datowników z omawianego okresu widoczne są na il. 2-3.

il. 1. Przesyłka sądowa (zwrotne poświadczenie odbioru) nadana 21.01.1946 – 14 przez Sąd Grodzki w Czarnkowie, opłacona znaczkiem urzędowym. Polski datownik międzywojenny, dwuobrączkowy z poprzeczką, z arabskimi cyframi miesiąca, wyróżnik „d" oraz druk sądowy, również z okresu przedwojennego, o czym świadczy rubryka „dnia…193…r." Stosowane w obrocie pocztowym po 1945 r.

il. 2. Polski datownik międzywojenny (Czarnków 15.03.1946), dwuobrączkowy z poprzeczką, z arabskimi cyframi miesiąca, wyróżnik „b"; znaczek Fi. 381 o nominale 3 zł – opłata za list o wadze do 20 g.

*il. 3. Przesyłka sądowa (zwrotne poświadczenie odbioru) nadana 2.10.1947 – 14 przez Wydział Zamiejscowy w Trzciance Sądu Okręgowego w Gorzowie n/ W. Polski datownik powojenny, jednoobrączkowy z rzymskimi cyframi miesiąca, wyróżnik „*aa*" oraz datownik Ag Sarbia potwierdzający wykonanie usługi; polski międzywojenny, dwuobrączkowy z poprzeczką (data nieczytelna). Dokument sądowy wykonany pismem maszynowym na fragmencie poniemieckiego druku.*

1. Łęcki W., Województwo pilskie, Warszawa-Poznań, 1982.
2. Jakubik J. Placówki pocztowe Poczty Polskiej 1944-1948, Warszawa, 2022.

Ciąg dalszy z (1) w Filatel.pl nr 8/2025 s. 589-591.

Bartłomiej Fedorczyk, Grzegorz Lech

Dobre praktyki kryptofilatelistyki (2)

W poprzednim numerze Filatel.pl [1] omówiono zasadę działania podstawowego narzędzia dla kryptofilatelisty – portfela kryptowalutowego, a także zdefiniowano dwa typy portfela *cold wallet* oraz *hot* wallet. W niniejszym opracowaniu opisane zostaną praktyczne aspekty zakładania swojego pierwszego portfela, gdzie postaramy się przeprowadzić nowego użytkownika tej technologii przez cały proces, aby był on zrozumiały i bezpieczny.

Pierwszym pytaniem, na które każdy kryptofilatelista powinien sobie odpowiedzieć jest to, jaki typ portfela jest najlepszy. Pominiemy tutaj sympatię do konkretnych rozwiązań, a skupimy się w możliwie jak najbardziej obiektywny sposób na ich bezpieczeństwie. Decyzję ostatecznie pozostawiamy Szanownym Czytelnikom, które rozwiązanie jest dla nich optymalne. Jeśli piszemy o bezpieczeństwie systemów kryptograficznych, to bezsprzecznie są one bardzo bezpieczne, a złamanie szyfru jest praktycznie niemożliwe. Niestety, nawet w świecie kryptografii kradzieże się zdarzały i zapewne będą się jeszcze zdarzać wiele razy. Trzeba w tym momencie zauważyć, że najsłabszym ogniwem tego systemu zawsze jest użytkownik, popełniający narażający go na niebezpieczeństwo błąd, który bezlitośnie wykorzystują złodzieje.

Z uwagi na powyższe, decydując się na wybór *cold wallet* lub *hot wallet* należy szczerze odpowiedzieć sobie na pytanie o poziom własnych kompetencji cyfrowych i wiedzy o cyberbezpieczeństwie. Polecamy wykonać test

https://quiz.sekurak.pl/. Trzeba mieć świadomość mechanizmów działania rozmaitych oszustw internetowych. To zagadnienie jest bardzo obszerne, więc poświęcimy mu osobne opracowanie w kolejnych numerach Filatel.pl.

Zatem rozwiązanie *hot wallet* jest darmowym narzędziem do obsługi posiadanej kolekcji kryptoznaczków, natomiast użytkownik musi mieć wysoki poziom kompetencji cyfrowych i bardzo dbać o bezpieczeństwo swojego komputera. W naszej społeczności kryptofilatelistów zdarzył się jeden przypadek, gdzie kontrola nad kontem pod *hot wallet* została przejęta od użytkownika, który posiadał zainstalowane na swoim komputerze płatne oprogramowanie antywirusowe. Na szczęście straty nie były duże, bo na tym koncie użytkownik przechowywał tylko niewielką część swojej kolekcji.

