KWARTALNIK NAUK O PRZEDSIĘBIORSTWIE

2/2024

dr hab. Dorota Ciesielska-Maciągowska, prof. SGH
Szkoła Główna Handlowa
w Warszawie
Instytut Rynków i Konkurencji
e-mail: dorota.ciesielska@sgh.waw.pl
ORCID: 0000-0002-6393-9491

mgr Łukasz Spyra
Szkoła Główna Handlowa
w Warszawie
e-mail: ukasz.spyra@gmail.com
ORCID: 0009-0006-8820-5060

Giełdy i portfele kryptowalut w systemie zdecentralizowanych finansów

Cryptocurrency exchanges and crypto wallets in the decentralized finance system

Słowa kluczowe:
blockchain, kryptowaluty, giełdy kryptowalutowe, CEX (centralized exchanges), DEX (decentralized exchanges), portfele kryptowalutowe, DeFi (decentralized finance)

Streszczenie: Kluczowym wyzwaniem dla inwestorów oraz użytkowników jest zrozumienie podstawowych mechanizmów umożliwiających efektywne zarządzanie i alokację cyfrowych aktywów. Rozwój kryptowalut zapoczątkował powstanie systemu giełd, które działają jako pośrednicy w obrocie cyfrowymi aktywami oraz portfeli kryptowalutowych. Scentralizowane giełdy kryptowalut funkcjonują jako pośrednik między kupującym a sprzedającym i pozyskują środki pieniężne dzięki prowizjom i opłatom transakcyjnym. Z kolei zdecentralizowana giełda pozwala na przeprowadzanie transakcji peer-to-peer bezpośrednio z portfela cyfrowego, bez udziału pośrednika. Portfele kryptowalut umożliwiają przechowywanie, wymianę oraz aktywne uczestnictwo i wspieranie sieci blockchain, czyli staking tokenów. W konsekwencji celem niniejszego artykułu jest przedstawienie specyfiki systemu giełd oraz portfeli kryptowalutowych. Metoda badawcza wykorzystana w niniejszym artykule obejmuje analizę literatury naukowej oraz badań dotyczących kryptowalut.

Keywords:
blockchain, cryptocurrencies, cryptocurrency exchanges, CEX (centralized exchanges), DEX (decentralized exchanges), cryptocurrency wallets, DeFi (decentralized finance)

Abstract: The key challenge for investors is to understand the basic mechanisms enabling the effective management and allocation of digital assets. The development of cryptocurrencies initiated the creation of a system of exchanges that act as intermediaries in the trading of digital assets and cryptocurrency wallets. Centralized cryptocurrency exchanges act as an intermediary between buyers and sellers and raise money through commissions and transaction fees. In turn, a decentralized exchange allows you to conduct peer-to-peer transactions directly from your digital wallet, without the involvement of an intermediary. Cryptocurrency wallets enable storage, exchange, and

active participation in and support of the blockchain network, i.e. token staking. Consequently, the aim of this article is to present the specifics of the system of cryptocurrency exchanges and currency wallets. The research method used in this article includes the analysis of scientific literature and research on cryptocurrencies.

JEL:
E42, E44, E47, E49, F31, F38, G11, G14, G23, 016

Wprowadzenie

W obliczu dynamicznie rozwijającego się rynku kryptowalut i ekspansji zdecentralizowanych finansów (DeFi), kluczowym wyzwaniem dla inwestorów oraz użytkowników jest zrozumienie podstawowych mechanizmów umożliwiających efektywne zarządzanie i alokację cyfrowych aktywów. Kryptowaluta to cyfrowy składnik majątku, zaprojektowany jako medium wymiany, które wykorzystuje kryptografię do zabezpieczenia transakcji finansowych, kontrolowania tworzenia dodatkowych jednostek i weryfikacji transferu aktywów [Sobiecki, 2014]. Istnieje wiele definicji kryptowalut, przy czym zgodnie z ustawą z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, kryptowaluty to „waluta wirtualna, czyli cyfrowe odwzorowanie wartości, które nie jest:

- prawnym środkiem płatniczym emitowanym przez NBP, zagraniczne banki centralne lub inne organy administracji publicznej,
- międzynarodową jednostką rozrachunkową ustanawianą przez organizację międzynarodową i akceptowaną przez poszczególne kraje należące do tej organizacji lub z nią współpracujące,
- pieniądzem elektronicznym w rozumieniu ustawy o usługach płatniczych,
- instrumentem finansowym w rozumieniu ustawy o obrocie instrumentami finansowymi,
- wekslem lub czekiem

oraz jest wymienialne w obrocie gospodarczym na prawne środki płatnicze i akceptowane jako środek wymiany, a także może być elektronicznie przechowywane lub przeniesione albo może być przedmiotem handlu elektronicznego". Należy wspomnieć, że w 2024 r. planowane jest wprowadzenie ustawy dotyczącej kryptowalut, przy czym obecnie prowadzone są prace nad tym projektem [Kancelaria Prezesa Rady Ministrów, 2024]. Kryptowaluta nie powinna być traktowana jako synonim waluty wirtualnej, ze względu na fakt, że istnieją waluty wirtualne, z których nie wszystkie wykorzystują technologię blockchain i powiązane z nią metody kryptograficzne do rejestracji transakcji [UKNF, 2021].

