Jak bezpiecznie
i bez pośpiechu wejść

W ŚWIAT KRYPTOWALUT

wydanie 2

Rafał ŁAPAĆ

Redakcja i skład: Korekto.pl

Projekt okładki: Mateusz Pelc

Wydawnictwo Leniwcowate

ISBN: 978-83-966180-2-3

www.leniwcowate.pl

kontakt@leniwcowate.pl

Partnerzy: Korekto.pl i mind-it.pl

Bardzo dziękuję mojej ukochanej żonie Natalii za wsparcie przy pisaniu tej książki i mojej cudownej córeczce Nataszy za uśmiechy, które dodawały mi otuchy w czasie pracy nad tą publikacją.

Notka prawna

Treści przedstawione w tej książce są prywatnymi opiniami autora i nie stanowią rekomendacji inwestycyjnych w rozumieniu Rozporządzenia Ministra Finansów z dnia 19 października 2005 roku w sprawie informacji stanowiących rekomendacje dotyczące instrumentów finansowych, ich emitentów lub wystawców (Dz. U. z 2005 roku, nr 206, poz. 1715). Autor nie ponosi odpowiedzialności za decyzje podjęte na podstawie treści zawartych w tej książce ani za szkody poniesione w wyniku decyzji inwestycyjnych podjętych na podstawie niniejszej publikacji.

Ta książka zawiera jedynie opinie na podstawie prywatnych obserwacji i doświadczeń autora. Nie jest to w żadnym przypadku podręcznik do nauczania inwestowania w kryptowaluty, ale zbiór własnych spostrzeżeń. W tej publikacji autor nie chce i nie daje czytelnikom żadnych zapewnień, że jego poglądy będą skuteczne przy inwestowaniu. Autor chce wyłącznie podzielić się swoimi spostrzeżeniami. Autor nie składa żadnych zapewnień co do tego, że zastosowanie się przez czytelnika do informacji zawartych w tej książce zapewni korzyści finansowe i nie odpowiada za ich brak, jak i za straty wynikające z inwestycji.

Pamiętaj, inwestowanie w kryptowaluty jest obarczone bardzo dużym ryzykiem inwestycyjnym. Przy braku odpowiedniej wiedzy i doświadczenia wiąże się z ryzykiem utraty całego zainwestowanego kapitału.

Kupując tę książkę, oświadczasz, że zapoznałeś/zapoznałaś się z powyższą notką prawną i w pełni ją akceptujesz.

Spis treści

Rozdział 1
Czym są kryptowaluty i po co powstały?

Rozdział 2
Gdzie kupować i sprzedawać kryptowaluty

Rozdział 3
Bezpieczeństwo kryptowalut 91

Rozdział 4
Jak bezpiecznie inwestować

Rozdział 5
Strategie inwestycyjne

Rozdział 6
Irracjonalny rynek i PR

Rozdział 7
DeFi – czym są i jaki mają potencjał

Rozdział 8
NFT – czym jest i jak na tym zarobić

Rozdział 9
Airdrop kryptowalut

Rozdział 10
Kryptowaluty w świecie gamingu

Rozdział 11
Analiza techniczna i fundamentalna kryptowalut

Rozdział 12
Staking i pasywne generowanie dochodu

Rozdział 13
Dywersyfikacja przychodów

Rozdział 14
Jak rozliczyć podatek z kryptowalut

Rozdział 15
Gdzie szukać informacji o kryptowalutach?

Rozdział 16
Jaka jest przyszłość kryptowalut?

Słowniczek kryptopojęć

Linki polecające

Wstęp

Witam Was wszystkich serdecznie. Jeśli zdecydowaliście się przeczytać tę książkę, to oznacza, że interesują Was kryptowaluty i technologie z nimi związane. To gorący temat w ostatnich latach. Postanowiłem zatem podzielić się z Wami moimi przemyśleniami na temat krypto i pokazać Wam, jak sam inwestuję w cyfrowe aktywa.

Oczywiście nie możecie traktować tej książki jako podręcznika czy poradnika inwestowania. Nic z tych rzeczy! To po prostu zbiór moich przemyśleń i doświadczeń na temat krypto. Nie jestem żadnym doradcą inwestycyjnym. Jestem zwykłym inwestorem krypto, który nabył już dużego doświadczenia w temacie wirtualnych walut. Właśnie tym doświadczeniem chcę się z Wami podzielić. Jednak wszelkie decyzje inwestycyjne musicie podejmować już sami, pamiętając, że kryptowaluty to bardzo ryzykowne aktywa i nie należy przeznaczać na nie więcej niż 5% wartości swoich środków dedykowanych inwestycjom. Tak doradzają eksperci, a ja dodam, że lepiej nawet przeznaczyć na krypto tylko 2–3%.

O czym przeczytacie w tej książce? Zaczynam od wyjaśnienia, czym są kryptowaluty, jak powstały i w jakim celu. Oczywiście musi pojawić się tajemnicza historia ojca bitcoina, czyli niejakiego Satoshiego Nakamoto. Do dziś nie wiemy, kim jest tak naprawdę, ani czy w ogóle istnieje

jako osoba (niektórzy twierdzą, że to grupa osób). O tym jednak dokładniej przeczytacie w pierwszym rozdziale.

Drugi rozdział koncentruje się na tym, gdzie kupować i sprzedawać kryptowaluty. Opisuję zatem najważniejsze giełdy kryptowalut i ich rodzaje. Podpowiadam także, na co zwracać uwagę przy wyborze giełdy, żeby bezpieczniej inwestować. Omawiam również inne miejsca, gdzie można zdobyć kryptowalutę, jak kantory krypto, bitomaty itp.

Trzeci rozdział traktuje o bezpieczeństwie kryptowalut. Wyjaśniam tam, gdzie należy przechowywać cyfrową walutę. Omawiam portfele cyfrowe i ich rodzaje, czym się różnią od siebie, które są najbezpieczniejsze. Piszę tam również o najpopularniejszych oszustwach i zagrożeniach, jakie czyhają na posiadaczy bitcoinów oraz innych kryptowalut.

Czwarty rozdział to temat bezpiecznego inwestowania. Podpowiadam, ile pieniędzy przeznaczyć na inwestycje, żeby za bardzo nie ryzykować. Piszę, dlaczego strategia hodl jest lepsza od tradowania i czym się różnią od siebie. Zachęcam też, żeby mieć wybraną strategię, zanim zacznie się inwestować, a to ze względów psychologicznych. Kto ciekawy, koniecznie powinien zajrzeć do tego rozdziału. Wyjaśniam również, dlaczego najczęściej wszystkie kryptowaluty spadają, gdy spada bitcoin. Nie zabraknie w tym rozdziale również refleksji nad tym, czy w polskich realiach „kopanie" krypto jest w ogóle opłacalne.

W rozdziale piątym omawiam strategie inwestycyjne. Wyjaśniam, jak podzielić procentowo w portfelu inwestycyjnym różne kryptowaluty i dlaczego. Piszę, kiedy warto kupować, a kiedy sprzedawać kryptowaluty, jak rozpoznać koniec hossy. Omawiam również aplikacje, jakie pomagają przy inwestowaniu w kryptowaluty. Wspominam również o pułapce powtarzalności, w którą wpada wielu inwestorów, a przecież reguła powtarzalności może nie zadziałać (jeśli coś wydarzyło się 1000 razy, to nie oznacza, że wydarzy się 1001 raz). W tym rozdziale opisuję swój przykładowy portfel inwestycyjny.

Rozdział szósty to kilka słów o rynku kryptowalut. Zwracam uwagę, że rynek jest irracjonalny, że w krypto coraz ważniejszy jest dobry PR. Natomiast w rozdziale siódmym wyjaśniam, czym są rynki DeFi i czy mają przyszłość, jaki możemy mieć z nich pożytek. Za to rozdział ósmy koncentruje się na tokenach NFT – czym są i jak można na nich zarabiać.

W rozdziałach siódmym i ósmym piszę o NFT i DeFi. Są to dość istotne rozdziały, pomagające szerzej poznać rynek kryptowalut.

W nowym wydaniu zostały również dodane cztery nowe rozdziały, które powstały na prośbę czytelników lub z potrzeby rynku. Są to:

- Rozdział dziewiąty: Airdropy kryptowalut – W tym rozdziale omawiam, czym są airdropy, jak działają

i jak można z nich skorzystać, aby zdobyć darmowe tokeny kryptowalutowe.

- Rozdział dziesiąty: Kryptowaluty w świecie gamingu – Tutaj opisuję, jak kryptowaluty są wykorzystywane w branży gier wideo, w tym wirtualne przedmioty, tokeny i gry oparte na blockchainie.

