Bartłomiej Fedorczyk, Dariusz Tyszka

Cyfrowa anatomia kodu austriackiego Crypto Stamp 1.0. Kryptograficzne ciekawostki i sekrety parowania walorów

Niniejszy artykuł jest dedykowany zaawansowanym kryptofilatelistom, którzy zwracają uwagę na szczegóły związane z numerami seryjnymi, specyfiką parowania waloru fizycznego z jego komplementarnym NFT, co przekłada się na rozmaite ciekawostki towarzyszące wydaniu austriackiego *CS 1.0* (*Crypto Stamp 1.0*). Jest to opracowanie badawcze polegające na mapowaniu całego nakładu tej serii i będzie ono szczególnie przydatne dla tych kolekcjonerów, którzy zastanawiają się nad zakupem waloru z rynku wtórnego. W takiej sytuacji sprzedający często zamieszcza zdjęcie wystawianego waloru, na którym widoczny jest Code[1] (il. 1). Każdy z trzech prezentowanych walorów ma już odkryty jeden wariant z pięciu dostępnych kolorów NFT [1]. Co prawda, skanowanie kodu QR pozwala podejrzeć dany wariant kolorystyczny, ale nie da się z tego poziomu sprawdzić, jaki numer porządkowy ma obserwowany walor w całym nakładzie. Istnieje gros kryptofilatelistów, dla których informacja o numerze seryjnym jest istotną ciekawostką cechującą dany przedmiot kolekcjonerski. Nasze opracowanie pozwala na zrozumienie mechanizmu parowania, jaki stoi za wydaniami austriackich kryptoznaczków oraz daje możliwość samodzielnego sprawdzenia stanu faktycznego dla danego waloru. Dzięki tej wiedzy kryptofilatelista w sposób świadomy może porządkować swoje zbiory i wybrać odpowiadającą mu drogę do kolekcjonerskiego spełnienia.

Współczesna kryptofilatelistyka, stanowiąca naturalny etap ewolucji tradycyjnego kolekcjonerstwa w dobie rozwiązań *Web 3.0*, redefiniuje pojęcie unikalności oraz autentyczności waloru pocztowego. Klasyczne badanie struktury papieru, analizowanie odcieni za pomocą próbnika barw czy weryfikacja perforacji zostają uzupełnione o zaawansowany aparat matematyczno-kryptograficzny. Zrozumienie systemu parowania waloru fizycznego oraz komplementarnego doń NFT jest kluczowe dla zaawansowanego kolekcjonera kryptowalorów, gdyż pozwala na pewne poruszanie się po współczesnym rynku i świadome budowanie zbiorów o wysokim stopniu rzadkości. W niniejszym opracowaniu mechanizm pracy systemu parującego został kompleksowo opisany i jest to pierwsze tego typu opracowanie na świecie, które ekstrapoluje się do wszystkich wydanych emisji kryptoznaczków austriackich oraz niektórych emisji łączonych, jak na przykład Austria-Holandia itd. Zasada działania systemu jest tożsama z emisji na emisję. Opracowanie to stanowi bezcenną wiedzę dla kolekcjonerów najbardziej rozpoznawalnych serii kryptoznaczków wydawanych przez Pocztę Austriacką (*Österreichische Post*), pioniera w tej dziedzinie o ugruntowanej pozycji na rynku światowym.

Gdy trzymamy w ręku tradycyjny, polimerowy (PCV) blok *Crypto Stamp 1.0*, nasz wzrok przyciąga unikalny element graficzny, nadrukowany bezpośrednio na fizycznym walorze, a więc tajemniczy ciąg alfanumeryczny określany w nomenklaturze emisyjnej jako Code[1] (il 1.). Dla niewtajemniczonego oka to jedynie ciąg przypadkowych znaków. W rzeczywistości ten niepozorny zapis pełni funkcję fundamentalnego pomostu między dwoma światami, bo stanowi ściśle zdefiniowany kod porządkowy, którego zadaniem jest bezbłędne, deterministyczne sparowanie fizycznego bloku z jego komplementarnym cyfrowym bliźniakiem (NFT) zapisanym w rozproszonej strukturze łańcucha bloków.

Dopiero gdy zajrzymy w głąb metadanych tego cyfrowego tokena (NFT), odkryjemy unikalną wartość *tokenID*, która jest numerem seryjnym odpowiadającym precyzyjnej pozycji danego egzemplarza w całym nakładzie. Numer seryjny jest reprezentowany w bazie danych jako wartość dziesiętna (DEC). Jest to swego rodzaju ciekawostka, gdyż emitenci zwykli nadrukowywać numery seryjne na walor, a tu zamiast tego mamy jedynie Code[1]. Drobiazgowa analiza pełnej populacji 150 000 takich par (od *tokenID* 0 do 149 999, bo takie numery seryjne nadano znaczkom *CS 1.0*) ukazuje fascynującą dyscyplinę matematyczną, algorytmiczne anomalie i ukryte prawidłowości, które dla zaawansowanego kolekcjonera stanowią ekscytujące pole do kwerend i poszukiwań.

il. 1. Zrzuty ekranu dla walorów wystawionych do sprzedaży na portalu aukcyjnym Delcampe.net. Stan na 4.06.2026 r. Każdy z walorów ma zasłoniętą zdrapkę i jest w stanie MHN, co w tradycyjnej filatelistyce wiąże się z kasowaniem, ale w kryptofilatelistyce niekoniecznie oznacza, że NFT nie jest zdeterminowane i odkryte. W polu oznaczonym [1] widoczny Code[1].

