INFORMATYKA ŚLEDCZA
I CYBERPRZESTĘPCZOŚĆ

WYBRANE ZAGADNIENIA W UJĘCIU POLICYJNYM

POD REDAKCJĄ
PAWŁA OLBERA

SZCZYTNO 2022

Recenzenci
dr hab. Wojciech Filipkowski, prof. UwB
dr hab. inż. Jerzy Kosiński

Redakcja Wydawcy
Beata Miszczuk
Adam Rogala

Projekt okładki
Agnieszka Kamińska

ISBN 978-83-7462-816-7
e-ISBN 978-83-7462-817-4

Druk i oprawa:
Dział Wydawnictw i Poligrafii Wyższej Szkoły Policji w Szczytnie
ul. Marszałka Józefa Piłsudskiego 111, 12–100 Szczytno
tel. 47 733 5410
e-mail: wwip@wspol.edu.pl
Objętość: 7,52 ark. wyd.

SPIS TREŚCI

Wstęp

Cyberprzestępczość stanowi jedno z wyzwań współczesnego świata, a jej złożony charakter potęguje rosnące zaangażowanie grup przestępczych. Wielopłaszczyznowy wymiar cyberprzestępczości oraz jej skala wynikają przede wszystkim z braku granic w świecie wirtualnym oraz zdolności cyberprzestępców do skutecznego przewidywania zachowań użytkowników sieci Internet i technologii informatycznych. Cyberprzestępczość przybiera różne formy, do których zaliczyć można wykorzystanie złośliwego oprogramowania, kradzież danych osobowych, rozpowszechnianie nielegalnych treści czy też sprzedaż nielegalnych towarów i usług.

Niewątpliwie działania cyberprzestępcze zostały spotęgowane w 2020 r., kiedy to okoliczności spowodowane pandemią COVID-19 wymusiły zmianę stylu życia i przeniesienie aktywności wielu użytkowników do sieci Internet. Z raportu rocznego CERT Polska wynika, że w 2020 r. zarejestrowano 10 420 incydentów cyberbezpieczeństwa, co stanowi wzrost o ok. 60% w porównaniu do roku ubiegłego. Najpopularniejszym typem incydentu był phishing, który stanowił 73% wszystkich obsłużonych incydentów. Przeprowadzone kampanie phishingowe miały na celu uzyskanie m.in. danych dostępowych do kont portali społecznościowych oraz serwisów bankowości internetowej. W 2020 r. odnotowano także serię incydentów związanych z wyciekami danych, spośród których znaczna część dotyczyła infrastruktury polskich uczelni oraz instytucji międzynarodowych[1].

Z kolei na arenie europejskiej zidentyfikowano 10 głównych kategorii zagrożeń, wśród których znajdują się zaawansowane ataki sieciowe (w tym ukierunkowane na usługi chmur obliczeniowych), kradzież danych czy też wykorzystanie złośliwego oprogramowania. Liczba zaawansowanych ataków sieciowych na instytucje, organy i agencje unijne wzrosła w 2020 r. o 60% w porównaniu do 2019 r.[2]

Aktywność cyberprzestępcza nie pozostaje jednak bez reakcji, czego przykładem mogą być działania Rady Unii Europejskiej, która przedłużyła do 18 maja 2022 r. obowiązywanie ram sankcji za cyberataki zagrażające Unii Europejskiej lub jej państwom członkowskim. Unia Europejska podejmuje także wiele innych

---

[1] CERT Polska, *Krajobraz bezpieczeństwa polskiego internetu w 2020 roku*, s. 13, <https://cert.pl/uploads/docs/Raport_CP_2020.pdf>, dostęp: 15 listopada 2021 r.

