzaje portfeli: gorące (hot), zimne (cold) oraz sprzętowe (hardware wallets).
- Klucze prywatne i publiczne – podstawy bezpieczeństwa.
- Podstawowe ryzyka i dobre praktyki przechowywania.

11:00 – 11:15 – przerwa

11:15 – 13:15 – Moduł 3: Aspekty techniczne obrotu kryptoaktywami i walutami wirtualnymi – część II

- Transakcje na giełdach kryptowalut
- Centralized Exchanges (CEX) vs. Decentralized Exchanges (DEX).
- Mechanizmy obsługi transakcji, order book, AMM (Automated Market Maker).
- Rynek DeFi (Decentralized Finance)
- Smart kontrakty – istota działania, przykładowe zagrożenia.
- Pożyczki, yield farming, staking i inne usługi DeFi.
- Typowe luki bezpieczeństwa (np. „rug pull”, exploit kontraktu).
- Zagrożenia techniczne i incydenty
- Ataki na giełdy (włamania, phishing, malwersacje personelu).
- Sposoby zabezpieczania transakcji i środków (MFA, sprzętowe klucze U2F, itp.).

13:15 – 14:00 – Przerwa obiadowa

14:00 – 16:00 – Moduł 4: Regulacje prawne obowiązujące obecnie i planowane zmiany

- Podstawy regulacji prawnych dla kryptoaktywów w Polsce i na świecie
- Status prawny kryptowalut w Polsce (podatki, definicje).
- Wytyczne KNF, NBP, Ministerstwa Finansów.
- Prawo UE: aktualne dyrektywy i rozporządzenia (MiCA – Markets in Crypto-Assets, 5AMLD/6AMLD dot. AML).
- KYC/AML w kontekście kryptowalut
- Know Your Customer (KYC) – wymogi identyfikacji użytkowników na giełdach krypto.
- Anti-Money Laundering (AML) – zapobieganie praniu pieniędzy, protokoły i procedury.
- Zgłaszanie podejrzanych transakcji (m.in. GIIF w Polsce).
- Regulacje w innych jurysdykcjach

Dzień 2 – prawne aspekty kryptowalut i analiza blockchain (9 godzin lekcyjnych + 75 minut przerw w ciągu dnia)

8:00 – 10:00 – Moduł 5: Analiza blockchain i weryfikacja transakcji

- Podstawy analizy blockchain
- Publiczność łańcucha bloków (np. Bitcoin, Ethereum) vs. prywatność.
- Explorery blockchain (np. Blockchain.com, Etherscan) – omówienie funkcjonalności.
- Identyfikacja adresów i transakcji
- Ustalanie relacji pomiędzy adresami (klastery, heurystyki).
- Techniki maskowania tożsamości (mixery, tumblery, transakcje łańcuchowe).
- Rola tzw. UTXO (Unspent Transaction Output) w BTC i stan konta w ETH.
- Narzędzia do analizy i monitorowania łańcucha
- Komercyjne rozwiązania (np. Chainalysis, Elliptic, CipherTrace).

- Aplikacje open source i darmowe skanery.
- Integracja z systemami AML i automatyczne alerty.

10:00 – 10:15 – przerwa

10:15 – 12:00 – Moduł 6: Identyfikacja podejrzanych transakcji i schematy nadużyć cz. I

- Wzorce i sygnały ostrzegawcze
- Podejrzane przepływy środków, gwałtowny wzrost/rozproszenie transakcji.
- „Layering”, „smurfing”, pranie pieniędzy przez DeFi (np. protokoły mikserów).
- Ransomware i płatności w kryptowalutach – jak je rozpoznać.
- Praktyczne przykłady i studia przypadków

12:00 – 12:15 – przerwa

12:15 – 14:00 – Moduł 7: Identyfikacja podejrzanych transakcji i schematy nadużyć cz. II

- Transakcje związane z Darknet Markets.
- Schematy Ponziego, piramidy finansowe z wykorzystaniem krypto.
- Bezprawne wykorzystanie NFT do prania pieniędzy.
- Najlepsze praktyki w zakresie analizy i raportowania
- Tworzenie procedur wewnętrznych (SOP – Standard Operating Procedures).
- Współpraca z organami ścigania i instytucjami nadzorczymi.
- Dokumentowanie i archiwizacja danych z analizy blockchain.

14:00 – 14:45 – przerwa obiadowa

14:45 – 15:15 – podsumowanie i sesja pytań i odpowiedzi

15:15 – 16:00 – test teoretyczny (walidacja)

1) Szkolenie odbywa się w godzinach dydaktycznych, czyli 1 godzina szkolenia równa się 45 minut, łącznie 18 godzin dydaktycznych.

2) Prowadzone w ramach szkolenia zajęcia realizowane są metodami interaktywnymi i aktywizującymi, rozumianymi jako metody umożliwiające uczenie się w oparciu o doświadczenie i pozwalające uczestnikom na ćwiczenie umiejętności.

3) W ciągu dnia są trzy przerwy o łącznej długości 75 minut, które nie są wliczane w czas trwania szkolenia.