Rozwój kryptowalut zapoczątkował powstanie systemu giełd, które działają jako pośrednicy w obrocie cyfrowymi aktywami oraz portfeli kryptowalutowych, umożliwiających przechowywanie posiadanych tokenów zróżnicowanym pod względem bezpieczeństwa oraz wymaganego poziomu doświadczenia i wiedzy użytkownika.

Celem artykułu jest przedstawienie kluczowych aspektów związanych z systemem giełd i portfeli kryptowalutowych umożliwiających przechowywanie, wymianę oraz staking tokenów. Charakterystyka i analiza istotnych cech giełd oraz portfeli kryptowalutowych umożliwia dokonanie użytkownikom kryptowalut najbardziej optymalnego wyboru, związanego z alokacją i przechowywaniem posiadanych środków. Istotne znaczenie dla użytkowników kryptowalut ma ponadto analiza czynników związanych z bezpieczeństwem, anonimowością, kosztami oraz zagrożeniami poszczególnych metod przechowywania i wymiany kryptowalut. Przedstawione przepływy kapitałowe między giełdami oraz portfelami kryptowalutowymi, umożliwią ilustrację praktycznego wymiaru poszczególnych etapów przepływu kapitału, istotnych z perspektywy wybranego środka przechowywania tokenów oraz potencjalnej alokacji z wykorzystaniem usług oferowanych przez zdecentralizowane finanse.

Specyfika giełd kryptowalut

System obrotu kryptowalutami odbywa się w wielu odmiennych od siebie formach. Funkcjonują zarówno giełdy kryptowalut, jak i kantory wymiany, portfele waluty wirtualnej oraz wymiany, a także bankomaty kryptowalut. Niniejszy artykuł jest poświęcony zagadnieniom związanym z niepowtarzalnym charakterem giełd kryptowalut. Należy podkreślić, że istotę funkcjonowania giełd oraz portfeli kryptowalutowych stanowi proces związany z przepływami strumienia gotówki i kryptowalut.

Wyróżnia się dwa rodzaje giełd wymiany kryptoaktywów. Pierwszą jest scentralizowana giełda, czyli CEX (centralized exchange), czyli taka, która posiada swoją siedzibę oraz widnieje w rejestrze przedsiębiorstw w danym kraju [Hyeji, Sung H. Han, Ju Hwan Kim, Kimin Kwon, 2021]. Drugi rodzaj stanowi zdecentralizowana giełda wymiany kryptowalut, czyli DEX (decentralized exchange), która stanowi niezależny od organów państwowych i instytucji podmiot zajmujący się obrotem kryptowalutami, nieumożliwiający ich przechowywania, gdyż w tym przypadku tokeny muszą pozostać na niepowierniczym portfelu kryptowalutowym. Korzystanie ze scentralizowanych i zdecentralizowanych giełd kryptowalut, w każdym przypadku wiąże się z pewnymi różnicami związanymi z bezpieczeństwem, anonimowością czy kosztami [Essén, Ekholm, 2020].

Scentralizowane giełdy kryptowalut działają jako pośrednik między kupującym a sprzedającym i pozyskują środki pieniężne dzięki prowizjom i opłatom transakcyjnym. Funkcjonują one w sposób podobny do tradycyjnej giełdy papierów wartościowych oraz

stanowią pierwszy etap w procesie zakupu kryptowalut, gdyż przyjmują przelew gotówki w formie waluty fiat oraz umożliwiają wypłatę fiat z powrotem na konto bankowe. Pierwszym etapem, prowadzącym do zakupu jednostki danej kryptowaluty na scentralizowanej giełdzie wymiany kryptowalut, jest przelew waluty fiat na konto giełdowe, na którym następnie będzie możliwa jej wymiana na wybrany token [Wang, Rujia Li, Qi Wang, Chen, 2021]. Popularne giełdy kryptowalut to Binance, Coinbase Exchange, Kraken czy KuCoin [Barbon, Ranaldo, 2023]. Podobnie jak strony internetowe lub aplikacje do handlu akcjami, giełdy te pozwalają inwestorom kupować i sprzedawać aktywa cyfrowe. Aktywa te można sprzedawać po obowiązującej cenie, zwanej spotem, lub pozostawiać zlecenia, które zostaną zrealizowane, gdy aktywo osiągnie pożądaną przez inwestora cenę docelową, określaną jako limit. Giełdy CEX działają opierając się na systemie księgi zamówień, co oznacza, że zlecenia kupna i sprzedaży są notowane i sortowane według zamierzonej ceny kupna lub sprzedaży. Algorytm giełdy następnie dopasowuje kupujących i sprzedających, opierając się na najlepszej możliwej do wykonania cenie, biorąc pod uwagę pożądaną wielkość partii. W związku z tym, cena aktywów cyfrowych będzie zależeć od podaży i popytu tego składnika aktywów w stosunku do innych, bez względu czy to waluta fiat, czy kryptowaluta [Qin, Zhou, Afonin, Lazzaretti, Gervais, 2021]. Obecność scentralizowanego kontrahenta na CEX, nakłada na niego domyślny stopień odpowiedzialności za utrzymanie porządku na rynku, dopełnienie kontroli KYC/AML wobec użytkowników, a także nakłada na giełdę obowiązek zapewnienia bezpieczeństwa kapitału ulokowanego przez inwestorów.