- Rozdział jedenasty: Analiza techniczna i fundamentalna kryptowalut – Wyjaśniam podstawy analizy technicznej i fundamentalnej, które pomagają inwestorom oceniać potencjał różnych kryptowalut.

- Rozdział dwunasty: Staking i pasywne generowanie dochodu – Omawiam metody pasywnego generowania dochodu z kryptowalut, takie jak staking, który pozwala zarabiać na trzymaniu określonych tokenów.

W rozdziale czternastym piszę o tym, jak ważna jest dywersyfikacja inwestycji, że warto inwestować w różne aktywa i budować powoli, ale konsekwentnie swój majątek. Rozdział czternasty dotyczy tak ważnej kwestii, jak rozliczenie podatku od kryptowalut. Od tego tematu nie ucieknie żaden inwestor krypto, zatem trzeba się zmierzyć z tym obowiązkiem.

W rozdziale piętnastym podpowiadam, gdzie warto zdobywać informacje o kryptowalutach. Zebrałem tam różne źródła – od portali internetowych przez blogi i social media aż po książki o krypto. Mam nadzieję, że każdy z Was znajdzie tam coś dla siebie.

W ostatnim rozdziale, szesnastym, zastanawiam się, jaka jest przyszłość kryptowalut, jak mogą się rozwinąć, czy zostaną z nami na dłużej. Sprawdzam, jak na krypto mogą wpływać takie czynniki jak regulacje prawne, konkurencja tradycyjnych rynków finansowych, a wreszcie jak na kryptowaluty wpłyną Web3, *metaverse* czy sztuczna inteligencja.

Książka kończy się słowniczkiem pojęć, w którym wyjaśniam w jak najprostszy sposób najbardziej popularne słownictwo używane w świecie kryptowalut.

Rafał Łapać

LENIWCOWATE

Rozdział 3

Bezpieczeństwo kryptowalut

O oszustwach związanych z kryptowalutami już wspomniałem w poprzednim rozdziale. Ten jest poświęcony bezpieczeństwu kryptowalut, zatem chciałbym na początek rozwinąć temat oszustw kryptowalutowych i napisać o nich nieco więcej, ponieważ to będzie dobry wstęp do tego, co chcę przekazać Wam w dalszej części tego rozdziału.

Zanim jednak do tego przejdę, chcę przestrzec szczególnie początkujących inwestorów w kryptowaluty: nigdy nie gubcie z pola widzenia kwestii bezpieczeństwa. To absolutna podstawa! Nigdy nie wierzcie, jeśli ktoś Wam mówi, że coś jest zupełnie bezpieczne. Nie ufajcie bezgranicznie giełdom, dbajcie o ochronę swoich haseł, z dużą ostrożnością podchodźcie do obietnic błyskawicznych zysków z użyciem rzekomo zaawansowanych narzędzi AI, uważajcie na fałszywe platformy inwestycyjne, na podejrzanych edukatorów i mentorów, na pop-upy wykradające frazę seed, na fałszywe tokeny, a nawet na fałszywe kancelarie prawne itp. Więcej o tym możecie poczytać na stronie Cashify.eu.

Do skali oszustw z kryptowalutami, jakie zostały dokonane w 2021 roku, nie będę już wracał. Jeśli chcecie przypomnieć sobie konkretne cyferki, zajrzyjcie do poprzed-

niego rozdziału. Tutaj chciałbym, żebyście uświadomili sobie skalę zagrożenia. Naprawdę wielu złych ludzi czyha na Wasze bitcoiny i inne cyfrowe pieniądze. Niestety, tak już jest zbudowany ten świat. Na tradycyjne pieniądze, jakie macie w portfelu, też nie brakuje amatorów. Nadal przecież napada się na konwoje z pieniędzmi, na stacje benzynowe czy sklepy, żeby ukraść gotówkę. Dlaczego zatem takich napadów miałyby unikać kryptowaluty? Zgoda, nikt nie terroryzuje ofiary przedmiotem przypominającym pistolet, żeby zabrać jej bitcoiny. W cyfrowym świecie przestępstwa są dużo bardziej wyrafinowane, a złodzieje kryptowalut stosują bardziej skomplikowane i przebiegłe metody niż grożenie atrapą broni. Skoro poświęcam ten rozdział bezpieczeństwu kryptowalut, muszę Wam dokładniej opowiedzieć o tych zagrożeniach.

W poprzednim rozdziale wspominałem już o tureckiej giełdzie Thodex i o oszukanych inwestorach kryptowalutowych. Niestety, takich przykładów jest bardzo wiele. Na początek, ku przestrodze, wymienię część z nich, chociaż lista przekrętów kryptowalutowych jest naprawdę długa. Czy wiecie, że od kilku lat FBI i Europol poszukują pani o imieniu i nazwisku Ruja Ignatova? To twórczyni kryptowaluty OneCoin, którą podejrzewa się o wyłudzenie ponad 3,5 mld funtów. Mało tego, to jedna z osób najbardziej poszukiwanych w Europie. Ignatovą nazywa się nawet ironicznie królową kryptowalut. Za pomoc w jej schwytaniu można dostać nawet 5 tys. euro. Wspomniana tu Bułgarka stworzyła własną kryptowalutę, w którą ludzie ze 175 krajów zainwestowali 3,5 mld funtów. Co więcej, Ignatovą typowano nawet na następ-

czynię Marka Zuckerberga. Nagle w 2019 roku królowa kryptowalut zniknęła. Cały projekt okazał się zwykłą piramidą finansową. Okazało się, że OneCoin nigdy nie miał swojej kryptowaluty ani technologii. Pani zniknęła z kasą, a oszukani ludzie zostali. Mało?

Kolejną piramidą finansową zbudowaną na kryptowalucie był BitConnect. W jego przypadku inwestorzy stracili 2 mld dolarów, a obiecywano im stopę zwrotu na poziomie 120%. Serio? Zbyt często wyłącza się ludziom myślenie! BitConnect to miała być platforma pożyczkowa i inwestycyjna w bitcoiny. Oszuści nie żałowali pieniędzy na reklamę i marketing. Obiecywali między innymi wyjątkowy algorytm handlowy, który oczywiście nigdy nie istniał. Za to istniały wyjątkowe apetyty oszustów. Nie dość, że raz nabrali inwestorów, to byli jeszcze na tyle bezczelni, że zaraz potem uruchomili drugie oszustwo (BitConnectX). Mało?

Wspomnę zatem o największym oszustwie związanym z kopaniem kryptowalut. Chodzi mianowicie o Bitclub Network. Znowu klasyczna piramida finansowa, ale opakowana w nowe technologie. Twórcy przekrętu przekonali inwestorów, że mają sprzęt do kopania kryptowalut i w ten sposób ukradli 722 mln dolarów. Mało?

To może chcecie przeczytać o Pincoin i iFan, które ukradły inwestorom 600 mln dolarów? Mogę również wspomnieć o Plexcoin, czyli ICO, które wyłudziło 20 mln dolarów. Natomiast twórcy innego projektu o wdzięcznej nazwie Savedroid ukradli 50 mln dolarów. I tak można wymieniać długo. Oszuści potrafią nawet uruchamiać

serwisy internetowe obiecujące podwajanie bitcoinów (*bitcoin doublers*). Wystarczy przesłać im swoje krypto. Zwykle kończy się to tym, że ślad znika zarówno po tych kryptowalutach, jak i po samym serwisie. Do tego pojawia się mnóstwo ofert oszustów w mediach społecznościowych, gdzie łowią naiwnych jak ryby w sieć. Ktoś powie, że opisuję tu głównie oszukanych inwestorów, którzy chcieli wziąć udział w takim czy innym projekcie kryptowalutowym. Zgoda, problem w tym, że pieniądze można także stracić, przechowując je na kontach giełd kryptowalut, na co również można przytoczyć wiele przykładów. Nieprzypadkowo ciągle powtarzam Wam, że nie wolno trzymać środków na giełdach poza tymi, których potrzebujecie do wykonywania zaplanowanych transakcji. Oto kolejna porcja przestróg.

Czy giełda kryptowalut może upaść? To ważne pytanie, które powinni zadawać sobie wszyscy użytkownicy giełd. Więc? Tak, każda giełda może upaść. Dlatego tak często się w tym temacie powtarzam. Niestety, nie wszyscy słuchają, dlatego tracą kasę. Kolejne przykłady dla niedowiarków.