W celu pełnego zrozumienia technicznej strony tego procesu należy wyjaśnić, czym jest system szesnastkowy (heksadecymalny), powszechnie wykorzystywany w informatyce i kryptografii. Jest to pozycyjny system liczbowy, w którym podstawą jest liczba 16. W odróżnieniu od klasycznego systemu dziesiętnego, którym posługujemy się na co dzień i który dysponuje dziesięcioma cyframi (od 0 do 9), system szesnastkowy wymaga szesnastu znaków do zapisu wartości. Do reprezentowania liczb od 0 do 9 używa się standardowych cyfr, natomiast dla wartości od 10 do 15 wprowadza się pierwsze litery alfabetu łacińskiego: A oznacza 10, B to 11, C to 12, D to 13, E to 14, a F odpowiada wartości 15. Zastosowanie systemu szesnastkowego pozwala na znacznie bardziej zwarty i czytelny dla maszyn zapis danych binarnych, gdzie jeden bajt informacji (osiem bitów) może być zawsze zapisany za pomocą dokładnie dwóch znaków heksadecymalnych (HEX).

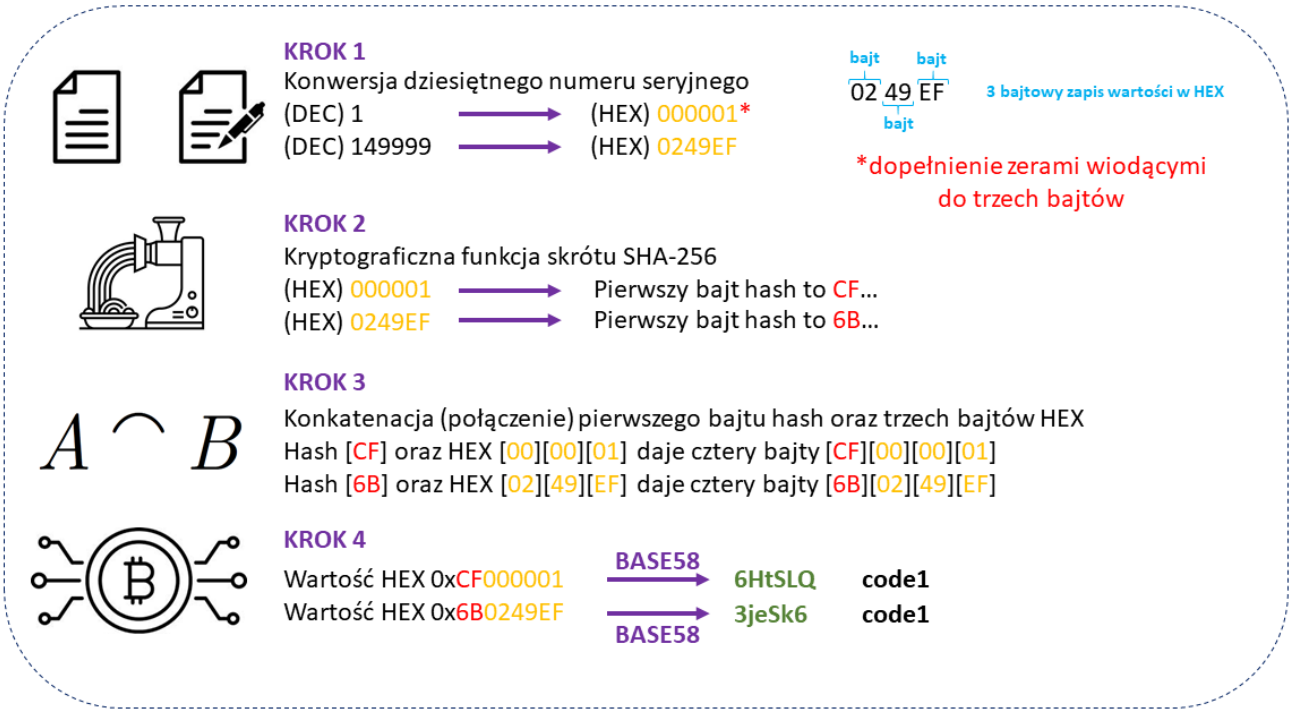
Proces wyliczania krótkiego kodu alfanumerycznego (Code[1], czyli wartości oznaczonej [1] na bloku kryptoznaczka na il. 1.) z dziesiętnego numeru seryjnego (DEC) opiera się na strukturze zbliżonej do tworzenia adresów w sieci Bitcoin. Algorytm realizuje dwa główne cele: maksymalne skrócenie zapisu danych na papierowym walorze oraz skuteczne zabezpieczenie przed błędami (literówkami) przy ręcznym przepisywaniu, dzięki wbudowanej sumie kontrolnej (wykrywalność błędów 99,6%). Procedura ta składa się z czterech precyzyjnych kroków matematyczno-kryptograficznych (il. 2):

Krok 1: Wyrównanie binarne numeru seryjnego (3 bajty). Wejściowy numer seryjny w zapisie dziesiętnym (DEC) zostaje przekonwertowany na wspomniany system szesnastkowy (HEX). W celu ujednolicenia struktury danych niezależnie od wielkości liczby, wynik jest wyrównywany do stałej długości 3 bajtów (czyli dokładnie 6 cyfr HEX) poprzez dopełnienie wiodącymi zerami z lewej strony.

Krok 2: Wygenerowanie sumy kontrolnej (kryptograficzny hash SHA-256). Wygenerowane 3 surowe bajty danych (traktowane jako ciąg binarny, a nie tekst ASCII) poddawane są jednostronnemu haszowaniu algorytmem SHA-256. Z otrzymanego, pełnego 32-bajtowego hasha wycinany jest wyłącznie pierwszy bajt (dwie pierwsze cyfry HEX oznaczone na czerwono), pełniący funkcję unikalnej sumy kontrolnej (*checksum*).