Scentralizowane giełdy oferują inwestorom mniej skomplikowany sposób handlu i inwestowania w kryptowaluty [Bentov, Ji, Zhang, Breidenbach, Daian, Juels, 2019] oraz bezpieczeństwo i niezawodność związaną z transakcjami i handlem. Ponoszą one ponadto odpowiedzialność za zdeponowane na nich aktywa. Scentralizowane giełdy ułatwiają również transakcję poprzez rozwiniętą, scentralizowaną platformę. Korzystanie z CEX wiąże się jednak z pewnymi zagrożeniami, co wynika z faktu, że giełdy są obsługiwane przez firmy, które są odpowiedzialne za środki swoich klientów [Bentov, Ji, Zhang, Breidenbach, Daian, Juels, 2019]. Giełdy takie przechowują kryptowaluty znacznej wartości, a w konsekwencji stają się celem ataków hakerów oraz potencjalnych kradzieży lub malwersacji[1] [Bentov, Ji, Zhang, Breidenbach, Daian, Juels, 2019]. Ponadto w przeciwieństwie do transakcji peer-to-peer, scentralizowane giełdy często pobierają wysokie w porównaniu z DEX, opłaty transakcyjne za swoje usługi.

[1] Przykład stanowi upadek giełdy FTX w listopadzie 2022 r., której zarząd dokonywał nieoficjalnych decyzji i wyprowadzał kapitał z giełdy, doprowadzając do jej upadku i utraty części lub całości zdeponowanych przez jej użytkowników środków.

Tabela 1. Analiza porównawcza scentralizowanej oraz zdecentralizowanej giełdy wymiany kryptowalut

Cechy	CEX	DEX
Rodzaj giełdy	Scentralizowana	Zdecentralizowana
Możliwość przechowywania kryptowalut	Tak	Nie, wymóg połączenia z portfelem kryptowalutowym typu Non-custodial
Zakup kryptowalut za pieniądze fiat	Możliwość kupna kryptowalut przy wykorzystaniu waluty fiat	Waluty Fiat wyłączone z obrotu, możliwość wykorzystania wyłącznie kryptowalut
Klucz Prywatny i Seed Phrase	Brak klucza prywatnego i seed phrase, dostęp do serwisu konsumenta oraz wsparcia technicznego	Konieczność zachowania klucza prywatnego do zdecentralizowanego portfela kryptowalutowego, jego utrata oznacza brak dostępu do środków
Dostęp do produktów inwestycyjnych	Ograniczenie dostępu jedynie do produktów inwestycyjnych dostępnych na giełdzie	Dostęp do pełnego spektrum projektów krypowalutowych oraz wybranych usług dostępnych dzięki zdecentralizowanym finansom
Anonimowość, rejestracja i walidacja konta	Brak anonimowości, konieczność rejestracji, podania danych osobowych i walidacji konta opierając się na lokalnych regulacjach	Pełna anonimowość, brak konieczności rejestracji i podania danych osobowych oraz nieograniczony dostęp do środków
Opłaty transakcyjne	Wysokie, najdroższa forma przechowywania i wymiany kryptowalut	Niskie, związane jedynie z walidacją transakcji na sieci blockchain, wymiana walut po cenie rynkowej
Poziom zaawansowania użytkownika	Transakcje poprzez rozwiniętą, scentralizowaną platformę, umożliwiają początkującym inwestorom mniej skomplikowany sposób handlu i inwestowania w kryptowaluty	Brak scentralizowanego administratora oznacza, że użytkownik jest całkowicie odpowiedzialny za swoje aktywa, przeznaczone są dla zaawansowanych inwestorów
Bezpieczeństwo	Administrator giełdy zarejestrowany w danym kraju, odpowiedzialny za bezpieczeństwo zgromadzonych na giełdzie środków. Jednak zagrożenie atakami hakerskimi, kradzieżą lub malwersacjami związanymi z działaniami zarządu	Pełna anonimowość i odpowiedzialność użytkownika za zgromadzone aktywa, zabezpieczenie kluczem prywatnym i seed phrase. Brak zagrożeń związanych z atakami hakerskimi, kradzieżą lub malwersacjami związanymi z działaniami zarządu

Źródło: badanie i analiza własna na podstawie Y. Wang, W. Lu, M.-B. Liu, R. Ren, W.K. Härdle [2024].