Rozwiązanie *cold wallet* wymaga zakupienia odpowiedniego urządzenia, którego koszt wynosi od kilkuset złotych wzwyż. To rozwiązanie zdecydowanie wybacza więcej błędów użytkownikowi, bo przejęcie kontroli nad kontem z poziomu komputera użytkownika jest zadaniem niezwykle trudnym, a atak musi być wycelowany w urządzenie *hot wallet*. Autoryzacja wykonywanej transakcji odbywa się poprzez naciśnięcie fizycznych przycisków na urządzeniu. Bezpieczeństwo tego portfela zależy od tego, w jaki sposób użytkownik zabezpieczy swoją frazę mnemoniczną przed dostępem osób niepowołanych. Zatem w sytuacji, gdy użytkownik dla przykładu przechowuje swoją frazę mnemoniczną na swoim koncie mailowym, to bezpieczeństwo jego kolekcji opiera się na mocy jego hasła do skrzynki mailowej. Można łatwo sprawdzić, czy dany adres mailowy w przeszłości stał się celem ataku i jego dane dostępowe „wyciekły" na stronie https://haveibeenpwned.com/. W sytuacji, gdy wskazany serwis potwierdza kradzież danych naszego konta zalecamy niezwłoczną zmianę hasła.

Przejdźmy zatem do omówienia sposobu zakładania adresu przy użyciu narzędzia typu *hot wallet*. Na rynku istnieje obecnie bardzo dużo aplikacji będących cyfrowymi portfelami, jednak z naszej praktyki konkretne dwa wyróżniają się na tle pozostałych, a są to: 1) MetaMask (https://metamask.io/), 2) Rabby (https://rabby.io/). Wymagają one zainstalowania rozszerzenia w przeglądarce internetowej. Z naszego doświadczenia najlepiej współpracują z nimi przeglądarki Google Chrome oraz Brave, natomiast Mozilla Firefox generuje niekiedy błędy. Należy pobrać oficjalne rozszerzenie z jednej z powyższych stron i dodać je do swojej przeglądarki internetowej. Po wybraniu „create new account" zostaniemy poproszeni o zdefiniowanie hasła do odblokowania portfela. Tym hasłem logujemy się do rozszerzenia portfela w przeglądarce internetowej przy każdym nowym uruchomieniu przeglądarki internetowej lub po zablokowaniu portfela na żądanie. Stanowi ono jedyne zabezpieczenie przed dostępem osób niepowołanych do portfela. W kolejnym kroku możemy zostać poproszeni o rozwiązanie krótkiego testu rozumienia zasady działania portfela. Następnie przechodzimy do wygenerowania frazy mnemonicznej. Algorytm generuje entropowo 12 słów ze słownika BIP-39 [2], które należy sobie przepisać na kartkę. Opcjonalnie możemy zostać zapytani w kolejnym kroku o podanie wyrywkowo słów tej frazy mnemonicznej lub o ich ułożenie w odpowiedniej kolejności. Ten mały test ma na celu wymuszenie na użytkowniku zapamiętania lub zapisania frazy mnemonicznej, ponieważ w przypadku utraty dostępu do portfela można odzyskać do niego dostęp poprzez podanie wszystkich słów frazy mnemonicznej. Po zakończeniu procedury portfel kryptowalutowy jest skonfigurowany i gotowy do użycia. Wyświetla się adres publiczny portfela, który został przypisany do frazy mnemonicznej. Klucz prywatny jest już zapisany w pamięci *hot wallet* i jest automatycznie podawany przy podpisywaniu transakcji na sieci *blockchain*. Zapraszamy do filmów instruktażowych, które wizualizują cały proces dla obu tych portfeli MetaMask oraz Rabby [3].

W kolejnym akapicie opiszemy czynności, jakie trzeba wykonać przy konfiguracji portfela sprzętowego *cold wallet*. Tego typu rozwiązania są produkowane m.in. przez markę Ledger. Dostępnych jest kilka rodzajów urządzeń w zależności od zasobności portfela użytkownika. Do zastosowań kryptofilatelistycznych w zupełności wystarczają modele Ledger Nano S plus lub Ledger Nano X. Urządzenia te należy sprowadzać z zagranicy przez oficjalną stronę producenta https://www.ledger.com/. Urządzenia są dostępne również w polskich sklepach internetowych, jednak należy się tu kierować zasadą ograniczonego zaufania, gdyż istnieje prawdopodobieństwo, że kupując od pośrednika trafimy na modyfikowane urządzenie, które nie będzie bezpieczne. Zamówione urządzenie powinno być oryginalnie zapakowane

