Bartłomiej Fedorczyk

Dobre praktyki kryptofilatelistyki (1)

Celem statutowym Polskiego Związku Kryptofilatelistów jest edukowanie społeczeństwa poprzez „popularyzowanie kryptofilatelistyki oraz technologii blockchain wśród kolekcjonerów tradycyjnych fizycznych walorów kolekcjonerskich oraz wśród wszystkich innych osób zainteresowanych kryptofilatelistyką" (il. 1).

il. 1. Kryptodruk 1.0 to specjalne, pamiątkowe, limitowane wydawnictwo łączące tradycyjną filatelistykę z cyfrową. Wersja fizyczna jest wydana przez Pocztę Polską S.A.. Źródło: Poczta Polska S.A. Walor dostępny jedynie dla członków PZKF. Link do animacji NFT: https://pzkf.pl/katalog-kz/katalog-kz.html.

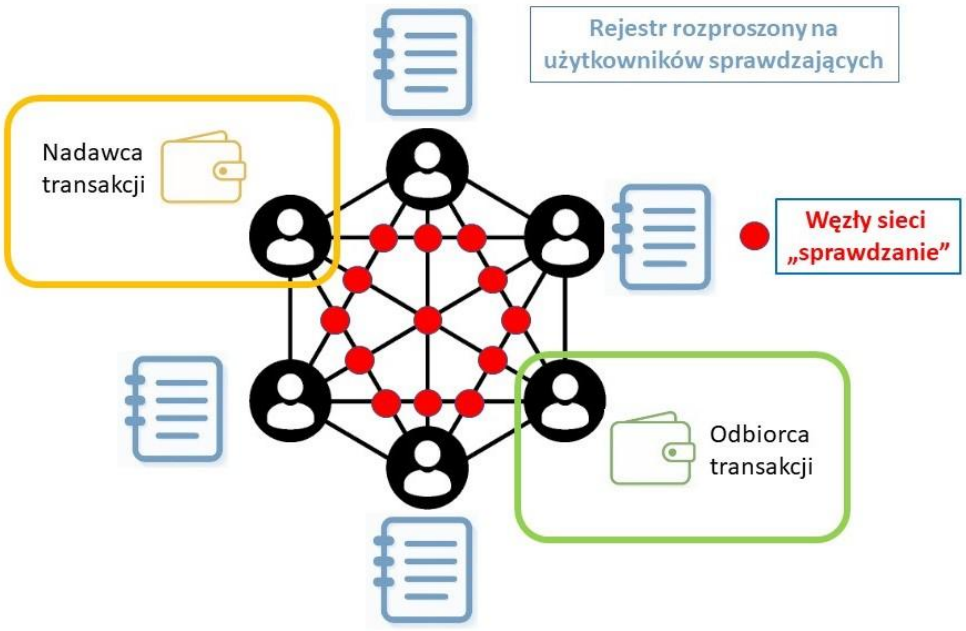
W poprzednich wydaniach Filatel.pl przedstawione zostały pewne definicje systematyzujące to, czym jest kryptoznaczek oraz jaka jest jego specyfika. Określono, co znaczy termin NFT [1] oraz jak w przypadku polskiego kryptoznaczka łączy się komplementarnie wersję cyfrową z walorem fizycznym [2, 3]. Wprowadzono nowe pojęcia odnoszące się do odmian oraz ich częstotliwości występowania w nakładzie walorów istniejących w domenie cyfrowej (warianty NFT) [4, 5].