Drugi rodzaj giełdy wymiany kryptoaktywów stanowi zdecentralizowana giełda DEX, która pozwala na transakcje peer-to-peer bezpośrednio z portfela cyfrowego, bez udziału pośrednika jak w przypadku CEX. Przykładami DEX są: Uniswap, Pancake-Swap, dYdX i Kyber. Zdecentralizowane giełdy opierają się na inteligentnych kontraktach, poprzez samowykonujące się części kodu na blockchainie [Kumar, Nikhil, Singh,

2020]. Taka forma wymiany pozwala na większą prywatność i szybszy przepływ tokenów niż w przypadku scentralizowanej giełdy. Jednak w przypadku DEX brak pośredniczącej strony trzeciej oznacza, że użytkownik jest całkowicie odpowiedzialny za swoje aktywa, dlatego zdecentralizowane giełdy przeznaczone są dla zaawansowanych inwestorów. W celu korzystania z DEX, potrzebny jest jedynie niepowierniczy portfel kryptowalutowy – i ze względu na jego zdecentralizowaną naturę nie ma wymogu rejestracji od użytkowników zdecentralizowanej giełdy.

Użytkownicy zdecentralizowanych giełd nie muszą przekazywać swoich aktywów stronie trzeciej, dlatego nie ma ryzyka związanego z atakami hakerskimi. Ponadto ze względu na możliwość wymiany kryptowalut peer-to-peer, zapobiegają manipulacjom rynkowym chroniąc swoich użytkowników przed utratą kapitału [McMenamin, Daza, Fitzi, O'Donoghu, 2022]. DEX nie wymagają od klientów wypełniania formularzy know-your-customer (KYC), oferując prywatność i anonimowość, a także umożliwiają dostęp do większej liczby kryptowalut i aktywów cyfrowych. Ponadto wiele altcoinów jest dostępnych tylko na giełdach zdecentralizowanych. Jednak korzystanie z zdecentralizowane giełd jest bardziej złożone, gdyż wymaga wykorzystania portfela niepowierniczego. Do jego obsług wymagany jest specjalny klucz (seed phrase), składający się z dwunastu słów i hasła, ich brak oznacza nieodwracalną utratę posiadanych tokenów i brak możliwości ich odzyskania [McMenamin, Daza, Fitzi, O'Donoghu, 2022]. DEX wymagają od użytkownika nauki i zapoznania się z platformą i procesem, w przeciwieństwie do scentralizowanych giełd, które oferują bardziej wygodny i przyjazny dla użytkownika mechanizm [Kumar, Nikhil, Singh, 2020]. Ponadto w przypadku DEX możliwy jest jedynie obrót kryptoaktywami, płatności walutą fiat[2] nie są możliwe. W pierwszej kolejności konieczne jest więc zdeponowanie środków w walucie fiat na CEX, a następnie po dokonanym zakupie danego kryptoakytwa możliwy jest jego transfer do zdecentralizowanego portfela kryptowalutowego i wykorzystanie DEX. Zdecentralizowane giełdy są więc istotnym instrumentem dla inwestorów szukających przejścia pomiędzy dwoma kryptoaktywami. Jednak zdecentralizowane giełdy wymiany kryptowalut nie są pozbawione wad, poza koniecznością posiadania zabezpieczonego frazą nasienną niepowierniczego portfela, w przypadku zdecentralizowanych giełd mogą wystąpić trudności z brakiem płynności, oraz znalezieniem kupujących i sprzedających przy niskim wolumenie obrotu [Platt, Pierangeli, Livan, Righi, 2020]. W celu rozwiązania tego problemu powstały Automatyczne Animatory Rynku (AMM – Automated Market Makers), stanowiące innowacyjny mechanizm stosowany przez zdecentralizowane giełdy kryptowalut, rewolucjonizując sposób handlu aktywami cyfrowymi, umożliwiając użytkownikom handel bez potrzeby tradycyjnego pośrednika lub księgi zleceń dedykowanej do parowania kupujących ze sprzedającymi, jednak przy zachowaniu płynności i pokry-

[2] Waluta fiat to legalny środek płatniczy na określonym terenie, czyli np. na obszarze danego państwa.