[2] CERT-EU, *Threat landscape report,* s. 3, <https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf>, dostęp: 15 listopada 2021 r.

działań, które stanowią bezpośrednią odpowiedź na istniejące cyberzagrożenia. W kwietniu 2019 r. UE przyjęła nowe przepisy o zwalczaniu oszustw związanych z płatnościami bezgotówkowymi, które zagrażają bezpieczeństwu UE i zapewniają znaczne dochody zorganizowanym grupom przestępczym. Unia Europejska pracuje także nad przepisami, które ułatwią i przyśpieszą transgraniczny dostęp do dowodów elektronicznych. Organy ścigania i wymiaru sprawiedliwości w coraz większym stopniu polegają bowiem na elektronicznym materiale dowodowym[3].

Przedstawione powyżej zagadnienia znajdują się również w kręgu zainteresowań pracowników i funkcjonariuszy Policji, dzięki którym powstała niezwykle wartościowa pod względem merytorycznym monografia. Przedstawione Państwu opracowanie zostało przygotowane przez funkcjonariuszy i pracowników Policji, posiadających bogate doświadczenie zawodowe w zakresie zwalczania cyberprzestępczości oraz realizacji kryminalistycznych badań informatycznych. To właśnie praktyczny wymiar przedmiotowej publikacji zasługuje na szczególną uwagę. Stanowi ona cenne źródło wiedzy na temat wybranych zagadnień dotyczących cyberprzestępczości oraz informatyki śledczej, pochodzącej bezpośrednio od praktyków, którzy zazwyczaj „dość niechętnie dzielą się wiedzą i swoimi metodami pracy"[4]. Istniejący stan rzeczy wynika z pewnością z faktu, że wiedza wspomnianych osób jest unikalna, bardzo często zgromadzona na podstawie własnych doświadczeń zawodowych.

Pierwsza część monografii zawiera publikacje, które są powiązane tematycznie z informatyką śledczą. Poszczególne prace odnoszą się do cyfrowych śladów aktywności przestępczej, które zapisywane są w pamięci różnych urządzeń i jednocześnie mogą znajdować się w odległych lokalizacjach. Do wspomnianych źródeł danych informatycznych zaliczyć można chociażby koparki kryptowalut, które mają coraz większe znaczenie w działalności przestępczej. Na uwagę zasługują także potencjalne ślady przechowywane w środowisku sieciowym, które (ze względu na słabe zabezpieczenia) stają się coraz częściej bezpośrednim celem zdalnych ataków, prowadzących ostatecznie do kradzieży danych i środków finansowych. W monografii zwrócono także uwagę na problematykę odzyskiwania danych z pamięci przenośnych flash, które często badane są przez biegłych z policyjnych laboratoriów kryminalistycznych oraz problematykę gromadzenia dowodów elektronicznych zlokalizowanych w środowisku chmury obliczeniowej.

Druga część monografii poświęcona została wybranym aspektom zwalczania cyberprzestępczości. W tej części opracowania umieszczone zostały publikacje dotyczące bezpieczeństwa technologii biometrycznych oraz bezpłatnych narzędzi informatycznych wspierających zwalczanie cyberprzestępczości. Zapotrzebowanie

[3] Rada Europejska, Rada Unii Europejskiej, *Cyberbezpieczeństwo: jak UE radzi sobie z cyberzagrożeniami,* <https://www.consilium.europa.eu/pl/policies/cybersecurity/>, dostęp: 15 listopada 2021 r.

[4] W.A. Kasprzak, *Ślady cyfrowe. Studium prawno-kryminalistyczne,* Warszawa 2015, s. 126.

na aktualną wiedzę oraz oprogramowanie mogące wspomóc funkcjonariuszy jest bowiem naturalną konsekwencją rozwoju przestępczości z wykorzystaniem narzędzi informatycznych. Powyższe zagadnienia uzupełniają tematy dotyczące znaczenia informacji i transakcji finansowych w skutecznym zwalczaniu cyberprzestępczości.