Kryptoznaczki obecnie wydaje wiele narodowych operatorów pocztowych, między innymi w takich krajach jak: Austria, Szwajcaria, Liechtenstein, Francja, Belgia, Holandia, Luksemburg, Irlandia, Włochy, Portugalia, Hiszpania, Chorwacja, Niemcy, Tajlandia, Malezja, Wyspy Owcze itd. Z miesiąca na miesiąc, pojawia się coraz więcej argumentów świadczących o tym, że kryptofilatelistyka z chwilowej mody zaczyna stawać się pełnoprawnym trendem nowoczesnego kolekcjonerstwa. Na poparcie tego przytoczę fakt, że w Szanghaju w dniach od 29.11. do 3.12.2024 r., podczas CHINA 2024 Asian International Stamp Exhibition, odbyła się pierwsza wystawa kryptoznaczków z całego świata, dumnie prezentowana przez Luca Mangin [6], który notabene w maju 2025 został członkiem honorowym Polskiego Związku Kryptofilatelistów.

Z uwagi na powyższe zdecydowano się rozpocząć nowy, kilkuczęściowy cykl artykułów o dobrych praktykach kryptofilatelisty, które będą opisywać po kolei aspekty technologiczne, kwestie zachowania bezpieczeństwa kolekcji, a także praktyczne porady jak zacząć, jak zarządzać oraz jak czerpać satysfakcję z tej formy kolekcjonerstwa.

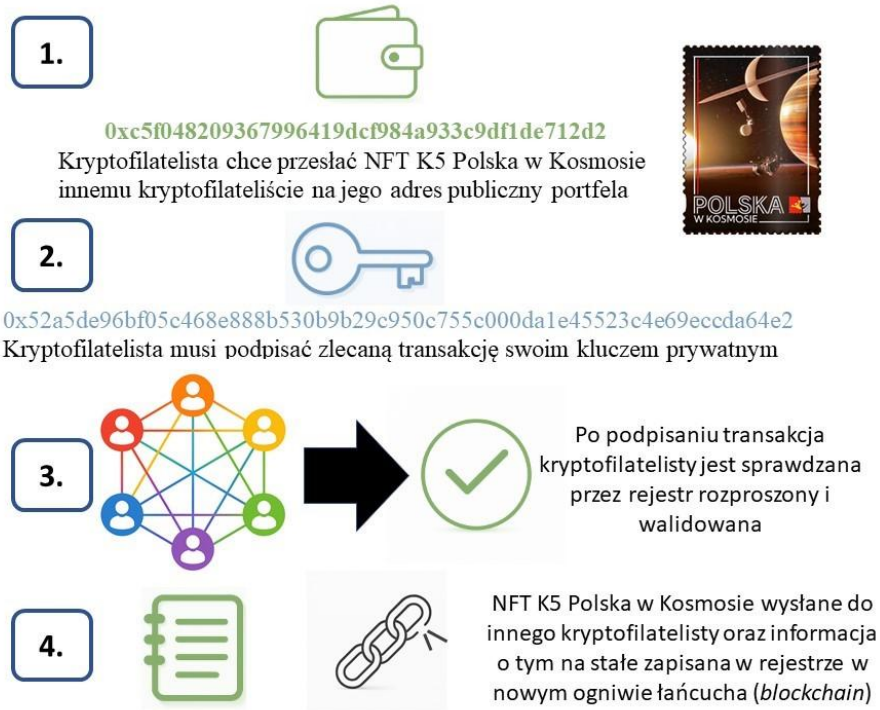
Na świecie istnieje wiele różnych sieci kryptowalutowych (*blockchain)*, a główne z nich to sieci bitcoin i ethereum. Pomińmy tutaj to, w jaki sposób osiągany jest w obu tych sieciach konsensus sieciowy, bo rozumienie tych mechanizmów nie jest potrzebne kryptofilateliście. Ważne jest by rozumieć to, że w obu sieciach konsensus jest zapewniany bez udziału tak zwanej strony trzeciej, a więc organu nadzorującego, który pełniłby rolę arbitra dla wszystkich transakcji dokonywanych na *blockchain* (il. 2). Zamiast „męża zaufania" mamy rejestr rozproszony, to znaczy, że użytkownicy sieci zarówno sami korzystają z sieci, jak również (jako społeczność) sprawdzają się wzajemnie pod kątem prawidłowości przeprowadzanych transakcji. W ten sposób znosi się problemy dotykające delikatnej sfery wzajemnego zaufania, bo jest ono zapewniane przez rozproszenie odpowiedzialności i decyzyjności między użytkownikami sieci. Dzięki temu osiąga się zgodność w sieci, czyli konsensus, a transakcje między użytkownikami sieci są zatwierdzane i skutecznie przeprowadzane. Każda czynność dokonana z użyciem sieci *blockchain* jest transakcją, która powoduje naliczenie opłaty za jej dokonanie. Opłaty wnosi się w formie natywnej kryptowaluty dla danego *blockchain*. Dla sieci ethereum płaci się ethereum, a dla sieci bitcoin płaci się bitcoinem. Zarysowaliśmy sobie w bardzo ogólny sposób, jak działają sieci blockchain oraz to, że jest ich bardzo dużo. Trzeba zorientować się, na której sieci obsługiwane są kryptoznaczki, które chcemy kolekcjonować. Dla przykładu polski