Największym upadkiem w dziejach rynku kryptowalut była plajta giełdy Mt. Gox. Ta dziwna nazwa to skrót od *Magic: The Gathering Online eXchange*, ponieważ na samym początku była to platforma wymiany kart do kolekcjonerskiej gry karcianej *Magic: The Gathering*. Ten serwis powstał jeszcze zanim ktokolwiek pomyślał o wykopaniu pierwszego bitcoina. Był rok 2006 i niejaki Jed McCaleb, dziś dość rozpoznawalna postać w świecie kryptowalut, wpadł na pomysł witryny do wymiany kart. Szybko jednak projekt został porzucony i uznany za niewypał, jednak strona mtgox.com powróciła w 2007 roku, żeby promować kolekcjonerską grę karcianą *The Far Wilds* autorstwa McCaleba. W 2010 roku Caleb dowiedział się przypadkowo o istnieniu bitcoina i koncepcja takiej waluty całkowicie go pochłonęła. Witryna Mt. Gox została reaktywowana po raz trzeci, ale już jako platforma handlowa dla bitcoina. McCaleb był zatem pierwszym, który stworzył giełdę kryptowalut z prawdziwego zdarzenia. Wiadomo: kto pierwszy, ten lepszy. W 2011 roku Mt. Gox została sprzedana francuskiemu programiście Markowi Karpelèsowi. Nowy właściciel skutecznie rozwinął giełdę, bo już w 2013 roku odpowiadała ona za 70% obrotu wszystkich bitcoinów znajdujących się w obiegu. Ciekawe jest jednak to, że gdy nowy właściciel Karpelès

zaczął robić audyt przejętej giełdy, wyszły różne „kwiatki". Okazało się na przykład, że straciła ona już środki w wyniku ataku hakerskiego i na kontach klientów brakowało 80 tys. BTC. W tamtym czasie 1 BTC odpowiadał 1 USD, więc właściciel giełdy nie bardzo przejął się stratą. Problem stawał się jednak coraz bardziej poważny, gdy cena BTC zaczęła rosnąć coraz mocniej, bo rósł jednocześnie dług w przeliczeniu na dolary. W 2011 roku doszło do następnego ataku hakerskiego, a w kolejnych latach Mt. Gox musiała borykać się z pozwami różnych instytucji oraz z oskarżeniami wysuwanymi przez Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych. W 2014 roku giełda zawiesiła działalność, a klienci nie mogli odzyskać swoich środków. Mark Karpelès wygłaszał uspokajające oświadczenia, a w tym czasie złożył wniosek o upadłość giełdy. Klienci stracili łącznie 65 mln dolarów. Wielu z nich trzymało swoje kryptowaluty tylko na tej giełdzie.

Opisałem tak obszernie upadek poprzedniej giełdy, ponieważ to była pierwsza na świecie platforma tego typu i w pewnym momencie stała się największą giełdą kryptowalut, a i tak upadła. Przestroga jest więc taka, że nawet największe giełdy nie są w 100% bezpieczne. Zawsze coś może się zdarzyć. Podobnych przykładów upadających giełd kryptowalut można znaleźć dużo więcej. Mogę wspomnieć o dwóch panach zza wschodniej granicy. Mam na myśli dwóch Rosjan: Alexandra Vinnika i Aleksieja Bilyuchenkę, którzy założyli giełdę BTC-e. Inwestorzy używali tam tradycyjnej waluty do zakupu tej cyfrowej, a do tego nie musieli się specjalnie tłumaczyć ze swojej

tożsamości. To było więc idealne miejsce do prania brudnych pieniędzy. W 2016 roku BTC-e stała się trzecią co do wielkości giełdą kryptowalut na świecie. Wkrótce zainteresowało się nią FBI. Zaczęto podejrzewać, że właśnie tam trafiły fundusze z okradzionej giełdy Mt. Gox. Klienci BTC-e wkrótce również stracili pieniądze. Tymczasem jeden z jej założycieli, Aleksiej Bilyuchenko, założył kolejną giełdę. To była Wex. Już wtedy szukał protekcji u ludzi związanych z Kremlem. Rzeczywiście ją znalazł, a z giełdą powiązali się ludzie z rosyjskich służb specjalnych. W 2018 roku handel na Wex niespodziewanie się zakończył, giełda upadła, a ludzie stracili 450 mln dolarów.

Na koniec tej części rozdziału już ostatni przykład upadającej giełdy, żeby Was nie katować dłużej tymi smutnymi przykładami. Chodzi o MyCryptoWallet z Melbourne. Została założona w 2017 roku i obsługiwała około 20 tys. klientów. Platforma radziła sobie całkiem nieźle. W końcu jednak zaczęły pojawiać się problemy. Coraz więcej osób składało skargi na MyCryptoWallet, a w 2019 roku konta giełdy zostały zablokowane po sporze z National Australia Bank. Dwa lata później giełda upadła. W ogóle 2021 rok nie był dobry dla australijskich platform kryptowalut. Kilka miesięcy przed MyCryptoWallet upadła inna australijska giełda kryptowalut – Blockchain Global Limited.

Osobiście wyznaję zasadę, że lepiej być mądrym przed szkodą niż po szkodzie. Mam nadzieję, że Wy również kierujecie się podobną filozofią. Dlatego właśnie zdecydowałem się poświęcić bezpieczeństwu osobny rozdział. Co innego bowiem stracić środki w wyniku nieudanych inwestycji (chociaż taką możliwość najlepiej zminimali-

zować), a co innego z powodu kradzieży lub upadku giełdy kryptowalut. Czy zatem można w ogóle bezpiecznie przechowywać kryptowaluty? Oczywiście, że tak i za chwilę przejdę do tej kwestii, wszystko Wam dokładnie wyjaśnię. Chcę jednak, żebyście uświadomili sobie, że aktywa kryptograficzne lub inaczej: pieniądze cyfrowe przechowuje się w nieco inny sposób niż tradycyjne banknoty. Nie dość, że kryptowaluty mają własne, specyficzne właściwości, to jeszcze żadna instytucja nie ma nad nimi takiej kontroli, jak w przypadku tradycyjnego pieniądza. To wszystko sprawia, że do kryptowalut trzeba podejść nieco inaczej. Właśnie na tym innym podejściu skoncentruję się w dalszej części tego rozdziału.

Musicie zawsze zdawać sobie sprawę z tego, że to w dużej mierze tylko od Was zależy bezpieczeństwo Waszej kryptowaluty i dokonywanych transakcji. Wszelkiej maści złodzieje, oszuści i cyberprzestępcy tylko czyhają na Wasz błąd. To Wy – nikt inny – musicie się zatroszczyć o to, żeby przez głupi błąd albo powierzenie środków nieodpowiedniej giełdzie nie stracić swojej kryptowaluty. Łatwiej bowiem pomylić się przy robieniu tradycyjnego przelewu i odzyskać wtedy pieniądze przy pomocy banku, niż pomylić się i odzyskać kryptowaluty. W przypadku cyfrowego pieniądza nie ma przecież trzeciej strony, która czuwałaby nad poprawnością operacji finansowych i pomagałaby rozwiązywać problemy z krypto. Być może w przyszłości ta kwestia się zmieni. Już podobno trwają prace nad blockchainem, który rozwiązywałby wspomniane tutaj problemy, testowane są rozwiązania typu *escrow* umożliwiające zaangażowanie w transakcje pośrednika itp.

Co z tego wszystkiego okaże się rzeczywiście przydatne i funkcjonalne, na pewno przekonamy się za kilka lat. Na razie musicie jednak pamiętać, że chociaż kryptowaluty korzystają z kryptografii i na pewno są bezpieczniejsze od zwykłej bankowości elektronicznej, to jednak one również narażone są na kradzież. To Wy sami musicie zadbać o ich bezpieczeństwo. Najważniejszym narzędziem w tym jest Wasz zdrowy rozsądek. Do tego warto pamiętać o kilku żelaznych zasadach:

- należy logować się do sieci tylko za pośrednictwem bezpiecznego Wi-Fi, najlepiej domowego. To dotyczy nie tylko dokonywania operacji na kryptowalutach, ale i w ogóle logowania się do banku;
- komputer, który używany jest do transakcji kryptowalutami lub do przechowywania cyfrowych środków, powinien być chroniony przez zaktualizowany program antywirusowy i do tego należy system regularnie skanować;
- jeśli używa się aplikacji portfela, trzeba koniecznie zabezpieczyć ją hasłem i to nie takim, które bez trudu rozszyfruje nawet słabo rozgarnięty haker (o portfelach za chwilę);
- nie zapominajmy o robieniu regularnego backupu portfela i trzymaniu kopii zapasowej poza komputerem;
- portfel z kluczami prywatnymi musi zostać ukryty w bezpiecznym miejscu, a najlepiej w kilku bezpiecznych miejscach (np. na kilku pendrive'ach);

- kryptowalutą należy handlować tylko na sprawdzonych, wiarygodnych giełdach kryptowalut, ale i tak powinno się trzymać tam jedynie minimalną ilość środków;
- lepiej unikać transakcji z kimś, kto sam się z Wami kontaktuje, jest nieznany i proponuje dokonanie transakcji za cenę o wiele niższą od rynkowej (takie okazje zawsze śmierdzą na kilometr);
- należy być bardzo ostrożnym w przypadku wymiany pozagiełdowej i dokonywać jej tylko ze sprzedawcą albo nabywcą o wysokiej reputacji (najlepiej sprawdzić ją u trzeciej strony, np. na wiarygodnym forum);
- lepiej unikać niepotrzebnego trzymania kryptowalut w serwisach transakcyjnych, a jeśli już, to włączyć dodatkową weryfikację (np. z wykorzystaniem smartfona);
- bez względu na to, czy korzystamy z różnych serwisów transakcyjnych, giełd, czy z innych platform, do każdego konta należy mieć inne hasło;
- nie wolno zapisywać haseł do serwisów finansowych w przeglądarce i trzeba pamiętać, żeby zawsze się z nich wylogowywać przy wychodzeniu;
- nie należy logować się nigdy w serwisach, które nie korzystają z szyfrowania SSL, i trzeba pamiętać o dokładnym czytaniu nazw domen (fałszywe potrafią różnić się tylko jedną literą).