Krok 3: Konkatenacja danych. Następuje fizyczne złączenie komponentów. Wyliczony bajt sumy kontrolnej zostaje doklejony bezpośrednio przed 3 bajty numeru seryjnego, tworząc spójny blok danych o stałej długości 4 bajtów (8 cyfr HEX).

Krok 4: Zmiana bazy liczbowej i kodowanie Base58. Powstały 4-bajtowy ciąg HEX interpretowany jest jako jedna duża liczba całkowita w systemie dziesiętnym, na której wykonywana jest operacja matematyczna polegająca na zamianie bazy z systemu dziesiętnego na system Base58. W procesie wykorzystywany jest oficjalny alfabet Bitcoin: 123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz. Alfabet ten celowo eliminuje znaki 0, O, I oraz l, aby zapobiec pomyłkom wizualnym przy odczycie kodu z fizycznego bloku. Jeśli w tym kroku pierwszy bajt jest zerowy [00], to przy kodowaniu Base58 dostawia się jedynki wiodące. Dla przykładu numeru seryjnego 454 pełny blok danych to 0x[00][00][01][C6], więc na początku są aż dwa bajty zerowe, za które dostawiane są jedynki wiodące w Code[1] i otrzymujemy 4-znakowy kod 118q (il. 2).



il. 2. Mechanizm parowania numeru seryjnego kryptowaloru wydawanego przez Pocztę Austriacką. Dla CS 1.0 „Jednorożec" numery seryjne zawierają się w przedziale od 0 do 149 999. Kolejne wydania mają numery seryjne z zachowaniem tej ciągłości, a więc CS 2.0 zaczyna się od 150 000. To sprawia, że w 3 bajtach numeru seryjnego można zakodować zakres od 0 do 16 777 216.

Prawdziwym fundamentem kryptofilatelistycznej architektury i obiektem pożądania poszukiwaczy jest długość znakowa nadrukowanego kodu. Choć 4-bajtowy blok wejściowy ma stałą strukturę, matematyczna konwersja na system zapisu Base58 sprawia, że algorytm odpowiedzialny za generowanie Code[1] dla poszczególnych *tokenID* działa w sposób wysoce funkcyjny, różnicując długość ostatecznego ciągu.

Większość fizycznych bloków paruje się z 6-znakowym Code[1]. To one stanowią standard emisyjny, czego doskonałym przykładem jest kod 3ajkTs przypisany do bardzo niskiego *tokenID* 2 z początku stawki, kod 4RfhoC połączony z *tokenID* 70759 ze środka, czy chociażby zamykający globalne zestawienie kod 3jeSk6 sprzężony z *tokenID* 149999 na samym końcu serii.

Druga pod względem liczności grupa to kody 5-znakowe. Ich rozpiętość w metadanych jest ogromna, bo odnajdziemy je zarówno na samym początku emisji w formie kodu nxcjr powiązanego z *tokenID* 9, w środku stawki jako kod SD51n przy *tokenID* 54573, jak i pod postacią kodu wsJzL przypisanego pod koniec zbioru do *tokenID* 149905.

Stosunkowo rzadkimi są kody 4-znakowe, które są poszukiwane przez kolekcjonerów. Ich populacja na tle całego nakładu jest bardzo niska, bo wynosi zaledwie 356 szt. na 150 000 szt. (tab. 1.) Rozmieszczenie 356 czteroznakowych kodów w nakładzie nie jest przypadkowe. Kod skraca się do czterech znaków tylko wtedy, gdy suma kontrolna SHA-256 wyniesie zero (szansa 1 do 256), a numer seryjny wypadnie w jednym z dwóch szczególnych przedziałów. Stąd dwa

rozłączne pasma: 13 sztuk między *tokenID* 454 a 2981 oraz 343 sztuki powyżej *tokenID* 65 752. Pomiędzy tymi pasmami kod czteroznakowy nie może wystąpić.

tab. 1. Zestawienie występowania danej kategorii Code[1] w całym nakładzie CS 1.0 „Jednorożec" wydanego przez Österreichische Post.

Kategoria Code[1]	Liczba [szt.]	Procent w nakładzie [%]
Kody 6-znakowe	126 476	84,3 %
Kody 5-znakowe	23 168	15,4 %
Kody 4-znakowe	356	0,2 %
pełny nakład	150 000	

Gdy wejdziemy głębiej w zmapowaną strukturę alfanumeryczną zapisów wszystkich Code[1], odkryjemy przypadki o ciekawych cechach, które z uwagi na swoją wyjątkowość również budzą zainteresowanie wśród kryptofilatelistów. Ukazuje się tutaj nieco naleciałości z dziedziny notafilistyki, bo numery seryjne są zdecydowanie domeną kolekcjonerską osób zbierających banknoty i rozmaite bilety skarbowe. Przekrój różnorodnych kategorii Code[1] w całej populacji CS 1.0 „Jednorożec" jest dość znaczący. Oprócz wyżej wymienionych kodów o różnej ilości użytych znaków mamy przypadki, gdzie w kodzie są użyte tylko litery lub tylko cyfry. Są też takie kody, w których występują jedynie wielkie litery lub jedynie małe litery (tabela 2).

tab. 2. Zestawienie występowania rzadkich podkategorii Code[1] w całym nakładzie CS 1.0 „Jednorożec" wydanego przez Österreichische Post.

