Bartłomiej Fedorczyk, Dariusz Tyszka

Pierwszy na świecie kryptoznaczek. Kryptograficzny „Jednorożec” jako fundament cyfrowej filatelistyki

Wybór jednorożca na motyw przewodni pierwszej historycznej emisji kryptoznaczka niesie ze sobą głęboką symbolikę, która doskonale spaja świat tradycji z nowoczesnością. To mityczne stworzenie, od wieków będące uosobieniem czystości, szlachetności i nieuchwytnej rzadkości, w dzisiejszym żargonie biznesowym zyskało zupełnie nowe znaczenie. Mianem jednorożca określa się bowiem niezwykle rzadkie i wyjątkowo intratne inwestycje, startupy, których wycena przekracza miliard dolarów. Ta dwoistość natury, a więc z jednej strony legenda, z drugiej synonim spektakularnego sukcesu rynkowego, czyni z austriackiego wydania walor skrojony pod oczekiwania kolekcjonera XXI wieku, który w klaserze szuka nie tylko piękna, ale też obiektywnie udokumentowanej rzadkości i proweniencji [1].

Transformacja cyfrowa, opisywana na łamach Filatel.pl, jest procesem, który realnie ma szansę trwale zmienić percepcję kolekcjonerskiej rzeczywistości. W historii filatelistyki mieliśmy wiele dat uznawanych za kamienie milowe. Równie ważną datą jest 11 czerwca 2019 roku. To właśnie wtedy Poczta Austriacka (*Österreichische Post AG*) nie tyle wyemitowała nowy znaczek, co otworzyła portal do nowego wymiaru istnienia waloru filatelistycznego. *Crypto Stamp 1.0* (*CS 1.0*, kryptoznaczek 1.0) stał się dowodem na to, że filatelistyka może iść w parze z najbardziej zaawansowaną kryptografią. Technologia *blockchain* nie jest po to, by niszczyć tradycję, lecz by ją ocalić, nadając jej „cyfrową duszę”, która jest niepodrabialna. Systemy te, operujące na liczbie kombinacji rzędu 10^{32}, co jak wiemy wielokrotnie przewyższa liczbę gwiazd w widzialnym Wszechświecie [2], dają nam fundament bezpieczeństwa, jakiego żadne pokolenie filatelistów nie znało wcześniej.

Z systematycznego punktu widzenia, w przypadku „Jednorożca” mamy do czynienia z samoprzylepnym walorem o nominale 6,90 EUR. Swoistym *novum* jest to, że znaczek ten jest osadzony na sztywnym bloku wykonanym z polichlorku winylu (PCV), który swoimi wymiarami 86 mm na 56 mm bardzo przypomina kartę kredytową, lecz z drobnymi wcięciami w połowie długości, z możliwością przełamania bloku na pół. Znaczek nie posiada perforacji *per se*, a jedynie jest na jego powierzchni nadrukowany odpowiedni wzór odpowiadający perforacji 13. Na awersie nadruk wykonany jest czarną farbą z opalizującymi elementami (il. 1). Został on wykonany przez firmę Variuscard Productions i użyto tu łączonej techniki sitodruku i druku offsetowego [3]. Znaczek powstał według projektu Julii Obermüller i w katalogu Michela jest oznaczony jako Mi 3470. Rewers znaczka jest biały, bez nadruku.

Jednak to, co czyni go unikatowym, ukryte jest pod warstwą zabezpieczającą (zdrapką, il. 1). Pierwszy właściciel waloru, usuwając warstwę ochronną, dokonuje swoistego aktu erekcyjnego, odsłaniając klucze dostępu pozwalające przejąć kontrolę nad cyfrowym bliźniakiem (NFT) w sieci Ethereum. Aby zaopiekować się swoimi zasobami i bezpiecznie przechowywać je w jednym miejscu w sieci [4], należy najpierw odzyskać klucz prywatny ukryty pod zdrapką, a następnie zaimportować go do portfela kryptowalutowego. Dysponując odpowiednią ilością tokena natywnego sieci ETH na pokrycie opłaty transakcyjnej (adres jest fabrycznie zasilony), możemy dokonać odkrycia wariantu NFT, a następnie transferować cyfrowy walor. Ten proces, choć techniczny, jest w istocie współczesną formą układania znaczków w klaserze, z tą różnicą, że nasz „klaser” jest odporny na wilgoć i grzyby, a każdy ruch w nim zapisany zostaje na zawsze w rejestrze rozproszonym.

Warto w tym miejscu pochylić się nad samym mechanizmem powiązania waloru fizycznego z komplementarnym NFT, który w przypadku austriackiej emisji oparto na autorskim algorytmie generowania kodu Code1. Podczas gdy w Polskim Kryptoznaczku analizowaliśmy funkcję parującą Cantora [5], Austriacy zastosowali system deterministyczny oparty na dwóch filarach nowoczesnej kryptografii: funkcji skrótu SHA-256 oraz kodowaniu Base58.

il. 1. Kryptoznaczek 1.0 (Crypto stamp 1.0; CS 1.0) Mi 3470 „Jednorożec". U góry walor z rynku wtórnego dostępny na jednej z licytacji z zachowaną zdrapką w polach oznaczonych [2] oraz [3]. Pod zdrapką w polu [2] ukryty jest klucz prywatny, a w polu [3] mamy ukrytą frazę mnemoniczną. Na dole wizualizacja bloku znaczka z uwidocznieniem elementów opalizujących. Grafika poglądowa wykonana przez emitenta Österreichische Post AG. Na obu prezentacjach widoczne charakterystyczne wcięcie w bloku ułatwiające jego przełamanie i zdjęcie samoprzylepnego znaczka.