Teraz przechodzę do tematu portfeli, ponieważ one odgrywają kluczową rolę w bezpiecznym przechowywaniu kryptowalut. Od razu napiszę, że każdy z Was powinien jak najszybciej zaopatrzyć się w co najmniej jeden z takich portfeli.

Ciągle powtarzam w tej książce, że nie należy przechowywać zbyt wielu środków na giełdach kryptowalut i żeby schować je do portfeli kryptowalut. Nadszedł czas, żeby wyjaśnić, czym właściwie są takie portfele. Na początek muszę jednak wyjaśnić bardzo istotną kwestię. Z czym kojarzy Wam się zwykły portfel, jaki większość z Was ma w swojej kieszeni lub torebce? To oczywiście przedmiot, do którego wkładacie banknoty i monety, mogąc je tam przechowywać i w miarę potrzeby wyjmować (np. przy dokonywaniu płatności). Cyfrowy lub nie, portfel kryptowalut jest tylko z nazwy podobny do klasycznego portfela skórzanego. Właściwie chodzi o taką samą ideę przechowywania, stąd korzystanie z określenia „portfel". I na tym właściwie podobieństwa się kończą. Do portfela kryptowalut nie włożycie przecież fizycznie bitcoina czy innej krypto, ani fizycznie jej stamtąd nie wyjmiecie. Musicie bowiem pamiętać, że ani bitcoiny, ani inne waluty cyfrowe nie opuszczają swojej sieci blockchain i nigdzie nie są fizycznie przesyłane, bez względu na to, czy to jakakolwiek giełda kryptowalut, czy właśnie portfel. Więc co to za portfel, do którego nie można włożyć kasy?

Pamiętacie, że do kryptowaluty przypisany jest określony klucz prywatny. Dzięki niemu zyskujemy dostęp do cyfrowej waluty i właśnie ona pozwala dokonywać nam róż-

nych operacji na tej kryptowalucie, czyli na przykład klucz prywatny pozwala przenieść określoną ilość kryptowaluty na inny adres w sieci danej krypto itd. Kwestia klucza prywatnego jest ważna dla naszego tematu, więc warto ją zapamiętać. Jeśli zatem znacie dany klucz prywatny, możecie korzystać dowolnie z zasobów cyfrowych, jakie są do niego przypisane. Tak to właśnie wszystko jest zorganizowane w kryptowalutach. Jak to się ma do portfeli kryptowalut?

Otóż precyzyjnie pisząc, gdy ktoś mówi o przechowywaniu kryptowalut, to w rzeczywistości ma na myśli przechowywanie kluczy prywatnych odnoszących się do tych kryptowalut. W portfelu krypto nie przechowujecie zatem żadnych kryptowalut, a jedynie (lub aż) klucze prywatne. Wspominałem już o tym w jednym z poprzednich rozdziałów, ale jeszcze przypomnę, że klucz prywatny ma

formę długiego ciągu cyfr i znaków, które są generowane losowo. Spróbujcie zapamiętać taki klucz! Życzę powodzenia! Na szczęście właśnie po to jest portfel krypto, żeby nie trzeba było zapamiętywać takich dziwnych informacji jak ciągi liczb oraz znaków. Pamięć również bywa ulotna, a byłoby głupio stracić dziesiątki lub setki tysięcy złotych, bo nie możecie sobie przypomnieć kilku cyfr i znaków. Utrata klucza prywatnego to utrata kryptowaluty. I tu wkracza na scenę portfel krypto, o którym Wam teraz dokładniej opowiem. Jesteście gotowe, leniwce? Jestem pewien, że tak! Zatem kontynuuję w temacie portfeli krypto. Kto ma hasło, ten ma władzę nad określonymi środkami w kryptowalucie. Tego hasła, czyli klucza prywatnego, trzeba pilnować jak przysłowiowego oka w głowie. Portfel kryptowalut jest więc Waszym sejfem z tym hasłem. Od razu dodam, że na rynku istnieją portfele przeznaczone dla konkretnej kryptowaluty (np. bitcoiny), ale i portfele uniwersalne. Jeśli posiadacie środki w różnych kryptowalutach, warto pomyśleć właśnie o tej ostatniej opcji, bo pozwala przechowywać tysiące aktywów. Z drugiej strony kwestia bezpieczeństwa nakazywałaby jednak każdą kryptowalutę trzymać osobno. Przychylam się do takiego poglądu, chociaż nie dajmy się zwariować! W każdym razie w portfelu nie upychacie na siłę żadnej kryptowaluty, a jest on formą dostępu do Waszych środków w różnych kryptowalutach lub w kryptowalucie jednego rodzaju.

Za chwilę przejdę do omówienia różnych rodzajów portfeli, bo nie ma jednego portfela, ale jeszcze krótko o kilku kwestiach. Po pierwsze warto sobie przypomnieć, jak w ogóle działają takie aktywa cyfrowe jak kryptowaluty.

Nie będę do tego wracał. Kto chce, może wrócić do poprzednich rozdziałów oraz odświeżyć sobie pamięć. Już trochę zacząłem pisać o funkcjonowaniu portfela kryptowalut, że chowacie tam klucze prywatne. Portfele kryptowalut mogą być w formie aplikacji, sprzętów lub w formie, nazwijmy to na razie, tradycyjnej, gdzie kluczowa jest kartka i długopis (do tego wrócę). Każdy z rodzajów tych portfeli działa nieco inaczej, ale wszystkie są tak zaprojektowane, żeby zapewnić bezpieczny dostęp do naszych cyfrowych walut. Po takim wstępie myślę, że jesteście już gotowi do dokładniejszego poznania różnych rodzajów portfeli.

Na rynku można znaleźć różne rozwiązania, które pozwalają w bezpieczny sposób przechowywać klucze prywatne kryptowalut. Takie portfele można podzielić na:

- zimne portfele (*cold wallets*) – do tego segmentu zalicza się sprzęt przechowujący klucze prywatne w trybie offline. To jest najwyższy poziom bezpieczeństwa. Za wadę można uznać wysoki koszt urządzenia;
- gorące portfele (*hot wallets*) – to aplikacje działające online, są wygodne i łatwe w użytkowaniu, ale o mniejszym poziomie bezpieczeństwa niż zimne portfele, bo połączone są z Internetem;
- fizyczne portfele – fizyczne przechowywanie kluczy prywatnych, darmowe i offline.

Na początek tylko taki ogólny podział portfeli, żebyście zyskali pogląd na omawiany tu problem. Teraz scharakteryzuję Wam dokładniej każdy z nich. Zacznijmy od

zimnych. Oczywiście to określenie przenośne, a chodzi o podkreślenie, że mają formę offline. To portfele sprzętowe (*hard wallets*) w formie bardzo małych urządzeń, często przypominających pendrive'y albo odtwarzacze MP3/MP4 (jeśli jeszcze pamiętacie, że takie coś było przed laty popularne). Takie urządzenia mają zainstalowane dedykowane oprogramowanie. Portfel sprzętowy łączy się z komputerem, przechowuje kryptowalutę. Taki rodzaj portfela może przechowywać bardzo wiele kryptowalut (niektóre dużo powyżej tysiąca), chociaż są również portfele sprzętowe o dużo skromniejszych możliwościach. Podłączacie taki portfel do komputera i generujecie adres, aby umieścić informacje o swoich aktywach w pamięci sprzętu. Gdy już to zrobicie, można dokonywać różnych operacji (np. przesyłać kryptowalutę na inny adres), które są podpisywane i szyfrowane. Wasz klucz prywatny nigdy nie opuszcza Waszego portfela sprzętowego. Wszystko jest tak skonstruowane i zabezpieczone, że nawet podłączenie urządzenia do zainfekowanego komputera nie stwarza zagrożenia, bo szyfrowanie odbywa się wewnątrz portfela. Producenci stosują różne rozwiązania, żeby zwiększyć bezpieczeństwo swoich portfeli sprzętowych. Na przykład jeden z liderów tego rynku (mam na myśli francuską firmę Ledger) montuje w swoich urządzeniach aż dwa czipy. Pierwszy to tzw. *Secure Element* i to właśnie on przechowuje wrażliwe dane kryptograficzne, do których chciałby dobrać się każdy cyberprzestępca. Jako ciekawostkę dodam, że tego rodzaju czipy są używane w kartach SIM, w kartach płatniczych, a także w niektórych smartfonach (chodzi o obsługujące Samsung Pay i Apple Pay). Wróćmy jednak do tematu.