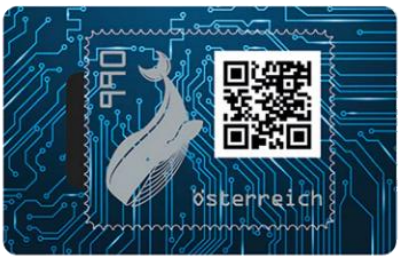
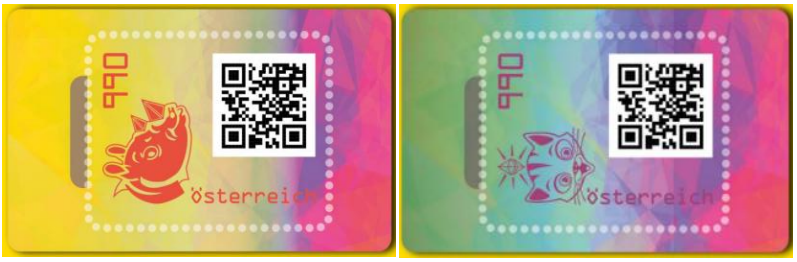
podkategoria Code[1]	Liczba [szt.]	Procent w nakładzie [%]
same litery	9 578	6,385 %
w tym: małe i wielkie litery	8 792	5,861 %
w tym: tylko wielkie litery	394	0,263 %
w tym: tylko małe litery	392	0,261 %
Same cyfry (1-9)	15	0,010 %
Palindromy	8	0,005 %

Prawdziwą perełką dla notafilistów są natomiast palindromy i tutaj kryptofilateliści również mają na co polować, choć tego szczęścia dostąpią jedynie nieliczni, bo typowych sekwencji palindromowych jest zaledwie 8 szt. w całym nakładzie CS 1.0 „Jednorożec" (tabela 3.). Ciekawostką jest palindrom 11G11 (*tokenID* 50 460): jego dwie początkowe jedynki to ślad zerowych bajtów, bo samo kodowanie Base58 dałoby trzyznakowy zapis G11. Swoją palindromiczność zawdzięcza zatem wyłącznie konwencji jedynek wiodących.

tab. 3. Zestawienie wszystkich unikalnych sekwencji palidromowych w nakładzie CS 1.0 „Jednorożec" wydanego przez Österreichische Post.

numer seryjny/tokenID	PALINDROMY Code[1]
6810	mUfUm
31713	pSmSp
47820	HK7KH
50460	11G11
92182	3ySy3
123860	MmTmM
127995	tuDut
138671	QjWjQ

tab. 4. Zakres numerów seryjnych dla wydań oficjalnych austriackiego Crypto Stamp 1.0 do 4.0 wydanych przez Österreichische Post.

Emisja	Zakres numerów seryjnych	Uwagi
CS1.0 Jednorożec 	0 – 149 999	Austria 2019, adres kontraktu na sieci ETH: 0x7e789e2dd1340971de0a9bca35b14ac0939aa330
CS2.0 Pieseł, Borsuk miodowy, Llama, Panda 	150 000 – 389 999	Austria, 2020 (luka 1 000 za serią), kolekcja na dwóch sieciach: Gnosis: 0x143e0e54695e7eb13571b019f87e927c1098066c oraz ETH: 0xa7f87e8d193e29bf1ed050fdd511b79fe0264d8b
CS3.0 Wieloryb 	391 000 – 490 999	Austria, 2021, kolekcja na dwóch sieciach: Gnosis: 0x5550f0d022f706d03ad25a72c477684d3416193f oraz ETH: 0xe38251813b08c2c048b0582a52501aca5df0baab
CS3.1 Kot, Nosorożec 	491 000 – 630 999	Austria, 2021 (luka 2 000 za serią), kolekcja na dwóch sieciach: Gnosis 0x3151B7Dd9F6e806D2709153765925c373af47089 oraz ETH: 0x6f906b03d5afda15118bc0029a4e9c31921e9072
CS4.0 Byk 	633 000 – 732 999	Austria, 2022, kolekcja na sieci Polygon: 0xd46ed1d0eaf1b633e698d2ce7e025ba0f5edacbb

Jak wcześniej wspominaliśmy system kodowania Code[1] został opracowany w taki sposób, by globalnie odnosić się zarówno do opisywanej w niniejszym opracowaniu serii *CS 1.0* „Jednorożec" ale również i do kolejnych serii emitowanych przez *Österreichische Post*. Dla przykładu prezentujemy zakresy numerów seryjnych dla edycji austriackiego

kryptoznaczka, który zostały wyemitowane później (tab. 4.). W trzech bajtach numeru seryjnego można zakodować aż 16 777 216 numerów seryjnych, więc tabela ta jest i jeszcze długo będzie rozbudowywana. Najnowszą kolekcją główną jest aktualnie *Crypto Stamp 5.0–5.3*, a w tej tabeli mają również swoje miejsce emisje łączone i emisje specjalne. Osoby zaciekawione tematem zapraszamy na stronę www.pzkf.pl, gdzie opublikowaliśmy obszerne zestawienia statystyczne oraz kalkulatory do przeliczania numeru seryjnego na Code[1] dla emisji sygnowanych przez *Österreichische Post.* Wierzymy, że narzędzie to będzie bardzo użyteczne dla wszystkich kryptofilatelistów. Globalna numeracja kryje jeszcze jedną niespodziankę: pula numerów seryjnych nie jest wyłącznie austriacka. Bezpośrednio za CS 4.0 (kończącym się na numerze 732 999) rozpoczyna się emisja holenderska NL Crypto Stamp (zakres od 733 000 do 872 999), w luce między CS 5.1 a CS 5.2 rezyduje kryptoznaczek Poczty Luksemburskiej (od 1 118 000), a tuż za CS 5.2 belgijski (od 1 320 000). Österreichische Post prowadzi zatem jeden wspólny rejestr numeracyjny dla emisji czterech europejskich poczt, a granice między nimi widać w samych kodach.