Wyrażam głęboką nadzieję, że niniejsza monografia dotrze do szerokiego kręgu odbiorców i stanowić będzie cenne źródło wiedzy i jednocześnie, choć w części, wypełni istniejącą lukę literatury z obszaru kryminalistycznych badań informatycznych oraz zwalczania cyberprzestępczości. Przede wszystkim mam nadzieję, że przedmiotowe opracowanie spotka się z przychylnym przyjęciem oraz okaże się pomocne zarówno w procesie edukacji, jak i w codziennej pracy zawodowej.

kom. dr Paweł Olber
Wyższa Szkoła Policji w Szczytnie

Marek Liszkiewicz[1]

Problematyka zabezpieczania koparek kryptowalut

Streszczenie: W opracowaniu przedstawiono zagadnienia związane z postępowaniem przy zabezpieczaniu specjalizowanych komputerów tzw. koparek kryptowalut. Poruszono ponadto problematykę portfeli kryptowalutowych, kluczy kryptograficznych oraz wybranych aspektów badań nośników cyfrowych w sprawach związanych z koparkami kryptowalut.

Słowa kluczowe: kryptowaluty, koparka kryptowalut, bitcoin, zabezpieczanie, dowód cyfrowy, wydobywanie kryptowalut

Wstęp

W obecnych czasach zauważalny jest wzrost zainteresowania rynkiem kryptowalut. Pozyskiwanie „cyfrowego pieniądza" przy wykorzystaniu dedykowanych komputerów staje się coraz bardziej powszechniejsze. Zjawisko to samo w sobie nie nosi znamion czynu zabronionego, nie jest też bezpośrednio w żaden sposób powiązane z zachowaniami kryminogennymi. Jednakże jedna z cech kryptowalut, tj. anonimowość posiadacza i transakcji, powodują, że są one niejednokrotnie wykorzystywane do lokowania środków finansowych pochodzących z szeroko rozumianych przestępstw.

Ze względu na dynamiczny rozwój walut wirtualnych przypuszczać można, że realizacja czynności procesowych i techniczno-kryminalistycznych związanych z zabezpieczaniem tzw. „koparek kryptowalut" będzie najprawdopodobniej odgrywać coraz większą rolę w pracy certyfikowanych specjalistów i biegłych policyjnych laboratoriów kryminalistycznych Policji zajmujących się dowodami cyfrowymi. Wobec braku wytycznych lub też sprecyzowanych procedur, specjaliści i biegli mogą napotkać problemy związane z zabezpieczaniem nietypowego sprzętu, jakim są z pewnością „koparki kryptowalut". Przy bliższym spojrzeniu na taki sprzęt i sprawdzeniu działającego na nim oprogramowania, okazuje się jednak, że sama

[1] Marek Liszkiewicz — podkom., specjalista Laboratorium Kryminalistycznego Komendy Wojewódzkiej Policji w Krakowie, biegły z zakresu kryminalistycznych badań informatycznych. Zainteresowania naukowe i zawodowe koncentrują się wokół informatyki śledczej, w szczególności zaś badań dowodów cyfrowych oraz zagadnień związanych z technicznymi aspektami zabezpieczania danych informatycznych. Ponadto zainteresowania autora obejmują tworzenie aplikacji webowych przy użyciu języków skryptowych JavaScript, PHP, Python. Kontakt z autorem za pośrednictwem redakcji.

procedura zabezpieczania nie różni się zbytnio od procedur zabezpieczania standardowych nośników informatycznych. Ewentualnym dodatkowym elementem są sprzętowe portfele kryptowalutowe.