Zrozumienie mechaniki *Crypto Stamp 1.0* wymaga zrozumienia działania SHA-256 (Secure Hash Algorithm 256-bit). Jest to matematyczny strażnik, który generuje wspomnianą wcześniej potęgę bezpieczeństwa. SHA-256 działa jak jednostronna, cyfrowa maszynka do mięsa: wrzucamy do niej surowe dane, a w zamian otrzymujemy przetworzony unikatowy, niemożliwy do podrobienia odcisk palca w postaci *hasha*. W austriackim algorytmie proces ten jest precyzyjny: numer seryjny znaczka (liczba dziesiętna nadrukowana osobno na walorze) konwertowany jest na trzy bajty, a następnie z tych bajtów obliczany jest *hash* SHA-256. Pobranie tylko pierwszego bajta z tego *hasha* służy jako suma kontrolna (*checksum*). To dzięki niej system natychmiast „wie", czy wpisany przez nas kod Code1 jest prawidłowy. To matematyczna pewność, która zastępuje tradycyjną weryfikację organoleptyczną waloru i chroni nas przed błędami przy przepisywaniu.

Otrzymany bajt sumy kontrolnej jest następnie doklejany na początku trzech bajtów numeru seryjnego, tworząc czterobajtowy ciąg. Tak powstały ciąg kodowany jest w alfabecie Base58, dając ostateczną postać Code1 (oznaczenie [1] na il. 1, np. 2P4nLz). W przeciwieństwie do standardowych systemów, Base58 celowo pomija znaki, które w druku mogą prowadzić do tragicznych w skutkach pomyłek: cyfrę 0 i wielką literę O oraz wielką literę I i małą literę l. To przykład tego, jak zaawansowana technologia pochyla się nad ludzką percepcją, by ucyfrowienie było wolne od frustracji. Co ciekawe, Base58 nie jest standardem informatycznym. Został zaprojektowany w 2009 roku przez Satoshiego Nakamoto specjalnie na potrzeby adresów Bitcoin, właśnie po to, by ich ręczne przepisywanie było odporne na pomyłki. Wybierając ten alfabet, Poczta Austriacka świadomie sięgnęła po kodowanie kryptowalutowe. Austriacki Code1 i adresy Bitcoin mówią dosłownie tym samym językiem znaków.

Tak rygorystyczne podejście do szyfrowania cyfrowej warstwy waloru pozwala na bezpieczne egzystowanie w domenie *blockchain* jego pięciu wariantów kolorystycznych (il. 2). Przy całkowitej emisji 150 000 sztuk bloków PCV, rozkład barw przedstawia się następująco: wariant czarny (*Black*) w liczbie 78 500 szt., zielony (*Green*) – 40 000 szt., niebieski (*Blue*) – 20 000 szt., żółty (*Yellow*) – 10 000 szt. oraz najbardziej pożądany, czerwony (*Red*), stanowiący zaledwie 1% nakładu (1 500 szt.). Czerwony Jednorożec stał się niemal natychmiast Świętym Graalem nowej dyscypliny, a fakt jego istnienia jest twardo i obiektywnie udokumentowany w rejestrze rozproszonym. Zabezpiecza to kolekcjonerów przed podróbkami, których odróżnienie wymagało niegdyś angażowania wysoko wykwalifikowanych specjalistów. Teraz każdy znaczek ma swój niezbywalny certyfikat autentyczności zapisany w *blockchain*.

il. 2. Zestawienie dostępnych wariantów NFT komplementarnych do znaczka fizycznego. Wariant czarny (Black) nakład 78 500 szt., zielony (Green) nakład 40 000 szt., niebieski (Blue) nakład 20 000 szt., żółty (Yellow) nakład 10 000 szt., czerwony (Red), nakład (1 500 szt.).

Warto podkreślić, że rejestr ten ma charakter w pełni publiczny i transparentny. Dzięki temu dokładnie wiadomo, który konkretnie adres publiczny posiada dany walor w danym momencie. Ta jawność eliminuje wszelkie niepewności i niedomówienia, tak powszechne w tradycyjnym handlu antykwarycznym, nie wspominając już o wymianie prywatnej między kolekcjonerami. Dzięki technologii NFT cały świat filatelistyczny staje się wielkości jednego pchlego targu, gdzie wszystkie walory i ich posiadacze są na wyciągnięcie ręki. *Blockchain* eliminuje bariery geograficzne i czasowe, a wymiana rzadkiego okazu trwa tyle, ile zatwierdzenie transakcji w sieci. To skrócenie dystansu jest kluczowe dla ewolucji naszej pasji, integrując pokolenia wokół wspólnego, globalnego rejestru. Austriacki *Crypto Stamp 1.0* udowodnił, że filatelistyka może być nowoczesna i absolutnie bezpieczna. Algorytmy i *hashowanie* to tylko narzędzia, które zaplatają łańcuchy bloków (*blockchain*). Te z kolei im są dłuższe, tym skuteczniej skracają dystans między nami, ludźmi połączonymi wspólną pasją.

1. Fedorczyk B., Kryptodruk – przykład jak blockchain może transformować filatelistykę, Filatel.pl, nr 5/2026, s. 496-498
2. Fedorczyk B., Wstęp do kryptofilatelistyki, Filatel.pl, nr 3/2025, s. 197-198.
3. Luc Mangin, https://crypto-stamps.org/catalogue/europe/austria/2019-2021/, dostęp 8.05.2026 r.
4. Fedorczyk B., Lech G., Dobre praktyki kryptofilatelistyki (4), Filatel.pl, nr 11/2025, s. 848-850.
5. Fedorczyk A., Fedorczyk B., Cantor wymiany numerów w Polskim Kryptoznaczku (1), Filatel.pl, nr 4/2025, s. 276-278.