Warto podkreślić, że w drobiazgowym opisaniu strukturalnej różnorodności Code[1] niezmiernie pomocne było wcześniejsze wykonanie wstecznej inżynierii samego algorytmu, które od czterech miesięcy jest dostępne publicznie na stronie https://bindaro.io/pl/, jako dodatkowe funkcje dla kolekcjonerów austriackich kryptoznaczków. Polecamy uwadze ten serwis kryptofilatelistyczny.

Analiza matematyczna algorytmu generowania Code[1] obnaża cechę tej architektury, a tym samym redefiniuje pojęcie bezpieczeństwa na rynku wtórnym. Obecny schemat ma bowiem pewną wadę: jest w pełni przewidywalny, a przez to podrabialny. Algorytm jest jawny, przez co każdy może wygenerować poprawny kod dla dowolnego *tokenID*. W ramach prac badawczych z powodzeniem zrobiliśmy to dla miliona sztuk, wliczając w to emisje, które jeszcze nie opuściły drukarni. Zastosowana tu 1-bajtowa suma kontrolna chroni wyłącznie przed ludzką literówką przy wpisywaniu znaków Base58, nie stanowiąc zapory przed fałszerzem. Ryzyko to materializuje się, gdy rynek wtórny sztucznie rozdziela formułę phygital*, handlując walorem fizycznym osobno, a cyfrowym NFT osobno. W takim scenariuszu jesteśmy całkowicie podatni na oszustwa. Ratunkiem pozostaje weryfikacja u źródła: dopóki śledzimy tokeny NFT bezpośrednio po oficjalnym adresie kontraktu emitenta na *blockchain*, system zachowuje pełną integralność, a fałszerstwo staje się niemożliwe. Musimy też wymagać komplementarnej pary od sprzedającego, a więc waloru fizycznego i przypisanego do niego NFT. Jak poruszać się bezpiecznie po *blockchain* opisujemy w cyklu „Dobre Praktyki Kryptofilatelistyki" [2].

Niniejsze opracowanie udowadnia, że współczesna kryptofilatelistyka przeniosła punkt ciężkości z klasycznej lupy na grunt inżynierii wstecznej i matematyki stosowanej. Zrozumienie mechanizmów rządzących edycjami *Crypto Stamp 1.0* pozwala na świadome poszukiwanie unikatowych anomalii rynkowych, takich jak opisane w tekście palindromy czy poszukiwane kody 4-znakowe. Udostępnione na stronie www.pzfk.pl kalkulatory i zestawienia statystyczne dają kryptofilatelistom realne narzędzie kontroli nad rzadkością i autentycznością walorów.

Wierzymy, że udostępnione przez nas rozwiązania znajdą szerokie zastosowanie praktyczne w codziennych realiach rynkowych oraz ułatwią kolekcjonerom sprawne systematyzowanie i katalogowanie swoich cyfrowo-fizycznych zbiorów.

**Phigital* to komplementarne połączenie przedmiotu fizycznego (*physical*) z jego cyfrowym bliźniakiem (*digital*) na blockchainie w jeden naddany walor kolekcjonerski

1. Fedorczyk B., Tyszka D., Pierwszy na świecie kryptoznaczek. Kryptograficzny „Jednorożec" jako fundament cyfrowej filatelistyki, Filatel.pl, nr 6/2026, s. 596-598
2. Fedorczyk B., Lech G., Dobre praktyki kryptofilatelistyki (1), Filatel.pl, nr 8/2026, s. 589-591

Bartłomiej Fedorczyk, Dariusz Tyszka

Digital Anatomy of the Austrian Crypto Stamp 1.0 Code. Cryptographic Features and Item Pairing Secrets

This article is dedicated to advanced crypto philatelists who pay close attention to details related to serial numbers and the specificities of pairing a physical item with its complementary NFT, which manifests in various technical features accompanying the issuance of the Austrian CS 1.0 (Crypto Stamp 1.0). This is a research study based on mapping the entire print run of this series, and it will be particularly useful for those collectors who are considering purchasing an item from the secondary market. In such situations, the seller often posts a photograph of the item offered, displaying the Code[1] (Fig. 1). Each of the three presented items has already revealed one variant out of the five available NFT colors [1]. Admittedly, scanning the QR code allows a preview of the specific color variant, but it is impossible to determine the item's serial number within the total print run from that level alone. There is a vast number of crypto philatelists for whom the serial number data represents a significant characteristic defining a given collectible item. Our study provides an understanding of the pairing mechanism behind the Austrian crypto stamp issues and enables the independent verification of the actual status of a given item. Armed with this knowledge, a crypto philatelist can organize their collection in an informed manner and select their preferred path to philatelic fulfillment.

Contemporary crypto philately, representing a natural stage in the evolution of traditional collecting in the era of Web 3.0 solutions, redefines the concepts of uniqueness and authenticity of a philatelic item. The classical examination of paper structure, color shade analysis using color guides, and perforation verification are augmented by an advanced mathematical and cryptographic apparatus. Understanding the system of pairing a physical item with its complementary NFT is crucial for the advanced crypto item collector, as it allows for secure navigation within the modern market and the informed cultivation of collections with a high degree of rarity. In this study, the operational mechanism of the pairing system has been comprehensively described; it is the first study of its kind in the world that extrapolates to all issued Austrian crypto stamp editions, as well as certain joint issues, such as Austria-Netherlands, etc. The operating principle of the system remains identical from issue to issue. This study provides invaluable knowledge for collectors of the most recognizable crypto stamp series issued by the Austrian Post (Österreichische Post), a pioneer in its field with an established position on the global market.

When holding a traditional polymer (PVC) Crypto Stamp 1.0 souvenir sheet, one's attention is drawn to a unique graphical element printed directly onto the physical item—namely, a mysterious alphanumeric string designated in the issuance nomenclature as Code[1] (Fig. 1). To the untrained eye, this is merely a sequence of random characters. In reality, this inconspicuous inscription functions as a fundamental bridge between two worlds, serving as a strictly defined ordinal code whose task is the flawless, deterministic pairing of the physical souvenir sheet with its complementary digital twin (NFT) recorded within the distributed structure of the blockchain.