kryptoznaczek jest obsługiwany przez sieć Polygon, która wykorzystuje EVM (Ethereum Virtual Machine), a więc jest pochodną sieci ethereum, a jej natywny token do pobierania opłat to POL.



il. 2. Schemat działania sieci opartej o rejestr rozproszony. Sieć łączy ze sobą wszystkich użytkowników w ramach węzłów sieci. Nadawca wysyła swoją transakcję do odbiorcy, która jest sprawdzana przez pozostałych użytkowników sieci posiadających część rozproszonego rejestru.

Zacznijmy zatem od narzędzia absolutnie podstawowego, które każdy kryptofilatelista musi posiadać. Jest to portfel kryptowalutowy, a ściślej rzecz ujmując adres publiczny, który jest prezentowany wszystkim użytkownikom sieci oraz klucz prywatny, który służy do składania i podpisywania dyspozycji na wykonanie danej transakcji przez sieć *blockchain*. Klucz prywatny należy ukrywać przed wszystkimi, bo daje on nieograniczony dostęp do portfela. Obie części są kodowane w systemie szesnastkowym i przykładowo wyglądają tak: 0xc5f048209367996419dcf984a933c9df1de712d2 – adres publiczny; 0x52a5de96bf05c468e888b530b9b29c950c755c000da1e45523c4e69eccda64e2 – klucz prywatny (il. 3.).



II. 3. Schemat przedstawiający jak adres publiczny i klucz prywatny są używane w poszczególnych etapach przeprowadzania transakcji na sieci blockchain na przykładzie przesyłania NFT K5 kryptoznaczka „Polska w Kosmosie”.

Jeśli nie posiadamy jeszcze żadnego własnego klucza prywatnego oraz przypisanego do niego adresu publicznego, to musimy go wygenerować samodzielnie. Dokonuje się to poprzez wykorzystanie słownika BIP-39 [7]. Jest to słownik

2048 wyrazów w języku angielskim, z którego wybiera się w zależności od standardu dwunasto- lub osiemnasto-, a nawet dwudziestoczterowyrazowe ciągi mnemoniczne (frazy mnemoniczne). Najczęściej losuje się te ciągi słów, ale można je sobie samemu zdefiniować. Na pierwszy rzut oka sprawia to wrażenie, że dwóch użytkowników może wylosować lub zapisać identyczny ciąg słów, ale na te wątpliwości można sobie odpowiedzieć zestawiając je z liczbą możliwych kombinacji fraz mnemonicznych, a więc 2048^{12}, 2048^{18}, 2048^{24}. Są to ogromne liczby, więc takie prawdopodobieństwo jest niezwykle niskie, a praktycznie zerowe. Fraza mnemoniczna jest następnie konwertowana funkcją SHA-265 (Secure Hash Algorithm) w pełnoprawny klucz prywatny, z którego dalej generowany jest sparowany do niego adres publiczny. Tak ogólnie ujmując tworzony jest świeży portfel kryptowalutowy do przechowywania na nim własnej kolekcji kryptoznaczków. Frazę mnemoniczną dobrze jest zapisać po to, by w razie utraty dostępu do portfela móc sobie go awaryjnie odtworzyć. Muszę tutaj również uczulić Czytelnika, że należy odpowiednio zabezpieczyć tę frazę i najlepiej nie przechowywać jej na cyfrowych nośnikach podpinanych do urządzeń z dostępem do internetu. Przed rozmaitym i wysublimowanym oprogramowaniem szpiegującym najlepiej chroni kartka papieru lub metalowa płytka z wyrytymi wyrazami.