cia dla wybranych par walutowych. AMM działają na modelach bazujących na pojęciu „cieczy", gdzie cena aktywów jest określana na podstawie zdefiniowanych algorytmów. Jedną z największych zdecentralizowanych giełd wykorzystujących AMM jest Uniswap, w uproszczonej formie DEX odwołuje się do równania $x * y = k$, gdzie x i y to ilości dwóch wymienianych aktywów stanowiących daną parę walutową, a k jest stałą. Model ten zapewnia, że całkowita wartość obu aktywów w puli pozostaje stała, gdyż zmiana wartości jednego z aktywów musi zostać skompensowana przez zwiększenie ilości tokenów drugiego aktywa, tak aby ich ostateczna suma równała się zawsze k. AMM używają puli płynności (liquidity pool), do których użytkownicy mogą wpłacać swoje aktywa, otrzymując w zamian tokeny LP (providera płynności), które reprezentują ich udział w puli. Gdy inny użytkownik chce dokonać wymiany, interakcje z pulą płynności powodują zmiany w zapasach aktywów, skutkujące automatyczną zmianą ich ceny według wskazanej formuły [Jiahua, Paruch, Cousaert, Feng, 2023].

Podsumowując, scentralizowana giełda wymiany kryptowalut jest preferowana przez niedoświadczonych inwestorów, gdyż jej obsługa jest mniej skomplikowana, bardziej przystępna i intuicyjna w obsłudze, dzięki stałej możliwości kontaktu z administratorem oraz wsparcia konsumenta. CEX stanowi pierwszy punkt wejścia dla podmiotu nieposiadającego wiedzy w zakresie obrotu kryptoaktywami. Natomiast zdecentralizowane giełdy są zazwyczaj preferowane przez doświadczonych inwestorów dzięki ich decentralizacji, niższym kosztom oraz pełnemu dostępowi do zdecentralizowanych finansów.

Charakterystyka portfeli kryptowalutowych

Kluczowe znaczenie w zakresie działania rynku kryptowalut stanowi zdefiniowanie pojęć portfela powierniczego (Custodial) i niepowierniczego (Non-custodial). Mają one kluczowe znaczenie dla charakterystyki metod przechowywania posiadanych kryptoaktywów. Różnica między portfelami powierniczymi i niepowierniczymi sprowadza się do kontroli tokenów przechowywanych w portfelu, użytkownika lub obsługi portfela.

Portfel powierniczy posiada usługę hostingu portfela, która przechowuje klucze do portfela danej kryptowaluty dla użytkownika, co oznacza, że jej posiadacz znajduje się pod nadzorem centralnej jednostki – przeważnie jest to giełda CEX, będąca administratorem portfela kryptowalutowego. Portfele giełdowe są powszechnym typem portfela i wybieranym przeważnie przez początkujących inwestorów. Giełdy w trakcie przechowywania kryptowalut wymagają stałego połączenia z internetem, w wyniku czego zabezpieczenia są bardziej podatne na zagrożenia w porównaniu z bardziej zaawansowanymi opcjami, takimi jak portfele programowe czy sprzętowe [Khan, Amjad Hussain, Muzammil, Riaz, 2019]. W portfelach niepowierniczych użytkownik ma pełną kontrolę nad swoimi tokenami, a także kluczami prywatnymi, które umożliwiają dostęp

do zgromadzonych na nich środków. Istnieją różne metody przechowywania kryptowalut na niepowierniczych nośnikach, jednak w tym artykule omówione zostaną portfele programowe i sprzętowe (hard-wallets). W tabeli 2 zaprezentowano wady i zalety portfeli giełdowych.

Tabela 2. Wady i zalety portfeli giełdowych CEX

Zalety	Wady
Darmowe w konfiguracji i zarządzaniu, użytkownicy w zależności od poziomu doświadczenia mogą uczestniczyć w obrocie kryptowalutami.	Portfele depozytowe, klucze i monety są przechowywane przez giełdę (CEX), podatne na ataki hakerskie oraz zagrożenia związane z kradzieżą lub malwersacjami finansowymi administratorów.
Portfele giełdowe umożliwiają przechowywanie, wymianę i transfery kryptowalut oraz przechowywanie waluty fiat.	Portfele te są stale połączone z internetem, zwiększając ryzyko ataków hakerskich, wymagają również spełnienia przez użytkownika wymogów KYC/AML.

Źródło: K. Chalkias, P. Chatzigiannis, J. Yan [2022].