i zupełnie nieskonfigurowane, to znaczy bez zdefiniowanej frazy mnemonicznej. Pierwsze uruchomienie urządzenia oraz ustawienie w nim frazy mnemonicznej jest przywilejem użytkownika urządzenia i gwarantuje pełnię bezpieczeństwa. Portfel sprzętowy podłącza się dołączonym do zestawu kablem USB do komputera. Na komputerze instaluje się aplikację Ledger Live do zarządzania portfelem sprzętowym. Na stronie producenta istnieje procedura sprawdzenia oryginalności posiadanego urządzenia. Gdy nic nie budzi wątpliwości, można przystąpić do wygenerowania frazy mnemonicznej. Urządzenie po pierwszym uruchomieniu prosi o zdefiniowanie kodu PIN od 4 do 8 cyfr. Będzie to służyło do odblokowywania urządzenia po jego ponownym uruchomieniu. W kolejnym etapie Ledger wyświetli pojedynczo każde z 24 słów frazy mnemonicznej, które należy sobie spisać. Po zakończeniu tego kroku zostaniemy poproszeni o przypisanie słów naszej frazy mnemonicznej w odpowiedniej kolejności w celu sprawdzenia poprawności jej zapisania. Po zakończeniu tych czynności mamy do dyspozycji adres publiczny portfela, który jest przypisany do stworzonej frazy mnemonicznej. Całość procesu przedstawiono na filmie instruktażowym [4].

Bardzo pomocne jest skorzystanie z połączenia wszechstronności aplikacji *hot wallet* z bezpieczeństwem klucza prywatnego *cold wallet*. Można tak skonfigurować oba narzędzia, że do interakcji własnego portfela kryptowalutowego z wszelkimi konsolami na stronach internetowych można wykorzystywać aplikację MetaMask lub Rabby, co jest bardzo wygodne dla użytkownika. Natomiast wszelkie tak wywołane transakcje (MetaMask, Rabby) autoryzuje się podłączając portfel sprzętowy (Ledger). Takie połączenie pozwala zachować prostotę obsługi operacji dokonywanych na kolekcji kryptofilatelistycznej z bezpieczeństwem klucza prywatnego, który mimo sparowania urządzenia Ledger z aplikacją MetaMask lub Rabby, dalej przechowywany jest w pamięci portfela sprzętowego i jest w całości *offline*. Film instruktażowy parowania portfela sprzętowego z aplikacjami MetaMask [5] oraz Rabby [6] zostały zdeponowane na stronie Polskiego Związku Kryptofilatelistów.

Stosując powyższe instrukcje można bezpiecznie założyć swój pierwszy adres publiczny, który posłuży do deponowania na jego koncie NFT kryptoznaczków i budowę swojej kolekcji kryptofilatelistycznej. W ten sposób adres publiczny jest trwale połączony z użytkownikiem, a NFT zdeponowane na adresie publicznym użytkownika są niepodważalnym dowodem posiadania danego waloru w swojej kolekcji. Fakt ten zostanie odnotowany na sieci *blockchain* oraz na stałe zostanie zapisany w rejestrze rozproszonym [1]. Ze względu na prowadzone wymiany oraz transakcje kupna-sprzedaży, NFT może zmieniać swoich właścicieli. Historia wszystkich transakcji, a tym samym następnych posiadaczy waloru, pozostaje w metryce danego NFT na zawsze, nie ma możliwości jej usunięcia. Dzięki temu możemy prześledzić "cyfrową drogę", jaką przebył walor oraz potwierdzić jego tożsamość, sprawdzając adres źródłowy - czyli oryginalnego twórcę/właściciela danego NFT. Ta cecha będzie nabierać wartości z czasem, bo gwarantuje łatwe rozróżnianie oryginalnych walorów od tych podrobionych.

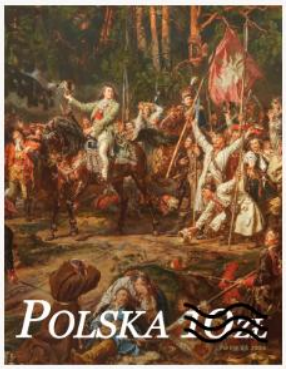
W kolejnej części dobrych praktyk kryptofilatelistyki omówione zostaną aspekty zasilania portfela natywną kryptowalutą popularnej sieci Polygon – POL oraz jak importować NFT kryptoznaczków.

1. Fedorczyk B., Dobre praktyki kryptofilatelistyki (1), Filatel.pl, nr 8/2025, s. 589-591
2. https://www.blockplate.com/pages/bip-39-wordlist?srsltid=AfmBOorbtWabFJTd4eyr4UHtLBRTsKbsooKYpnM8M1SzZkeIGcj4Pyun
3. MetaMask https://youtu.be/qfcUnK29ZUg, Rabby https://youtu.be/Zr9FR7w565k, dostęp 30.08.2025 r.
4. Nadanie frazy mnemonicznej https://youtu.be/GwlBaqc5kSk, instalacja aplikacji ETH https://youtu.be/LbW5zM_9GAE, dostęp 30.08.2025 r.
5. https://youtu.be/4HfLc7e2xOg, dostęp 30.08.2025 r.
6. https://youtu.be/Fp5cX28-ACg, dostęp 30.08.2025 r.