Użytkownik ma do dyspozycji odpowiednie narzędzia, które usprawniają powyższy proces zakładania portfela i sprowadzają się do instalowania aplikacji na własnym komputerze oraz do zapisania i zabezpieczenia frazy mnemonicznej do nowego portfela kryptowalutowego. Kryptofilatelista ma do wyboru dwa rodzaje rozwiązań do zarządzania swoim portfelem, nazywane *hot wallet* oraz *cold wallet*. Pierwszy typ: *gorący portfel* jest aplikacją, rozszerzeniem przeglądarki internetowej, w którym integralnie przechowywane są fraza mnemoniczna oraz klucz prywatny. Rozwiązanie to nosi taką nazwę, ponieważ jest podatne na działanie oprogramowania szpiegującego i trzeba bardzo dobrze dbać o bezpieczeństwo swojego komputera, aby nie paść ofiarą złodzieja, który bez najmniejszego trudu opróżni przejęty portfel. Drugim typem jest *zimny portfel*, który jest fizycznym urządzeniem. Działa on w ten sposób, że dane wrażliwe, a więc fraza mnemoniczna oraz klucz prywatny, są zapisane w pamięci tego urządzenia. Urządzenie podłącza się do komputera przez złącze USB i używa do podpisania zlecanej transakcji. Klucz prywatny jest wówczas dodatkowo szyfrowany i w momencie interakcji z komputerem podłączonym do internetu jest prezentowany do podpisania i zatwierdzenia transakcji. Urządzenie przechowuje klucz prywatny w całości *offline*, a więc informacja o kluczu prywatnym nie jest eksponowana ani przechowywana w pamięci komputera.

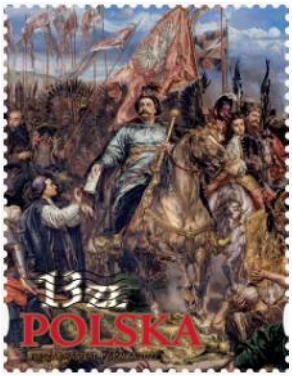
Powyżej opisane zostały aspekty technologiczne wyjaśniające zasadę działania podstawowego narzędzia do deponowania swojej kolekcji kryptofilatelistycznej. W kolejnym numerze przejdziemy do praktycznych przykładów i omówimy krok po kroku, jak w świadomy i bezpieczny sposób założyć swój pierwszy portfel kryptowalutowy by rozpocząć swoją przygodę z kryptofilatelistyką.

1. Fedorczyk B., Wstęp do kryptofilatelistyki, Filatel.pl, nr 3/2025, s. 197-198
2. Fedorczyk A., Fedorczyk B. Cantor wymiany numerów w Polskim Kryptoznaczku. Filatel.pl, nr 4/2025, s. 276-278
3. Fedorczyk A., Fedorczyk B. Katalog polskich kryptoznaczków, Filatel.pl, nr 5/2025, katalog nowości polskich.
4. Fedorczyk B., Warianty w cyfrowym świecie polskiego kryptoznaczka (1), Filatel.pl nr 6/2025, s. 422-426.
5. Fedorczyk B., Warianty w cyfrowym świecie polskiego kryptoznaczka (2), Filatel.pl nr 7/2025, s. 506.
6. https://www.linkedin.com/posts/lucmangin_crypto-stamp-philately-activity-7265795597578682368-tfhj, dostęp: 12.07.2025 r. oraz oraz https://youtu.be/LZToupmqkHo?si=opGV8vVQsH86v2R8, dostęp 12.07.2025 r.
7. https://www.blockplate.com/pages/bip-39-wordlist?srsltid=AfmBOorbtWabFJTd4eyr4UHtLBRTsKbsooKYpnM8M1SzZkeIGcj4Pyun

Ciąg dalszy (2) w Filatel.pl nr 9/2025.