Wspomniałem o dwóch czipach. Drugi natomiast ma ogólne zastosowanie i zajmuje się wykonywaniem różnych zadań peryferyjnych. Taki czip odpowiada więc za utrzymanie połączenia z komputerem, za sterowanie urządzeniem (np. wyświetlaczem, przyciskami) itd. Można napisać, że jest on czymś na kształt pośrednika między użytkownikiem portfela a *Secure Element*. Wykonując więc różne czynności z urządzeniem, korzystacie właśnie z czipa o zastosowaniu ogólnym. Natomiast inny czołowy producent portfeli sprzętowych, Trezor, zrezygnował z czipu *Secure Element* i bazuje tylko na czipie ogólnego zastosowania, który wykorzystuje architekturę ARM. W tym przypadku zatem jeden czip zarówno przetwarza i przechowuje zaszyfrowane dane, jak i steruje urządzeniem. Specjaliści twierdzą jednak, że Trezor bardzo dobrze zabezpieczył swój portfel. Do tej kwestii jeszcze wrócę, bo chcę Wam pokazać, że nie jest wcale tak różowo w kwestii bezpieczeństwa.

Musicie mieć świadomość, że nie każdy, kto wejdzie w posiadanie Waszego portfela sprzętowego, będzie mógł bez problemu go otworzyć i dokonać dowolnej operacji na Waszych cyfrowych aktywach. Nie trzeba się zatem bać, że zgubicie takie urządzenie lub zostanie Wam ono skradzione. Jak już wspomniałem, dane w sprzętowym portfelu są przechowywane w formie szyfrowanej. Aby zyskać do nich dostęp, konieczne jest wprowadzenie ustalonego wcześniej numeru PIN. Sama utrata portfela sprzętowego nie jest jeszcze tragedią, bo jego zawartość można odzyskać dzięki kopii bezpieczeństwa. Oczywiście trzeba ją przechowywać w jakimś

bezpiecznym miejscu. W rzeczywistości w dużej mierze (niestety, niecałej) to od Was zależy, czy Wasz portfel sprzętowy będzie przyzwoicie zabezpieczony. Wspomniałem o PIN-ie. To ważne zabezpieczenie i warto się przyłożyć do wymyślenia kodu. O PIN-ach typu „1234" nie warto nawet wspominać. Kolejna kwestia to zabezpieczenie klucza prywatnego. Nie jest łatwo dostać się do portfela osobie postronnej, ale przecież może się zdarzyć, że zapomnicie hasła. Na szczęście w takich sytuacjach z pomocą przychodzi tzw. seed. Portfele obsługują protokół BIP30. To lista 2048 słów w języku angielskim. Seed to takie hasło złożone z dwunastu przypadkowych słów po angielsku. Jeśli zgubicie swój portfel sprzętowy lub po prostu nastąpi jego awaria, odzyskacie swoje kryptowaluty dzięki seedowi. Musicie jednak przechowywać seed w bezpiecznym miejscu. Ustala się go przy pierwszym użyciu portfela. W żadnym razie nie przechowujcie seeda online. Najlepiej zrobić kilka jego kopii i przechowywać w różnych miejscach. Gdy będziecie mieli podejrzenie, że doszło do wycieku danych, utwórzcie natychmiast nowy portfel i tam przelejcie swoje środki.

Wcześniej wspomniałem o używaniu dwóch lub jednego czipu w portfelach sprzętowych, jak również o tym, że bezpieczeństwo Waszego portfela zależy w dużej mierze od Was. Niestety, nie na wszystko macie wpływ. Nie jest tak, że do portfela sprzętowego nie można się w ogóle włamać, choć poziom bezpieczeństwa takich urządzeń jest naprawdę wysoki. Natknąłem się na informacje przygotowane przez firmę Kaspersky (znany producent oprogramowania antywirusowego), z których wynika, że za-

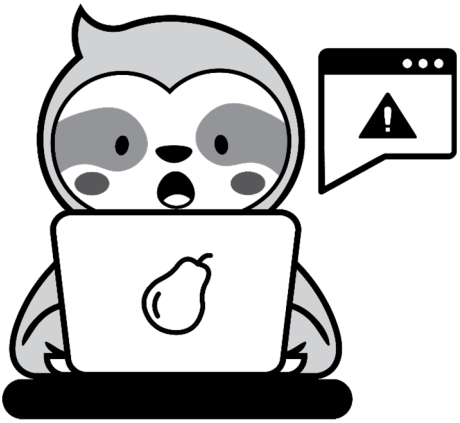
równo do portfela sprzętowego Ledger, jak i Trezor można się włamać, chociaż nie jest to łatwe. Nie będę rozpisywał się tutaj dokładnie nad metodami „włamu", bo to nie podręcznik dla hakerów. Wspomnę tylko ogólnie, że w przypadku Ledgera podmieniono oprogramowanie urządzenia na zhakowaną wersję, wpisując w określony adres pamięci określoną wartość. Inny sposób to użycie implantu sprzętowego umieszczonego w portfelu. Następnie taki implant przestępca uruchamia drogą radiową i może zdalnie wcisnąć przycisk potwierdzający. Jak na tym tle wygląda portfel Trezor z jednym czipem? Tutaj z kolei biegły haker może wykorzystać technikę manipulowania napięciem (*voltage glitching*), przełączając w ten sposób czip na „dostęp częściowy", a potem zaktualizować oprogramowanie. Podczas tego procesu w pamięci RAM tymczasowo przechowywany jest seed i można go odczytać[1]. Oczywiście te wszystkie włamania są dość wyrafinowane i trudne do przeprowadzenia, zatem portfele sprzętowe pozostają w dużej mierze bezpieczne. Jeśli chcecie się zaopatrzyć w taki portfel, kupcie go u zaufanego sprzedawcy albo bezpośrednio od producenta. W innym przypadku może istnieć podejrzenie, że ktoś manipulował przy urządzeniu. Po co ryzykować? W każdym razie portfele sprzętowe to i tak najbezpieczniejszy sposób na przechowywanie kryptowalut. Minusem może być co najwyżej konieczność podłączenia do komputera, żeby wykonać jakąś operację, ale to tylko kwestia wygody i można przeżyć.

[1] Zob. *Jak zhakować sprzętowy portfel kryptowalutowy*. Dostępne w Kaspersky.com: https://leniwcowate.pl/zrodlo/14.

Czas teraz na gorące portfele. To tak naprawdę aplikacje pełniące funkcję portfeli (*software wallets*). Jakie są ich zalety? Oczywiście macie pełną kontrolę nad swoimi aktywami cyfrowymi, takie portfele są bezpłatne, łatwe w użyciu, możecie szybko wysyłać i odbierać kryptowaluty. Niestety, są również minusy takich portfeli, a właściwie jeden, ale duży. Kryptowaluty są przechowywane online, a wiadomo, że co jest online, może stać się łupem cyberprzestępców. Ryzyko włamania nie jest duże, ale jest. Nie należy zatem trzymać w takim portfelu wszystkich aktywów. Lepiej je rozdzielić na różne portfele (warto część schować w portfelach sprzętowych). Rozróżnia się tutaj portfele na urządzenia mobilne (np. na smartfony) oraz na komputery (desktopowe). Pierwsze są dość wygodne do płacenia kryptowalutą (przyjmuje ją coraz więcej sprzedawców na świecie). Musicie jednak pamiętać, że klucze szyfrowania przechowywane są w takim przypadku w telefonie. Jeśli zgubicie zatem Wasz smartfon, możecie nie odzyskać cyfrowych aktywów. Oczywiście nie grozi to Wam, gdy przechowujecie klucze prywatne

w bezpiecznym miejscu. W takim przypadku wystarczy przywrócić portfel krypto na innym urządzeniu.