Harmonogram

Liczba przedmiotów/zajęć: 15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 15 Moduł 1: Wprowadzenie do szkolenia i świata kryptowalut	Wojciech Graczyk	26-07-2025	08:00	09:00	01:00
2 z 15 Przerwa	Wojciech Graczyk	26-07-2025	09:00	09:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 15 Moduł 2: Aspekty techniczny obrotu kryptoaktywami i walutami wirtualnymi – część I	Wojciech Graczyk	26-07-2025	09:15	11:00	01:45
4 z 15 przerwa	Wojciech Graczyk	26-07-2025	11:00	11:15	00:15
5 z 15 Moduł 3: Aspekt techniczny obrotu kryptoaktywami i walutami wirtualnymi – część II	Wojciech Graczyk	26-07-2025	11:15	13:15	02:00
6 z 15 Przerwa obiadowa	Wojciech Graczyk	26-07-2025	13:15	14:00	00:45
7 z 15 Moduł 4: Regulacje prawne obowiązujące obecnie i planowane zmiany	Wojciech Graczyk	26-07-2025	14:00	16:00	02:00
8 z 15 Moduł 5: Analiza blockchain i weryfikacja transakcji	Wojciech Graczyk	27-07-2025	08:00	10:00	02:00
9 z 15 przerwa	Wojciech Graczyk	27-07-2025	10:00	10:15	00:15
10 z 15 Moduł 6: Identyfikacja podejrzanych transakcji i schematy nadużyć cz. I	Wojciech Graczyk	27-07-2025	10:15	12:00	01:45
11 z 15 przerwa	Wojciech Graczyk	27-07-2025	12:00	12:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 15 Moduł 7: Identyfikacja podejrzanych transakcji i schematy nadużyć cz. II	Wojciech Graczyk	27-07-2025	12:15	14:00	01:45
13 z 15 przerwa obiadowa	Wojciech Graczyk	27-07-2025	14:00	14:45	00:45
14 z 15 podsumowanie i sesja pytań i odpowiedzi	Wojciech Graczyk	27-07-2025	14:45	15:15	00:30
15 z 15 test teoretyczny (walidacja)	-	27-07-2025	15:15	16:00	00:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 000,00 PLN
Koszt przypadający na 1 uczestnika netto	3 000,00 PLN
Koszt osobogodziny brutto	166,67 PLN
Koszt osobogodziny netto	166,67 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Wojciech Graczyk

Wojciech Graczyk – trener kompetencji miękkich oraz cyfrowych, który podczas swoich szkoleń stawia na praktykę i efekty. W ciągu ostatnich pięciu lat przeprowadził ponad 2300 godzin szkoleń, w tym ponad 400 godzin zegarowych w zakresie cyberbezpieczeństwa. Obecnie jest administratorem danych osobowych w spółce pod firmą KORYCKI & GRACZYK CONSULTING GROUP sp. z o.o. oraz jest odpowiedzialny za zabezpieczanie systemów, danych oraz informacji w

infrastrukturze firmowej. Ukończył specjalistyczne szkolenia w zakresie zaawansowanych technik cyberbezpieczeństwa ze szczególnym uwzględnieniem prawnych aspektów cyberbezpieczeństwa oraz ustalania haseł. Dodatkowo ukończył kurs w zakresie ochrony danych osobowych na wydziale psychologii i prawa Uniwersytetu SWPS w Poznaniu. Współpracował z Marcinem Smreczakiem w celu popularyzacji wiedzy technicznej i prawnej w zakresie kryptowalut. Jest również autorem e-booka w zakresie kryptowalut i licznych artykułów.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Komplet materiałów zostanie wysłany w wiadomości e-mail dla każdego z uczestników szkolenia.

Zestaw materiałów szkoleniowych składa się z **prezentacji** oraz **skryptu szkolenia**.

Informacje dodatkowe

1) Uczestnik szkolenia otrzyma zaświadczenie o ukończeniu szkolenia dopiero **po pozytywnym wyniku walidacji**, która składa się z **testu sprawdzającego wiedzę**, który odbędzie się w ostatnim bloku zajęciowym oraz **obserwacji w warunkach symulowanych** kompetencji zdobytych podczas szkolenia. Warunkiem otrzymania zaświadczenia o ukończeniu szkolenia jest pozytywny wynik walidacji (próg zdawalności **80%**) oraz frekwencja na minimalnym poziomie **80%**.

2) Informujemy, że szkolenie będzie nagrywane!

3) Jeśli szkolenie będzie dofinansowane ze środków publicznych w **co najmniej 70%**, to szkolenie będzie **zwolnione z podatku VAT** (podstawa prawna: par. 3 ust. 1 pkt 14 *Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień* (t.j. Dz. U. z 2023 r. poz. 955 z późn. zm.)).

Warunki techniczne

1. **Platforma komunikacyjna** – Google Meet

2. **Wymagania sprzętowe**: komputer stacjonarny/laptop, mikrofon, słuchawki/ głośniki, system operacyjny minimum Windows XP/MacOS High Sierra, min. 2 GB pamięci RAM, pamięć dysku minimum 10GB,

3. **Sieć**: łącze internetowe minimum 50 kb/s,

4. **System operacyjny** minimum Windows XP/MacOS High Sierra, przeglądarka internetowa (marka nie ma znaczenia)

5. **Okres ważności linku**: od 1 h przed godziną rozpoczęcia szkolenia w dniu pierwszym do godziny po zakończeniu szkoleń w dniu ostatnim

Kontakt



Wojciech Graczyk

E-mail wojciech.graczyk@korycki-graczyk.pl

Telefon (+48) 698 291 420