Pojęcie kryptowaluty

W literaturze przedmiotu równolegle funkcjonują trzy terminy: „kryptowaluta" (ang. *cryptocurrency*), „waluta wirtualna" (ang. *virtual cryptocurrency*) oraz „waluta cyfrowa" (ang. *digital currency*). Wszystkie nawiązują do wyrazu „waluta", który jednak ma tutaj bardziej znaczenie umowne, niż formalne dotyczące środka płatniczego w danej jurysdykcji. Pojęcie kryptowaluty po raz pierwszy zdefiniował w 1998 r. Wei Dai, który w pewien wizjonerski sposób przedstawił koncepcję waluty opartej na rozwiązaniach kryptograficznych zastępujących władze centralne i organy odpowiedzialne za emisję pieniądza. Mimo problemu definicyjnego to właśnie kryptograficzna natura jest niewątpliwym wyróżnikiem tych aktywów. Ich użytkowanie opiera się na kryptografii asymetrycznej, a do ich wydobywania wykorzystywane są kryptograficzne funkcje skrótu[2].

Samo pojęcie kryptowaluty nie jest ściśle definiowane w ustawodawstwie polskim. Pojęcie waluty wirtualnej pojawia się jedynie w ustawie z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[3]. Zgodnie z przedmiotową ustawą waluta cyfrowa jest cyfrowym odwzorowaniem wartości, która niej jest:

a) „prawnym środkiem płatniczym emitowanym przez NBP, zagraniczne banki centralne lub inne organy administracji publicznej,
b) międzynarodową jednostką rozrachunkową ustanawianą przez organizację międzynarodową i akceptowaną przez poszczególne kraje należące do tej organizacji lub z nią współpracujące,
c) pieniądzem elektronicznym w rozumieniu ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych,
d) instrumentem finansowym w rozumieniu ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, wekslem lub czekiem" [4].

Jednocześnie przepisy ustawy stanowią, że kryptowaluta jest wymienialna na prawne środki płatnicze i jest akceptowana jako środek wymiany. Może być także przechowywana w sposób elektroniczny lub przeniesiona albo może być przedmiotem handlu elektronicznego[5].

---

[2] P. Rodwald, *Kryptowaluty z perspektywy informatyki śledczej*, Gdynia 2021, s. 14.

[3] Ustawa z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, tekst jedn. DzU z 2021, poz. 1132.

[4] Tamże, art. 2 ust. 2 pkt 26.

[5] Tamże.

Lista i liczba kryptowalut podlegają ciągłym zmianom. Na koniec 2019 r. było ich ponad trzy tysiące. Jedne projekty upadają, inne powstają. Technologia jest już na tyle znana, że stworzenie nowej kryptowaluty nie stanowi większego problemu. Oczywiście, to nie gwarantuje powszechności jej użycia, ani tym bardziej sukcesu. Do najpopularniejszych kryptowalut należą ciągle Bitcoin (BTC) i Ethereum (ETH)[6].

Bitcoin został opracowany i wdrożony w 2009 r. przez osobę bądź grupę osób o pseudonimie Satoshi Nakamoto. Mimo wielu domniemywań związanych z autorem do dziś nie udało się ustalić jego rzeczywistej tożsamości[7].

Twórcą Ethereum jest Vitalik Buterin. W 2011 r. ten siedemnastoletni wówczas Kanadyjczyk rosyjskiego pochodzenia został współzałożycielem i jednym z czołowych autorów czasopisma „Bitcoin Magazine", rozwinął koncept nowej zdecentralizowanej sieci opartej na technologii blockchain (która jednak ma znacznie szersze zastosowanie od sieci Bitcoin) i finalnie w 2013 r. opublikował tzw. białą księgę (ang. *white paper*) Ethereum[8].

Przechowywanie kryptowalut — adresy, portfele, klucze publiczne i prywatne

Kryptowaluty przechowywane są pod adresami, co oznacza, że każda jednostka kryptowaluty, która została już wydobyta, musi przynależeć do konkretnego adresu. Adres to unikalny ciąg alfanumeryczny pozwalający na wysyłanie i odbieranie danej kryptowaluty. Przykład adresu w sieci Bitcoin:

— 0x15gZhgbX1f1JC1ZUxwWBqedXGuTaLaYYdb,

oraz w sieci Ethereum:

— 0xbd7bFfA53283c26151AdbDDc3302ec876a5d11F9.