Portfele desktopowe, czyli dedykowane na komputery lub laptopy, wystarczy zainstalować na swoim urządzeniu. Macie wtedy dużą kontrolę nad swoimi cyfrowymi zasobami. Znowu jednak połączenie z Internetem to podatność na cyberataki. Przestępcy stosują różne techniki. Mogą na przykład zainfekować Wasz komputer złośliwym oprogramowaniem i wykradać w ten sposób hasła. Mogą wreszcie przejąć zdalnie komputer i wykonywać na nim różne operacje, nie wyłączając z tego użycia portfela desktopowego. Tutaj także trzeba przechowywać klucz prywatny w bezpiecznym miejscu (koniecznie offline), bo wystarczy awaria dysku twardego, żeby wydarzyła się katastrofa!



Wspomniałem jeszcze w naszym podziale o fizycznych portfelach i nie chodzi mi tutaj o żadne urządzenia. Teraz kilka słów na ten temat. Co właściwie należy rozumieć przez „fizyczny portfel kryptograficzny”?

Najczęstsza i klasyczna forma to zwykła kartka. Na takiej kartce można wydrukować klucz publiczny i klucz prywatny. Wydruk może być w formie ciągu znaków, ale i może przybierać formę kodu QR. Te dwa klucze to właściwie wszystko, czego potrzebujemy, żeby wykonywać operacje na naszych kryptowalutach. Jeśli macie formę QR, to oczywiście wystarczy takie klucze zeskanować. W przeciwnym przypadku konieczne jest mozolne, ręczne wprowadzanie znaków. Istotne jest jednak to, że to portfele offline, a więc bezpieczne, pod warunkiem że je dobrze ukryjemy, najlepiej w kilku egzemplarzach. Możemy jednak bezpiecznie przechowywać klucze właściwie bez żadnych kosztów. Innym wariantem fizycznego portfela jest zapisywanie klucza prywatnego na metalowych płytkach, zamiast na kartce. Na każdej płytce zapisywana jest tylko część klucza. Po złożeniu płytek otrzymacie kompletny ciąg klucza. Zaletą tego rozwiązania jest to, że płytka nie zniszczy się tak szybko jak papier.

Zapewne jesteście ciekawi, jakie portfele kryptowalut polecam i jakich sam używam. Zaraz podzielę się z Wami tą wiedzą. Będą to informacje płynące z doświadczenia i przetestowania naprawdę wielu rozwiązań, jeśli chodzi o portfele. Zacznę od portfeli sprzętowych. W tym segmencie polecam oczywiście lidera tego typu urządzeń, czyli francuską firmę Ledger, o której już wspominałem. To lider w aplikacjach blockchain oraz rozwiązaniach infrastruktury dla kryptowalut. Sam używam dwóch modeli: Nano S i Nano X. Przybliżę Wam te dwa urządzenia. Ten pierwszy to jeden z najpopularniejszych portfeli na rynku. To całkiem uniwersalne urządzenie, bo obsługu-

je aż 1500 kryptowalut. Jak jest zbudowany Ledger, już opisywałem (sprawa z dwoma czipami). Nano S ma ekran LCD oraz dwa przyciski do obsługi i w ogóle wygląda jak pamięć USB. Jego dużą zaletą jest to, że nie potrzebuje Internetu do podpisywania transakcji, wszystko wykonywane jest offline. Muszę też podkreślić, że to jedyny na rynku portfel sprzętowy, który ma certyfikat bezpieczeństwa ANSSI (ważna francuska agencja bezpieczeństwa cybernetycznego). Nano S ma również własny system operacyjny BOLOS, który potrafi izolować aplikacje i chroni przed atakami.

Jak używać Ledgera Nano S? Najlepiej zacząć od ściągnięcia najnowszej wersji oprogramowania Ledger Live, bo to właśnie za jego pomocą będziecie zarządzali zasobami portfela. Oprogramowanie ma także wersje mobilne na Androida i iOS. W kolejnym kroku musicie skonfigurować Nano S. Trzeba go podłączyć do komputera kabelkiem USB, a potem potwierdzić konfigurację, wciskając dwa razy przycisk na urządzeniu. Potem ustawiacie własny PIN i wykonujecie kopię zapasową (*recovery seed*). Ten Wasz klucz zapasowy (24 słowa) przepisujecie na specjalny arkusz, który został dołączony do Nano S. Pamiętajcie, kopię chowacie w bezpiecznym miejscu! Po wykonaniu *recovery seed* potwierdzacie operację, wciskając jednocześnie obydwa przyciski na obudowie portfela. W kolejnym kroku wypełniacie checklistę bezpieczeństwa. W końcu Ledger Live łączy się z Nano S i przeprowadzana jest weryfikacja portfela. Jeśli miałbym wymienić zalety Ledger Nano S, napisałbym o dobrej cenie urządzenia, możliwości obsługi wielu kryptowalut,

o prostej obsłudze, ale przede wszystkim o wysokim stopniu bezpieczeństwa tego sprzętu. Minusy? Jeśli ktoś ma za duże paluchy, to ma problem z przyciskami, które znajdują się za blisko siebie na urządzeniu. Mało wygodne jest wpisywanie klucza zapasowego z użyciem przycisków, a do tego wpisanie błędnego PIN-u trzy razy kasuje dane z portfela.

(Link afiliacyjny portfela Ledger)

Drugi model Ledgera, jakiego używam, to Nano X. W zasadzie używa się go podobnie do Nano S. Oczywiście są różnice. Nano X można łączyć z komputerem nie tylko przez USB, ale i przez Bluetooth. W ten sam sposób można się także łączyć ze smartfonem. Wystarczy zatem mieć w kieszeni telefon i Nano X, żeby w dowolnym miejscu wykonać transakcję kryptowalutą. Do tego Nano X kosztuje dwa razy tyle, co Nano S. Na tym pierwszym można zainstalować 100 aplikacji, a na Nano S – 6 (wystarczy jednak odinstalować nieużywaną, a potem w razie potrzeby znowu ją zainstalować, więc faktycznie dosta-

jemy więcej możliwości niż tylko wspomnianych 6 aplikacji). Nano X ma większą baterię (1000 mAh) i większy wyświetlacz. Standardy bezpieczeństwa są takie same w obydwu portfelach. Przy okazji dodam, że warto także korzystać z portfela sprzętowego Trezora, chociaż osobiście jeszcze go nie używam. Kiedyś na pewno się skuszę.

Z portfeli przeglądarkowych używam MetaMask. Jego dużą zaletą jest możliwość łączenia się ze zdecentralizowanymi giełdami jak Uniswap, Panakae, 1inch itp. MetaMask działa jako rozszerzenie przeglądarki (obsługuje wszystkie najpopularniejsze), co pozwala na łatwy dostęp do aplikacji. Wystarczy ją zainstalować. Portfel ten pozwala dokonywać transakcji na adresy ethereum, a do tego można przechowywać tokeny ERC-20 i ERC-721. MetaMask pozwala także zainstalować inne blockchainy (np. Binance Smart Chain, który jest podobny w strukturze do ethereum). Przy pierwszym uruchomieniu trzeba ustawić hasło oraz frazę zapasową (*seed phrase*). Poza użytkownikiem nikt nie ma tu dostępu do jego aktywów cyfrowych.

Jak założyć i używać MetaMask? Wbrew pozorom nie jest to wcale skomplikowane. Zacznijmy od procesu zakładania tego portfela. Cały proces można sprowadzić do poniższych punktów.

1. **Wejdźcie na stronę MetaMask** – pierwszym krokiem jest odwiedzenie oficjalnej strony MetaMask. Upewnijcie się, że witryna, na której się znajdujecie, jest autentyczną stroną projektu, sprawdzając URL – powi-

nien zaczynać się od „https://metamask.io". Fałszywe strony (phishingowe) mogą naśladować oryginalną stronę, aby wykraść Wasze dane. Kliknięcie „Pobierz" przekieruje Was do wyboru odpowiedniej wersji rozszerzenia w zależności od przeglądarki internetowej, jakiej używacie.

2. **Zainstalujcie rozszerzenie MetaMask w przeglądarce internetowej** – po wybraniu odpowiedniej wersji dla swojej przeglądarki (np. Chrome, Firefox, Brave, Edge lub Opera) zostaniecie przekierowani do oficjalnego sklepu z rozszerzeniami przeglądarki, gdzie możecie zainstalować MetaMask. Postępujcie zgodnie z instrukcjami instalacji, które zazwyczaj obejmują kliknięcie przycisku „Dodaj do przeglądarki" lub „Zainstaluj".