□□□

Na kolejnej stronie przedstawiamy dalszy ciąg 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.



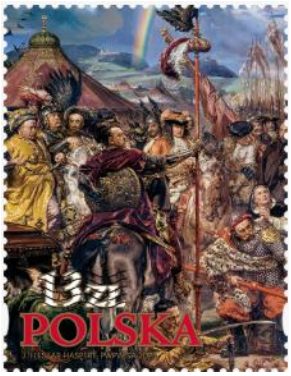
Odsiecz Wiedeńska

Wariant podstawowy

Nakład: 1460 szt.

Obraz statyczny:

https://opensea.io/assets/matic/0xccc9d2f983632cdf1d5d1d154eda8526ad828916/887773



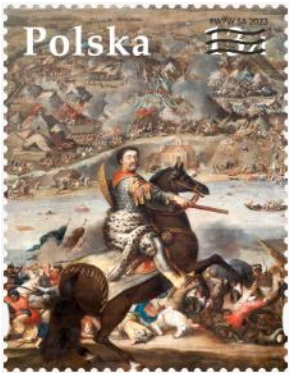
Odsiecz Wiedeńska

Wariant z Towarzyszem hufców z buńczukiem w dłoni

Nakład: 340 szt.

Obraz statyczny:

https://opensea.io/assets/matic/0xccc9d2f983632cdf1d5d1d154eda8526ad828916/886441



350-lecie Bitwy pod Chocimiem

Wariant podstawowy

Nakład: 1363 szt.

Obraz statyczny:

https://opensea.io/assets/matic/0x738059f56475be69a727dddeda9d194e3be8132d/208327

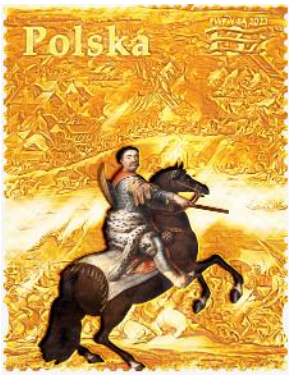
350-lecie Bitwy pod Chocimiem

Wariant srebrny

Nakład: 267 szt.

Animacja i dźwięk:

https://opensea.io/assets/matic/0x738059f56475be69a727dddeda9d194e3be8132d/131320



350-lecie Bitwy pod Chocimiem

Wariant złoty

Nakład: 70 szt.

Animacja i dźwięk:

https://opensea.io/assets/matic/0x738059f56475be69a727dddeda9d194e3be8132d/131833

230. rocznica Insurekcji Kościuszkowskiej

Wariant Kościuszko pod Racławicami

Nakład: 1000 szt.

Obraz statyczny:

https://opensea.io/assets/matic/0x92225e214880c6449fe3740c0045ac0a613eeaee/1233223

230. rocznica Insurekcji Kościuszkowskiej

Wariant Tadeusz Kościuszko

Nakład: 400 szt.

Obraz statyczny:

https://opensea.io/assets/matic/0x92225e214880c6449fe3740c0045ac0a613eeaee/1231653

230. rocznica Insurekcji Kościuszkowskiej

Wariant Hugo Kołłątaj

Nakład: 200 szt.

Obraz statyczny:

https://opensea.io/assets/matic/0x92225e214880c6449fe3740c0045ac0a613eeaee/96568

230. rocznica Insurekcji Kościuszkowskiej

Wariant Bartosz Głowacki

Nakład: 100 szt.

Obraz statyczny:

https://opensea.io/assets/matic/0x92225e214880c6449fe3740c0045ac0a613eeaee/735066

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

Dokończenie w następnym numerze.