Only upon delving into the metadata of this digital token (NFT) do we discover the unique tokenID value, which serves as the serial number corresponding to the precise position of the given specimen within the total print run. This serial number is represented in the database as a decimal (DEC) value. This constitutes a particular technological peculiarity, as issuers conventionally print serial numbers directly onto the philatelic item, whereas here we are presented solely with Code[1]. A meticulous analysis of the entire population of 150,000 such pairs (from tokenID 0 to 149,999, as these were the serial numbers assigned to the CS 1.0 stamps) reveals a fascinating mathematical discipline, algorithmic anomalies, and hidden regularities that provide an exciting field of archival inquiry and research for the advanced collector.

fig. 1. Screenshots of assets listed for sale on the Delcampe.net auction portal. As of June 4th, 2026. Each item has its scratch off layer intact and is in MHN condition, which in traditional philately implies cancellation but in crypto philately does not necessarily mean that the NFT has not been determined and revealed. The Code[1] is visible in the field marked as [1].

In order to fully comprehend the technical dimension of this process, it is necessary to explain the hexadecimal (base-16) numeral system, which is universally utilized in computer science and cryptography. This is a positional numeral system with a base of 16. In contrast to the conventional decimal system used in daily life, which employs ten digits (from 0 to 9), the hexadecimal system requires sixteen characters to represent values. Standard digits are used to denote numbers from 0 to 9, whereas the first letters of the Latin alphabet are introduced for values from 10 to 15: A represents 10, B denotes 11, C signifies 12, D equals 13, E stands for 14, and F corresponds to the value 15. The application of the hexadecimal system allows for a significantly more compact and machine-readable representation of binary data, wherein one byte of information (eight bits) can always be expressed using precisely two hexadecimal (HEX) characters.

The process of calculating the short alphanumeric code (Code[1], which is the value designated as [1] on the crypto stamp souvenir sheet in Fig. 1) from the decimal serial number (DEC) is based on a structure closely resembling the generation of Bitcoin network addresses. The algorithm fulfills two primary objectives: minimizing the data string length printed on the physical item and providing effective protection against human error (typos) during manual transcription, thanks to a built-in checksum (with an error detection rate of 99.6%). This procedure consists of four precise mathematical and cryptographic steps (Fig. 2):

Step 1: Binary alignment of the serial number (3 bytes).

The input serial number in decimal notation (DEC) is converted into the aforementioned hexadecimal system (HEX). In order to standardize the data structure regardless of the magnitude of the number, the result is padded with leading zeros from the left to a fixed length of 3 bytes (which corresponds to exactly 6 HEX characters).

Step 2: Generation of the checksum (Cryptographic SHA-256 hash).

The generated 3 raw bytes of data (treated as a binary sequence rather than ASCII text) are subjected to one-way hashing using the SHA-256 algorithm. From the resulting full 32-byte hash, only the first byte is extracted (the first two HEX characters indicated in red), which functions as a unique checksum.

Step 3: Data concatenation.

The physical joining of the components takes place. The calculated checksum byte is appended directly before the 3 bytes of the serial number, creating a cohesive data block with a fixed length of 4 bytes (8 HEX characters).

Step 4: Base conversion and Base58 encoding.

The resulting 4-byte HEX sequence is interpreted as a single large integer in the decimal system, upon which a mathematical operation is performed to convert the base from the decimal system to the Base58 system. This process

utilizes the official Bitcoin alphabet: 123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz. This alphabet deliberately eliminates the characters 0, O, I, and l to prevent visual confusion when reading the code from the physical souvenir sheet. If the first byte in this step is a zero byte [00], leading ones are prepended during the Base58 encoding. For example, for serial number 454, the full data block is 0x[00][00][01][C6]meaning there are two leading zero bytes at the beginning, for which leading ones are prepended in Code[1], resulting in the 4-character code 118q (Fig. 2).