3. **Zaakceptujcie regulamin i stwórzcie nowy portfel** – po zainstalowaniu MetaMask otwórzcie rozszerzenie w Waszej przeglądarce i przejdźcie przez proces powitalny. Będziecie musieli zaakceptować regulamin usługi, co jest standardowym krokiem podczas tworzenia nowego konta. Po akceptacji warunków wybierzcie opcję „Utwórz nowy portfel", aby rozpocząć proces tworzenia Waszego portfela kryptowalutowego.

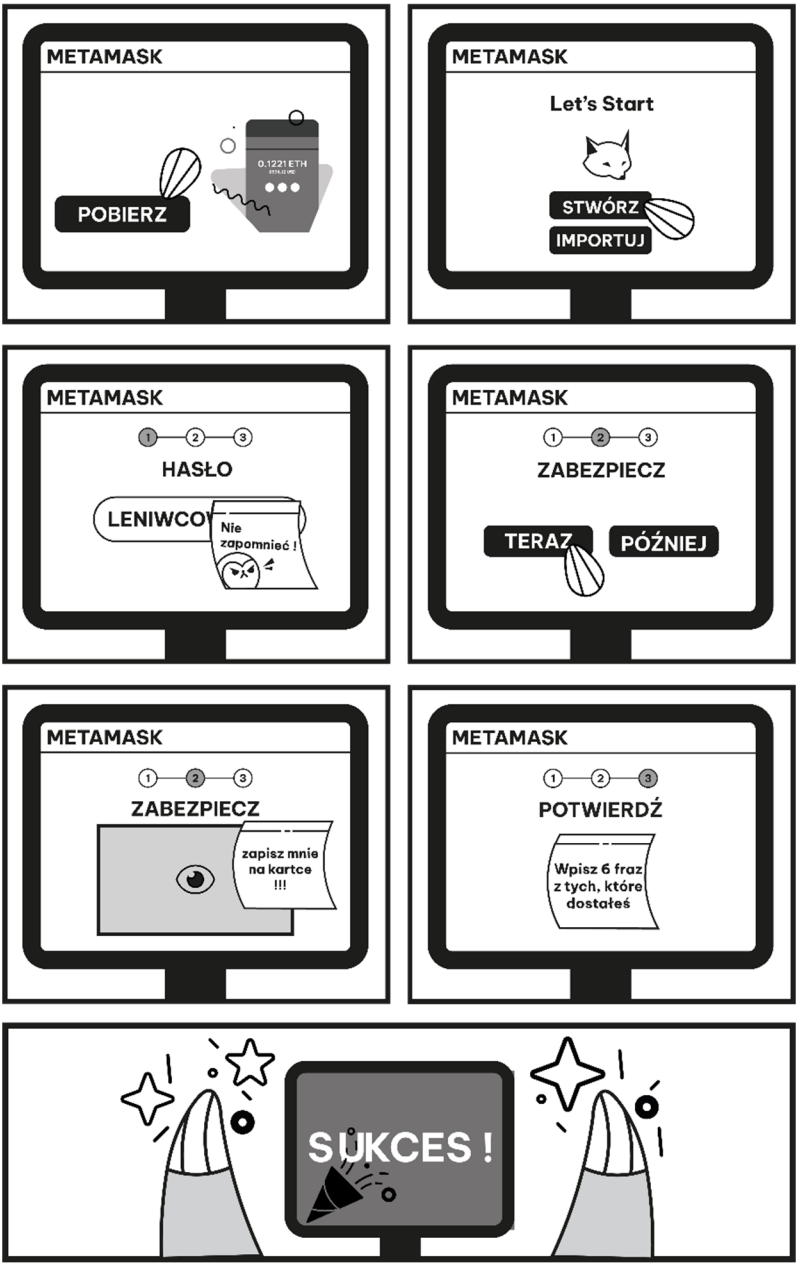
4. **Wyraźcie zgody (opcjonalnie)** – MetaMask może prosić o zgodę na gromadzenie i wysyłanie anonimowych danych statystycznych do poprawy swoich usług. To całkowicie opcjonalne i możecie zdecydować, czy chcecie udostępnić te informacje. Niezależnie od Waszej decyzji nie wpływa to na działanie portfela.

5. **Utwórzcie hasło do portfela i pamiętajcie, że jest ono nie do odzyskania** – podczas procesu tworzenia nowego portfela zostaniecie poproszeni o utworzenie silnego hasła. Pamiętajcie, że hasło to jest kluczowe do dostępu do Waszego portfela w przeglądarce i nie może być odzyskane, jeśli je zapomnicie. Zapiszcie je w bezpiecznym miejscu, najlepiej poza komputerem.

6. **Zabezpieczcie swój portfel, zapisując frazę odzyskiwania** – po utworzeniu hasła MetaMask wygeneruje dla Was „frazę odzyskiwania", która składa się z 12 losowych słów. To najważniejszy element bezpieczeństwa Waszego portfela, ponieważ umożliwia odzyskanie dostępu do Waszych funduszy w przypadku utraty hasła.

7. **Przechowujcie frazę odzyskiwania bezpiecznie i poza elektronicznymi nośnikami danych** – zapiszcie swoją frazę odzyskiwania na papierze i przechowujcie w bezpiecznym, prywatnym miejscu. Unikajcie przechowywania frazy odzyskiwania w formie elektronicznej (np. na komputerze lub wchmurze), ponieważ może to zwiększyć ryzyko kradzieży przez hakerów.

8. **Przejdźcie przez proces potwierdzenia frazy odzyskiwania** – w ostatnim kroku MetaMask poprosi Was o potwierdzenie frazy odzyskiwania – wybierzcie słowa we właściwej kolejności. To krok weryfikujący, czy prawidłowo zanotowaliście i zrozumieliście swoją frazę odzyskiwania. Dokładne potwierdzenie frazy gwarantuje, że w razie konieczności będziecie mogli odzyskać dostęp do Waszego portfela.


METAMASK
POBIERZ
0.1221 ETH
METAMASK
Let's Start
STWÓRZ
IMPORTUJ
METAMASK
1 2 3
HASŁO
LENIWCO
Nie zapomnieć !
METAMASK
1 2 3
ZABEZPIECZ
TERAZ
PÓŹNIEJ
METAMASK
1 2 3
ZABEZPIECZ
zapisz mnie na kartce !!!
METAMASK
1 2 3
POTWIERDŹ
Wpisz 6 fraz z tych, które dostałeś
SUKCES !

9. **Jak używać portfela MetaMask?** To również nie jest wcale skomplikowane. Wyjaśnię Wam to na trzech przykładach.

    1) Kupowanie kryptowalut na giełdzie zcentralizowanej za pomocą MetaMask:

        — zarejestrujcie się na giełdzie zcentralizowanej, takiej jak Binance lub Coinbase. Może być wymagana weryfikacja konta;

        — dokonajcie zakupu wybranej kryptowaluty, używając środków fiat lub innych dostępnych opcji płatności;

        — prześlijcie zakupione kryptowaluty na Wasz adres w MetaMask, kopiując własny adres publiczny z MetaMask i używając go przy wypłacie środków z giełdy.

    2) Kupowanie kryptowalut w kantorze kryptowalut Cashify za pomocą MetaMask:

        – odwiedźcie lokalny kantor Cashify lub umówcie się na spotkanie;

        – zróbcie transakcję bezpośrednio z przedstawicielem Cashify, wybierając kryptowalutę, którą chcecie kupić;

        – podajcie swój adres z MetaMask, na który mają być przesłane kryptowaluty.

3) Kupowanie kryptowalut bezpośrednio w portfelu MetaMask:

   – otwórzcie MetaMask i wybierzcie opcję „Kup” lub „Buy & Sell”;

   – skorzystajcie z integracji MetaMask z platformami umożliwiającymi zakup kryptowalut, np. przez karty płatnicze;

   – postępujcie zgodnie z instrukcjami na ekranie, aby zakończyć transakcję i mieć środki bezpośrednio w MetaMask.

Pamiętajcie, aby zawsze dokładnie sprawdzać adresy i być świadomymi opłat transakcyjnych podczas przeprowadzania zakupów oraz transferów.

Dodam jeszcze tylko, że interakcja z DeFi lub smart kontraktem wymaga połączenia z portfelem MetaMask. Taką opcję na pewno znajdziecie na platformie, którą chcecie podłączyć do MetaMask. W przypadku tego portfela, chociaż jest online, klucz prywatny jest przechowywany u Was, gdy na przykład w przypadku giełdy przechowuje go serwer giełdy. Dostrzegacie różnicę w bezpieczeństwie?

Używam także mobilnego portfela BlueWallet, który działa na platformie iOS oraz Android i obsługuje protokół Lightning Network. Tak, wyjaśniam. To architektura sieci blockchain, która jest dedykowana mikropłatnościom. Dzięki temu protokołowi można wykonywać błyskawiczne transfery z udziałem kanałów transakcyjnych

funkcjonujących poza siecią bitcoin. W każdym razie BlueWallet to jeden z lepszych portfeli mobilnych bitcoina, a do tego jest bardzo łatwy w obsłudze. Portfel działa na oprogramowaniu *open source*. Backup portfela można wykonywać za pomocą kodu QR lub adresu URL.