Drugą z omawianych opcji są portfele niepowiernicze. Zaliczają się do nich portfele programowe czy sprzętowe, jednak podział ten nie stanowi wyczerpującego wyliczenia. Portfele niepowiernicze, które są zdecentralizowane i niezależne od odgórnego administratora tak jak w przypadku CEX i nie w każdym przypadku są stale połączone z internetem. Perspektywa konieczności stałego połączenia z internetem wymaga wyróżnienia portfeli gorących (hot storage) i zimnych (cold storage). Do pierwszej kategorii można zaliczyć np. portfele powiernicze typu custodial takie jak CEX lub portfele programowe, natomiast do drugiej kategorii można zaliczyć np. portfele papierowe czy sprzętowe, które zostaną dalej przeanalizowane. Portfele niepowiernicze przechowują klucze prywatne, które są ciągami liter i cyfr zapisanymi w sieci blockchain, reprezentującymi tokeny posiadanej kryptowaluty, w danej sieci [Chen You-Ping, Ju-Chun Ko, 2019]. Klucze prywatne pozwalają na wysyłanie i odbieranie kryptowalut, a także na przenoszenie kryptowalut między portfelami. Istotnym elementem omawianych portfeli niepowierniczych, czyli programowych i sprzętowych, jest ich zabezpieczenie za pomocą frazy nasiennej (seed phrase), którą jest zazwyczaj od 12 do 24 losowych słów i jest ona kluczem głównym, tożsamym z danymi wymaganymi przy logowaniu się do konta bankowego [Simplilearn.com, 2023]. Portfele programowe są podobne do portfeli giełdowych pod tym względem, że w większości wykorzystana jest gorąca pamięć masowa i są stale połączone z internetem. Nie są one jednak hostowane przez giełdę, która nie jest depozytariuszem zgromadzonych na nich środków. Aby użyć portfela programowego do handlu na giełdzie, konieczne jest podłączenie do wybranej platformy obsługującej daną sieć blockchain, której przykład może stanowić zdecentralizowana giełda

wymiany kryptowalut DEX [Canessane, Srinivasan, Abinash, Ashwini, Kumar, 2019]. Portfele programowe mogą być również hostowane na pulpicie lub aplikacji mobilnej, która nie jest połączona z giełdą. Do najpopularniejszych zdecentralizowanych portfeli kryptowalutowych zaliczają się MetaMask czy Phanthom. W tabeli 3 zaprezentowano wady i zalety portfeli programowych [Taylor, Ho-Yong Kim, Akram Zainol Ariffin, Siti Norul Huda Sheikh, 2022].

Tabela 3. Wady i zalety portfeli programowych

Zalety	Wady
Portfele programowe nie są powiernicze, co oznacza, że użytkownik posiada pełny dostęp, kontrolę nad posiadanymi jednostkami kryptowaluty.	Portfele programowe, które używają gorącej pamięci masowej mogą być podatne na pewne naruszenia bezpieczeństwa. Ponadto użytkownik ponosi pełną odpowiedzialność za posiadane klucze prywatne (seed phrase).
Większość portfeli programowych jest łatwo dostępna przy użyciu komputera lub urządzenia mobilnego przy dostępie do internetu oraz ich założenie nie wymaga nakładu finansowego.	Brak możliwości przechowywania waluty fiat.

Źródło: T. Sans, L. Ziming, K. Oh [2023].

Ostatnim z analizowanych rodzajów portfeli kryptowalutowych są portfele sprzętowe (hardware wallets), zaliczające się do grupy portfeli zimnych, czyli niewymagających stałego połączenia z internetem. Zaliczają się do nich np. Trezor [Tyler, Piscitelli, Shavrov, Baggili, 2020] czy Ledger [Gkaniatsou, Arapinis, Kiayias, 2017]. Portfele sprzętowe są fizycznymi dyskami, które wykorzystują zimną pamięć do przechowywania kluczy prywatnych dla danej kryptowaluty. Są portfelami niepowierniczymi, gdyż umożliwiają użytkownikom pełną kontrolę nad ich kluczami prywatnymi i nie wymagają zaufania od trzeciej strony. Mogą one wyglądać jak małe urządzenia podręczne, ale są zabezpieczone kodem PIN potrzebnym do uzyskania dostępu do informacji, a także opcjonalnym hasłem. Jednak kod PIN i hasło nie są jedynymi środkami bezpieczeństwa, ponieważ utworzona przez użytkownika fraza nasienna umożliwia odzyskanie danych zapisanych na dysku, nawet w przypadku jego utraty [Samer, Qais, Khalil, 2022]. W tabeli 4 zaprezentowano wady i zalety portfeli sprzętowych.

Zarówno giełdy kryptowalut, jak i portfele kryptowalutowe cechują się zróżnicowaniem względem licznych aspektów związanych z poziomem bezpieczeństwa, dostępem oraz kosztami użytkowania i przeprowadzania transakcji. Kluczową różnicą między portfelami powierniczymi, a niepowierniczymi jest fakt posiadania pełnej kontroli nad kluczami prywatnymi. Każdy rodzaj portfela ma swoje wady i zalety związane z bezpieczeństwem, wygodą i kontrolą użytkownika nad środkami. Portfele cold storage uważane są za bardziej bezpieczne ze względu na izolację od potencjalnych zagrożeń, natomiast

portfele hot storage oferują większą wygodę transakcji i zarządzania środkami. W praktyce wielu użytkowników stosuje połączenie obydwu typów przechowywania, używają „cold storage" do długoterminowego przechowywania większości środków oraz „hot storage" do codziennego użytku i mniejszych ilości środków na bieżące transakcje. Wybór odpowiedniego portfela zależy od indywidualnych potrzeb, kwoty środków przeznaczonych do przechowywania i zrozumienia związanego ryzyka. Bezpieczeństwo zawsze powinno być priorytetem przy wyborze portfela oraz metod zakupu i wymiany kryptowalut.