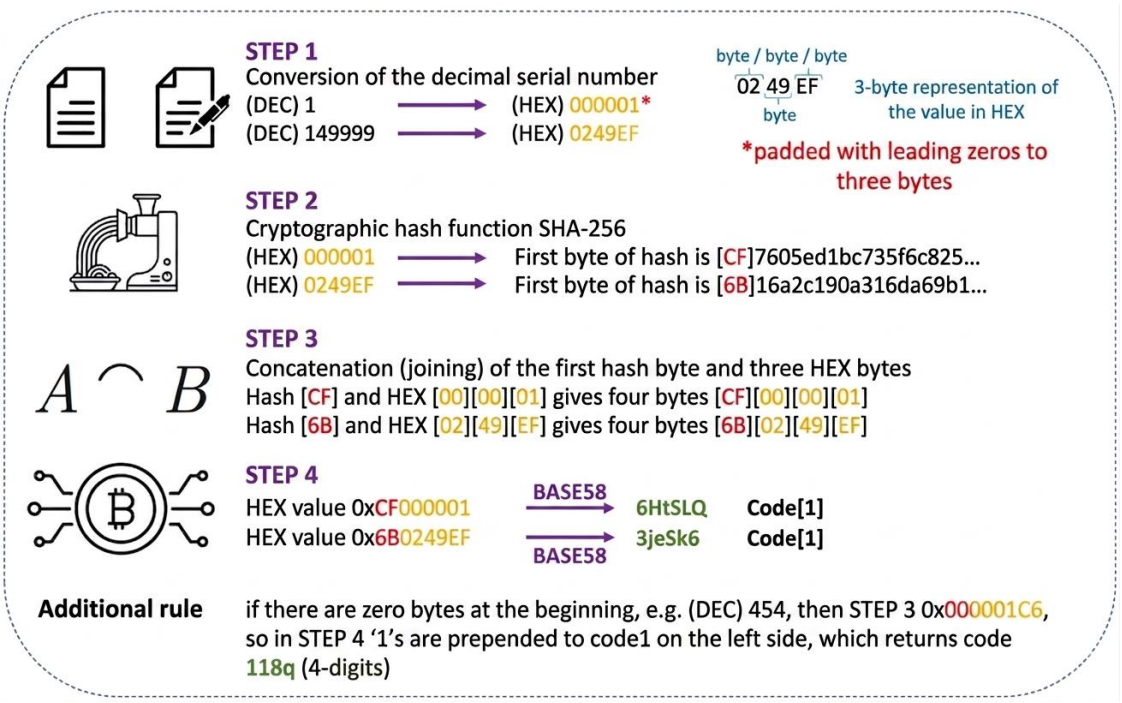


fig. 2. The mechanism for pairing the serial number of a crypto asset issued by Austrian Post. For CS 1.0 'Unicorn', the serial numbers fall within the range of 0 to 149,999. Subsequent releases maintain this continuity, meaning CS 2.0 begins at 150,000. Consequently, a range from 0 to 16,777,216 can be encoded within the three bytes allocated for the serial number.

The true foundation of the crypto philatelic architecture and the primary object of desire for collectors is the character length of the printed code. Although the 4-byte input block possesses a fixed structure, the mathematical conversion into the Base58 notation system causes the algorithm responsible for generating Code[1] for individual tokenID values to operate in a highly functional manner, differentiating the length of the final string.

The majority of physical souvenir sheets pair with a 6-digit Code[1]. These constitute the issuance standard, a prime example of which is the code 3ajkTs assigned to the very low tokenID 2 from the beginning of the run, the code 4RfhoC linked to tokenID 70759 from the middle, or even the code 3jeSk6 closing out the global registry, coupled with tokenID 149999 at the very end of the series.

Note on nomenclature: It is worth noting that the issuers themselves conventionally refer to this string as a "6-digit" code. While this has become the accepted terminology within the crypto philatelic community, it is technically a misnomer, as the Base58 string consists of both letters and numbers (alphanumeric characters) rather than numerical digits alone.

The second most populous group consists of 5-digit codes. Their distribution within the metadata is remarkably vast; we find them at the very beginning of the issue in the form of the code nxcjr linked to tokenID 9, in the middle of the run as the code SD51n at tokenID 54573, and also under the guise of the code wsJzL assigned near the end of the collection to tokenID 149905.

Relatively rare are the 4-digit codes, which are highly sought after by collectors. Their population across the entire print run is remarkably low, amounting to a mere 356 pieces out of 150,000 (Table 1). The distribution of these 356 four-

digit codes within the print run is by no means random. The code shrinks to just four characters only when the SHA-256 checksum yields zero (a 1 in 256 chance) and the serial number falls into one of two specific intervals. Hence, they occur within two disjoint bands: 13 pieces located between tokenID 454 and 2981, and 343 pieces above tokenID 65,752. Between these two bands, a 4-digit code mathematically cannot occur.

tab. 1. Breakdown of Code[1] categories within the entire print run of CS 1.0 'Unicorn' issued by Österreichische Post.

Code[1] Category	Quantity [pcs.]	Percentage of Print Run [%]
6-digit codes	126,476	84.3 %
5-digit codes	23,168	15.4 %
4-digit codes	356	0.2 %
Total print run	150,000	

When we delve deeper into the mapped alphanumeric structure of all Code[1] records, we uncover cases with intriguing characteristics that, due to their uniqueness, also attract significant interest among crypto philatelists. A certain influence from the field of notaphily (the study and collection of paper currency) becomes apparent here, as striking serial numbers are traditionally the collecting domain of those who gather banknotes and various treasury notes. The cross-section of diverse Code[1] categories across the entire CS 1.0 'Unicorn' population is quite substantial. In addition to the aforementioned codes varying in character length, there are instances where the code consists entirely of letters or entirely of digits. Furthermore, certain codes feature exclusively uppercase letters or exclusively lowercase letters (Table 2).

tab. 2. Breakdown of rare Code[1] subcategories within the entire print run of CS 1.0 'Unicorn' issued by Österreichische Post.

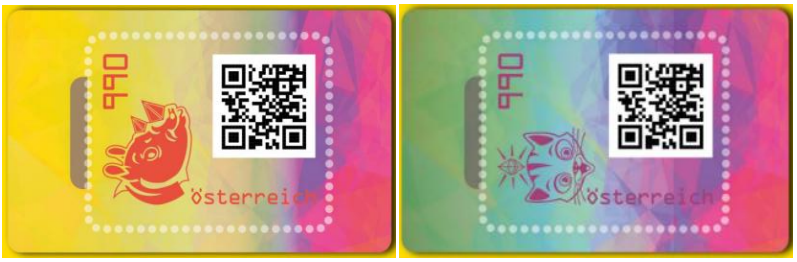
Code[1] Subcategory	Quantity [pcs.]	Percentage of Print Run [%]
Letters only	9,578	6.385 %
including mixed case letters	8,792	5.861 %
including uppercase letters only	394	0.263 %
including lowercase letters only	392	0.261 %
Digits only (1 to 9)	15	0.010 %
Palindromes	8	0.005 %

A true gem for notaphilists however is palindromes, and here too crypto philatelists have something extraordinary to hunt for though this fortune is granted only to a few, as there are a mere 8 classic palindromic sequences in the entire CS 1.0 'Unicorn' print run (Table 3). An intriguing curiosity is the palindrome 11G11 (tokenID 50,460): its two initial ones are the footprint of zero bytes, since the Base58 encoding itself would have yielded the three character string G11. Its palindromic nature is therefore owed entirely to the convention of leading 1.

tab. 3. Breakdown of all unique palindromic sequences within the print run of CS 1.0 'Unicorn' issued by Österreichische Post.