Możecie także zwrócić uwagę na portfele dedykowane konkretnym projektom. Jako przykład mogę podać Cardano (np. Eternl, Nami, Flint, Yoroi) lub Deadalus (niezbyt dobry dla nowicjusza). W pierwszym przypadku macie platformę do zawierania smart kontraktów opartych na ADA. Za pomocą portfela Cardano można na przykład przesyłać tokeny między różnymi portfelami. Także Deadalus jest dedykowany kryptowalucie ADA, a do tego jest darmowy, prosty w obsłudze i dość bezpieczny, jak na darmowe narzędzie. Jednak najlepsze rozwiązanie to zabezpieczać portfele softwarowe portfelem sprzętowym. To pozwala zyskać większą funkcjonalność bez utraty bezpieczeństwa. Weźcie pod uwagę taki mariaż.

Portfeli krypto jest naprawdę mnóstwo. Wymieniłem i krótko opisałem tylko te, których używam, co nie znaczy, że nie ma również innych dobrych rozwiązań. Z czasem zaczniecie sami testować różne portfele. Proponuję Wam jednak zacząć od tych, które opisałem. Teraz krótko o tym, na co zwrócić uwagę, wybierając portfel kryptowalut. Najważniejsze kryteria to:

- szyfrowanie i kwestie bezpieczeństwa – to kluczowy temat, warto poczytać opinie o wybranym portfelu;
- intuicyjność – portfel powinien być łatwy w użytkowaniu;

- dostępne funkcje – czy są tylko podstawowe usługi, czy coś więcej;
- wsparcie techniczne – przydaje się, gdy pojawia się problem z portfelem, co może się przytrafić każdemu;
- aktualizacje – warto zwrócić uwagę, czy portfel jest rozwijany i pojawiają się aktualizacje oprogramowania.

Na koniec szybkie przypomnienie najważniejszych zasad dotyczących przechowywania kryptowalut:

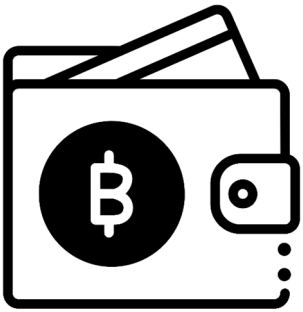
- większość aktywów cyfrowych trzymajcie w portfelu sprzętowym, a najlepiej w kilku portfelach;
- w gorących portfelach trzymajcie niewielką ilość kryptowalut – tyle, ile jest potrzebne do transakcji;
- jeśli używacie portfeli kryptograficznych, zapisujcie seedy lub klucze na kartkach albo metalowych płytkach;
- dane do odzyskiwania dostępu do portfeli trzymajcie w takich miejscach, do których tylko Wy macie dostęp;
- nie udostępniajcie nikomu kluczy prywatnych ani seedów, nie trzymajcie ich na komputerze;
- przeznaczcie jeden komputer lub laptop do robienia transakcji z wykorzystaniem portfela i nic więcej na nim nie róbcie (szczególnie nie zaglądajcie na podejrzane strony z miłymi paniami w pełnej krasie);
- i powtórzę po raz tysięczny: nie trzymajcie dużych kwot na giełdach kryptowalut!

Zapamiętaj!

- W przeszłości wielu inwestorów straciło mnóstwo pieniędzy z powodu nieuczciwych właścicieli giełd kryptowalut.
- Giełda kryptowalut może upaść, co kończy się utratą aktywów cyfrowych.
- Na giełdzie należy przechowywać tylko niewielką część kryptowalut, potrzebną do przeprowadzania transakcji.
- Nawet największe giełdy nie są w 100% bezpieczne.
- Tylko od Was zależy bezpieczeństwo Waszej kryptowaluty i dokonywanych transakcji.
- W portfelu krypto nie przechowujecie żadnych kryptowalut, a jedynie klucze prywatne.
- Klucza prywatnego trzeba pilnować jak przysłowiowego oka w głowie.
- Na rynku istnieją portfele przeznaczone dla konkretnej kryptowaluty (np. bitcoiny), ale i portfele uniwersalne.
- Portfele dzielą się na sprzętowe (zimne), aplikacje (gorące) i fizyczne (np. kartka z kluczem prywatnym).
- Seed to takie hasło złożone z dwunastu przypadkowych słów po angielsku. Jeśli zgubicie swój

portfel sprzętowy lub po prostu nastąpi jego awaria, odzyskacie swoje kryptowaluty dzięki seedowi.

- Portfele gorące dzielą się na mobilne i desktopowe.
- Najważniejsze kryteria wyboru portfela kryptowalut: bezpieczeństwo, intuicyjność obsługi, dostępne funkcje, wsparcie techniczne, aktualizacje.



LENIWCOWATE

Drogi Czytelniku

Dziękuję, że przeznaczyłeś swój czas na przeczytanie trzeciego rozdziału mojej książki „Jak bezpiecznie i bez pośpiechu wejść w świat kryptowalut – wydanie 2". Mam nadzieję, że zawarte tutaj informacje były dla Ciebie wartościowe i pomocne.

Jeżeli chcesz kontynuować swoją przygodę z kryptowalutami i zgłębić temat jeszcze bardziej, serdecznie zapraszam do zakupu pełnej wersji książki na mojej stronie internetowej.

Kupując bezpośrednio u mnie, masz gwarancję najniższej ceny oraz dostęp do ekskluzywnych materiałów dodatkowych, które pomogą Ci jeszcze lepiej zrozumieć rynek kryptowalut.

Odwiedź https://**leniwcowate.pl**/
i dołącz do grona świadomych inwestorów już dziś.

Z serdecznymi pozdrowieniami,

Rafał Łapać

O KSIĄŻCE

Chciałbyś w końcu dowiedzieć się, czym są kryptowaluty i na czym polega ich technologia? Ta książka jest właśnie dla Ciebie! Jesteś leniwcem, bo szukasz dobrego sposobu na zainwestowanie pieniędzy bez nieustannego zawracania sobie tym głowy? Ta książka jest właśnie dla Ciebie! Szukasz dobrej strategii inwestowania w kryptowaluty? Musisz koniecznie przeczytać tę książkę!

To wyjątkowa pozycja wydawnicza: nie dość, że w prosty sposób wyjaśnia zawiłości rynku kryptowalut, to jeszcze z pozycji praktyka pokazuje, jakie strategie bywają najskuteczniejsze. Z tej książki dowiesz się także, jaka może być przyszłość kryptowalut i technologii z nimi związanych. To kompletny przewodnik po świecie kryptowalut napisany przez człowieka, który od lat inwestuje w krypto i doskonale zna tajniki tego rynku. Dzięki tej książce:

- dowiesz się w końcu, czym naprawdę są kryptowaluty
- przekonasz się, jaki jest potencjał krypto
- zrozumiesz, jak działa rynek kryptowalut
- poznasz nowe możliwości finansowe
- zyskasz wiedzę, aby inwestować mądrze

Idealny poradnik dla początkujących i tych, którzy nie chcą poświęcać całego dnia na swoje inwestycje. Nie pozwól, żeby inwestycje w krypto Cię pochłonęły! Panuj nad nimi, unikaj pułapek inwestycyjnych i bądź skuteczny, a wolny czas poświęcaj rodzinie lub swojej pasji! To właśnie mądre inwestowanie dla leniwców! Dzięki tej książce wejdziesz w świat kryptowalut bezpiecznie, z solidną wiedzą.

Z zamiłowania jestem inwestorem na giełdzie kryptowalut. Zawodowo jestem przedsiębiorcą.

Od 2015 roku samodzielnie zdobywam doświadczenie w świecie kryptowalut. Od ponad 10 lat inwestuję na rynkach tradycyjnych w akcje, surowce, metale i od ponad 8 lat inwestuję w nieruchomości.

Wiem, w jak trudnych czasach żyjemy i jak z tego powodu ważna jest dywersyfikacja majątku.

Rafał Łapać

Sponsor: cashify – KRYPTOWALUTY I METALE SZLACHETNE

Patroni: NamZalezy.pl, Mike Satoshi, Kryptoekipa, crypto-anonym.pl, Comparic, JPK Traders, FOREX CLUB, Finansowa Flotka, FXMAG.PL

ISBN 978-83-966180-2-3

wydawnictwo LENIWCOWATE
www.leniwcowate.pl

Ocena: 5.0 / 5 allegro Ocena: 8.7 / 10 na lubimyczytac.pl