Tabela 4. Wady i zalety portfeli sprzętowych

Zalety	Wady
Portfele sprzętowe stanowią najbezpieczniejszą metodę przechowywania kryptowalut.	Użytkownicy muszą posiadać fizyczne urządzenie, istnieje ryzyko jego zagubienia lub kradzieży. Jednak fraza nasienna umożliwia odzyskanie danych zapisanych na dysku nawet w przypadku jego utraty.
Cena początkowa portfela sprzętowego wynosi 77 USD za Trezor i 79 USD za Ledger, co czyni je dostępnymi przy niewielkich kosztach inwestycyjnych.	Nie obsługują depozytów i transferów w postaci waluty fiat, konieczny może być wcześniejszy transfer środków na CEX w celu zakupu jednostek danej kryptowaluty.

Źródło: analiza własna na podstawie T. Fareed [2023].

Wnioski

Wyróżnia się dwa typy giełd: kryptowalutowe giełdy (CEX) i zdecentralizowane giełdy (DEX). Scentralizowane giełdy charakteryzują się centralnym zarządzaniem funduszami użytkowników, co zapewnia wygodę, ale wiąże się z ryzykiem. W przeciwieństwie do tego, giełdy zdecentralizowane działają bez centralnej administracji, oferując większą kontrolę użytkownikom, jednakże wymagając określonego poziomu doświadczenia. Kluczowe znaczenie w zakresie działania rynku kryptowalut stanowi zdefiniowanie pojęć portfela powierniczego i niepowierniczego. Główna różnica pomiędzy ww. typami portfeli występuje w zakresie kontroli tokenów. W portfelach niepowierniczych użytkownicy mają pełną kontrolę nad swoimi tokenami, które umożliwiają dostęp do zgromadzonych na nich środków. Z kolei portfele niepowiernicze, które są zdecentralizowane i niezależne od odgórnego administratora tak jak w przypadku CEX i nie w każdym przypadku są stale połączone z internetem.

Bibliografia

Barbon A., Ranaldo A. [2023], *On the Quality of Cryptocurrency Markets: Centralized Versus Decentralized Exchanges*, Cornell University, https://doi.org/10.48550/arXiv.2112.07386.

Bentov I., Ji Y., Zhang F., Breidenbach L., Daian P., Juels A. [2019], *Tesseract: Real-Time Cryptocurrency Exchange Using Trusted Hardware*, CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, November, s. 1521–1538, https://dl.acm.org/doi/abs/10.1145/3319535.3363221.

Canessane R.A., Srinivasan N., Abinash B., Ashwini S., Kumar B.M. [2019], *Decentralised Applications Using Ethereum Blockchain*, International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, s. 75–79, https://doi.org/10.1109/ICONSTEM.2019.8918887.

Chalkias K., Chatzigiannis P., Yan J. [2022], *Broken Proofs of Solvency in Blockchain Custodial Wallets and Exchanges*, Cryptology ePrint Archive, https://eprint.iacr.org/2022/043.

Chen You-Ping, Ju-Chun Ko [2019], *CryptoAR Wallet: A Blockchain Cryptocurrency Wallet Application That Uses Augmented Reality for On-Chain User Data Display*, Proceedings of the 21st International Conference on Human-Computer Interaction with Mobile Devices and Services, MobileHCI'19, New York, s. 1–5, https://doi.org/10.1145/3338286.3344386.

Essén A., Ekholm A. [2020], *Centralization vs. decentralization on the blockchain in a health information exchange context*, Digital Transformation and Public Services, s. 58–82.

Fareed T. [2023], *A Systemic Review of Payment Technologies with a Special Focus on Digital Wallets*, w: Turi A.N. (red.), *Financial Technologies and DeFi. Financial Innovation and Technology*, Springer, Cham, s. 89–97, https://doi.org/10.1007/978-3-031-17998-3_6.

Gkaniatsou A., Arapinis M., Kiayias A. [2017], *Low-Level Attacks in Bitcoin Wallets*, w: Phong Q. Nguyen, Jianying Zhou (red.), *Information Security*, „Lecture Notes in Computer Science", vol. 10599, Springer International Publishing, Cham, s. 233–253, https://doi.org/10.1007/978-3-319-69659-1_13.