Serial number/tokenID	Palindromes Code[1]
6810	mUfUm
31713	pSmSp
47820	HK7KH
50460	11G11
92182	3ySy3
123860	MmTmM
127995	tuDut
138671	QjWjQ

tab. 4. Serial number ranges for the official editions of the Austrian Crypto Stamp 1.0 to 4.0 issued by Österreichische Post.

Crypto stamp issuance	Serial numbers range	Remarks
CS1.0 Unicorn 	0 – 149 999	Austria 2019, contract address on the ETH network: 0x7e789e2dd1340971de0a9bca35b14ac0939aa330
CS2.0 Doge, Honey Badger, Llama, Panda 	150 000 – 389 999	Austria, 2020 (a gap of 1,000 per series), collection on two networks: Gnosis: 0x143e0e54695e7eb13571b019f87e927c1098066c and ETH: 0xa7f87e8d193e29bf1ed050fdd511b79fe0264d8b
CS3.0 Whale 	391 000 – 490 999	Austria, 2021, collection on two networks: Gnosis: 0x5550f0d022f706d03ad25a72c477684d3416193f and ETH: 0xe38251813b08c2c048b0582a52501aca5df0baab
CS3.1 Cat, Rhino 	491 000 – 630 999	Austria, 2021 (a gap of 2,000 per series), collection on two networks: Gnosis: 0x3151B7Dd9F6e806D2709153765925c373af47089 and ETH: 0x6f906b03d5afda15118bc0029a4e9c31921e9072
CS4.0 Bull 	633 000 – 732 999	Austria, 2022, collection on the Polygon network: 0xd46ed1d0eaf1b633e698d2ce7e025ba0f5edacbb

As previously mentioned, the Code[1] encoding system was designed to apply globally, encompassing not only the CS 1.0 'Unicorn' series described in this study but also subsequent series issued by Österreichische Post. As an example, we present the serial number ranges for the Austrian crypto stamp editions that were released later (Table 4).

A total of 16,777,216 serial numbers can be encoded within the three bytes allocated for the serial number, which means this table is continuously expanding and will be for a long time to come. The latest main collection is currently Crypto Stamp 5.0–5.3, and joint issues as well as special editions also have their place in this table. Anyone interested in the topic is welcome to visit the website www.pzkf.pl, where we have published extensive statistical compilations and calculators for converting serial numbers into Code[1] for issues signed by Österreichische Post. We trust that this tool will prove highly useful for all crypto philatelists. The global numbering scheme holds yet another surprise: the serial number pool is not exclusively Austrian. Directly after CS 4.0 (which ends at number 732,999), the Dutch NL Crypto Stamp issue begins (ranging from 733,000 to 872,999). In the gap between CS 5.1 and CS 5.2 resides the crypto stamp of the Luxembourg Post (starting from 1,118,000), and right after CS 5.2 comes the Belgian one (starting from 1,320,000). Österreichische Post therefore maintains a single shared registry for the issues of four European postal administrations, and the boundaries between them are clearly visible within the codes themselves.

It is worth highlighting that in meticulously describing the structural diversity of Code[1], the prior reverse engineering of the algorithm itself was immensely helpful. This has been publicly available for four months on the website https://bindaro.io/pl/ as additional features for collectors of Austrian crypto stamps. We highly recommend this crypto philatelic service to your attention.

A mathematical analysis of the Code[1] generation algorithm exposes a defining characteristic of this architecture, thereby redefining the concept of security on the secondary market. The current scheme possesses a vulnerability: it is fully predictable, and consequently, forgeable. The algorithm is open, meaning anyone can generate the correct code for any given tokenID. As part of our research, we successfully did this for a million pieces, including issues that have not even left the printing house yet. The 1-byte checksum utilized here serves solely to prevent human typos when entering Base58 characters, offering no barrier against a counterfeiter. This risk materializes when the secondary market artificially splits the phygital* formula, trading the physical item separately from the digital NFT. In such a scenario, we are completely susceptible to fraud. The only salvation lies in verification at the source: as long as we track the NFTs directly via the issuer's official contract address on the blockchain, the system retains full integrity, and forgery becomes impossible. We must also demand a complementary pair from the seller, meaning both the physical asset and its assigned NFT. How to navigate the blockchain safely is described in our series 'Good Practices of Crypto Philately' [2]

This study proves that modern crypto philately has shifted its focal point from the classic magnifying glass onto the ground of reverse engineering and applied mathematics. Understanding the mechanisms governing the Crypto Stamp 1.0 editions allows for an informed pursuit of unique market anomalies, such as the palindromes or the highly sought after 4-digit codes described in this text. The calculators and statistical compilations made available on the www.pzkf.pl website provide crypto philatelists with a tangible tool to control both the rarity and the authenticity of these collectibles.

We believe that the solutions we have shared will find wide practical application in everyday market realities and will make it easier for collectors to efficiently systemize and catalogue their digital physical collections.

* *Phygital* is a complementary combination of a physical object and its digital twin on the blockchain into a single, enhanced collectible asset.

1. Fedorczyk B., Tyszka D., Pierwszy na świecie kryptoznaczek. Kryptograficzny „Jednorożec" jako fundament cyfrowej filatelistyki, Filatel.pl, no. 6/2026, s. 596-598
2. Fedorczyk B., Lech G., Dobre praktyki kryptofilatelistyki (1), Filatel.pl, no. 8/2026, s. 589-591