Ciąg dalszy (3) w Filatel.pl nr 10/2025.

□□□

Na kolejnej stronie przedstawiamy dokończenie tabeli nr 1 do artykułu „Warianty w cyfrowym świecie polskiego kryptoznaczka”, którego tekst był publikowany w Filatel.pl nr 6 i 7/2025. Sama tabela jest publikowana od nr 7/2025.



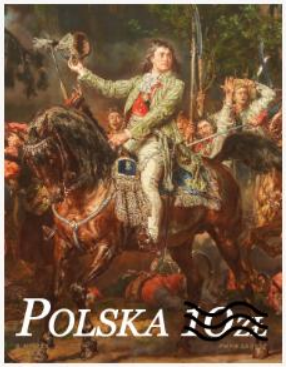
230. rocznica Insurekcji Kościuszkowskiej

Wariant Kościuszko pod Racławicami

Nakład: 1 000 szt.

Obraz statyczny:

https://opensea.io/assets/matic/0x92225e214880c6449fe3740c0045ac0a613eeaee/17002



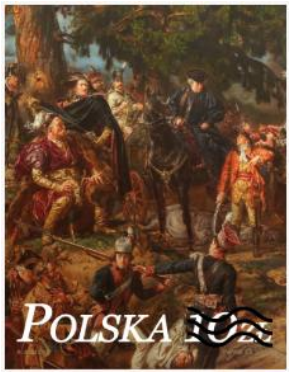
230. rocznica Insurekcji Kościuszkowskiej

Wariant Tadeusz Kościuszko

Nakład: 400 szt.

Obraz statyczny:

https://opensea.io/assets/matic/0x92225e214880c6449fe3740c0045ac0a613eeaee/874485



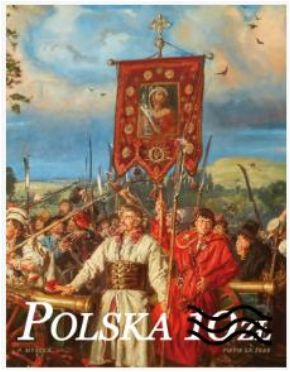
230. rocznica Insurekcji Kościuszkowskiej

Wariant Hugo Kołłątaj

Nakład: 200 szt.

Obraz statyczny:

https://opensea.io/assets/matic/0x92225e214880c6449fe3740c0045ac0a613eeaee/333318



230. rocznica Insurekcji Kościuszkowskiej

Wariant Bartosz Głowacki

Nakład: 100 szt.

Obraz statyczny:

https://opensea.io/assets/matic/0x92225e214880c6449fe3740c0045ac0a613eeaee/1222248

Wielka Orkiestra Świątecznej Pomocy

Wariant bujny

Nakład: 1 000 szt.

Obraz statyczny:

https://opensea.io/assets/matic/0xa49152874760f535c138a4b163926f7da56827fe/2008987

Wielka Orkiestra Świątecznej Pomocy

Wariant przerzedzony

Nakład: 900 szt.

Obraz statyczny:

https://opensea.io/assets/matic/0xa49152874760f535c138a4b163926f7da56827fe/2010992

Wielka Orkiestra Świątecznej Pomocy

Wariant rzadszy

Nakład: 600 szt.

Obraz statyczny:

https://opensea.io/assets/matic/0xa49152874760f535c138a4b163926f7da56827fe/1961167

Wielka Orkiestra Świątecznej Pomocy

Wariant bujny

Nakład: 1 000 szt.

Obraz statyczny:

https://opensea.io/assets/matic/0xa49152874760f535c138a4b163926f7da56827fe/1830710

Wielka Orkiestra Świątecznej Pomocy

Wariant przerzedzony

Nakład: 900 szt.

Obraz statyczny:

https://opensea.io/assets/matic/0xa49152874760f535c138a4b163926f7da56827fe/1834539

Wielka Orkiestra Świątecznej Pomocy

Wariant rzadszy

Nakład: 600 szt.

Obraz statyczny:

https://opensea.io/assets/matic/0xa49152874760f535c138a4b163926f7da56827fe/1832624

W tabeli przedstawiono statyczne obrazy wariantów NFT dla danego wydania kryptoznaczka oraz odnośniki prowadzące do przeglądarki umożliwiającej obejrzenie ich animacji, jeśli występuje.