Hyeji J., Sung H. Han, Ju Hwan Kim, Kimin Kwon [2021], *Usability Evaluation for Cryptocurrency Exchange*, w: Gutierrez A.M.J., Goonetilleke R.S., Robielos R.A.C. (red.), *Convergence of Ergonomics and Design*, „Advances in Intelligent Systems and Computing", vol. 1298, Springer International Publishing, Cham, s. 192–196, https://doi.org/10.1007/978-3-030-63335-6_20.

Jiahua Xu, Paruch K., Cousaert S., Feng Y. [2023], *SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols*, „ACM Computing Surveys", vol. 55(11), s. 1–50, https://doi.org/10.1145/3570639.

Kancelaria Prezesa Rady Ministrów [2024], *Projekt ustawy o kryptoaktywach*, Kancelaria Prezesa Rady Ministrów, Portal gov.pl, https://www.gov.pl/web/premier/projekt-ustawy-o-kryptoaktywach (data dostępu: 1.06.2024).

Khan A.G., Amjad Hussain Z., Muzammil H., Riaz U. [2019], *Security Of Cryptocurrency Using Hardware Wallet And QR Code*, International Conference on Innovative Computing (ICIC), Lahore, Pakistan, https://doi.org/10.1109/ICIC48496.2019.8966739.

Kumar M., Nikhil N., Singh R. [2020], *Decentralising Finance Using Decentralised Blockchain Oracles*, International Conference for Emerging Technology (INCET), Belgaum, India, s. 1–4, https://doi.org/10.1109/INCET49848.2020.9154123.

McMenamin C., Daza V., Fitzi M., O'Donoghu P. [2022], *FairTraDEX: A Decentralised Exchange Preventing Value Extraction*, ACM CCS Workshop on Decentralized Finance and Security, Association for Computing Machinery, New York, s. 39–46, https://doi.org/10.1145/3560832.3563439.

Platt M., Pierangeli F., Livan G., Righi S. [2020], *Facilitating the Decentralised Exchange of Cryptocurrencies in an Order-Driven Market*, Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, s 30–34, https://doi.org/10.1109/BRAINS49436.2020.9223286.

Qin K., Zhou L., Afonin Y., Lazzaretti L., Gervais A. [2021], *CeFi vs. DeFi – Comparing Centralized to Decentralized Finance*, Cornell University, https://doi.org/10.48550/arXiv.2106.08157.

Samer B., Qais H., Khalil Y. [2022], *Comparison of Hardware and Digital Crypto Wallets*, „Journal of Southwest Jiaotong University", vol. 57(6), http://jsju.org/index.php/journal/article/view/1414 (data dostępu: 30.05.2024).

Sans T., Ziming L., Oh K. [2023], *A Decentralized Mnemonic Backup System for Non-Custodial Cryptocurrency Wallets*, w: Jourdan G.-V., Mounier L., Adams C., Sèdes F., Garcia-Alfaro J., *Foundations and Practice of Security*, Lecture Notes in Computer Science, Springer Nature Switzerland, Cham, s. 355–370, https://doi.org/10.1007/978-3-031-30122-3_22.

Simplilearn.com [2023], *What Is Blockchain Wallet and How Does It Work?* https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-wallet (data dostępu: 30.05.2024).

Sobiecki G. [2014], *Walut światy równolegle*, „Kwartalnik Nauk o Przedsiębiorstwie", vol. 33(4).

Taylor S., Ho-Yong Kim S., Akram Zainol Ariffin K., Siti Norul Huda Sheikh A. [2022], *A Comprehensive Forensic Preservation Methodology for Crypto Wallets*, „Forensic Science International: Digital Investigation", vol. 42–43, https://doi.org/10.1016/j.fsidi.2022.301477.

Tyler T., Piscitelli M., Shavrov I., Baggili I. [2020], *Memory Foreshadow: Memory FOREnSics of HArDware CryptOcurrency Wallets – A Tool and Visualization Framework*, „Forensic Science International: Digital Investigation", vol. 33, https://doi.org/10.1016/j.fsidi.2020.301002.

UKNF [2021], *Ostrzeżenie Urzędu KNF o ryzykach związanych z nabywaniem oraz z obrotem kryptoaktywami (w tym walutami wirtualnymi oraz kryptowalutami)*, Urząd Komisji Nadzoru Finansowego, Warszawa, 12 stycznia, https://www.knf.gov.pl/knf/pl/komponenty/img/Ostrzezenie_UKNF_o_ryzykach_zwiazanych_z_nabywaniem_oraz_z_obrotem_kryptoaktywami_72241.pdf (data dostępu: 30.05.2024).

Wang Q., Rujia Li W., Qi Wang, Chen S. [2021], *Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges*, Cornell University, http://arxiv.org/abs/2105.07447.

Wang Y., Lu W., Liu M.-B., Ren R., Härdle W.K. [2024], C*ross-Exchange Crypto Risk: A High-Frequency Dynamic Network Perspective*, „International Review of Financial Analysis", vol. 94, https://doi.org/10.1016/j.irfa.2024.103246.