Adresy nie zawierają żadnej informacji na temat ich właściciela. Każdy użytkownik danej sieci (Bitcoin, Ethereum) może mieć wiele adresów[9]. W przypadku kiedy właściciele sami się nie ujawnią, stanowi to istotny problem w ich identyfikacji. Użytkownicy posiadają więc wysoki poziomi anonimowości, a wykorzystując dodatkowe usługi anonimizujące, są bardzo trudni do identyfikacji[10].

Adres jako ciąg alfanumeryczny może być prezentowany w kilku formatach: zaczynając od dość trudnej w codziennym użytkowaniu notacji alfanumerycznej,

---

[6] GPWInfoSfera, *Ranking kryptowalut — jakie są najpopularniejsze?*, <https://www.gpwinfostrefa.pl/ranking-kryptowalut-jakie-sa-najpopularniejsze-i-dlaczego/>, dostęp: 9 września 2021 r.

[7] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, <https://bitcoin.org/bitcoin.pdf>, dostęp: 10 czerwca 2021 r.

[8] V. Buterin, *A next generation smart contract & decentralized application platform*, <https://whitepaper.io/document/5/ethereum-whitepaper>, dostęp: 10 czerwca 2021 r.

[9] P. Rodwald, *Kryptowaluty z perspektywy…*, wyd. cyt., s. 17.

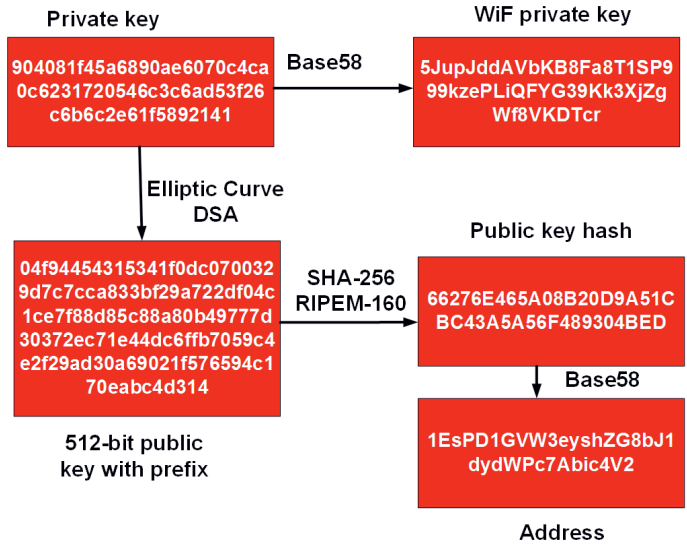
[10] J. Konieczny, R. Prabucki, R. Wielki, *Kryptowaluty. Perspektywa kryminologiczna i kryminalistyczna*, Warszawa 2018, s. 432.

na wygodnych kodach QR (ang. *quick response code*) kończąc. Szukając analogii do adresu w świecie walut fiducjarnych, adres waluty wirtualnej można porównać do numeru rachunku bankowego. Tak jak użytkownik walut fiducjarnych może posiadać wiele kont bankowych z wieloma rachunkami, tak w przypadku kryptowalut użytkownicy mogą dysponować wieloma portfelami, a na każdym z nich może znajdować się wiele adresów. Każda kryptowaluta ma swój sposób generowania adresu z klucza publicznego bądź prywatnego.

Portfelem (ang. *wallet*) nazywa się miejsce przechowywania pary kluczy (wyróżnić można klucz prywatny oraz klucz publiczny), przy czym klucz publiczny nie musi być przechowywany, ponieważ można go wyznaczyć na podstawie klucza prywatnego[11]. Portfel może składać się z wielu adresów.

Klucz publiczny służy do stworzenia adresu w sieci blockchain (odpowiednik adresu email czy numeru konta bankowego). Klucz prywatny zaś służy do podpisywania transakcji. Transakcja to przesłanie środków z jednego konta na drugie. Aby transakcja z danego adresu mogła zostać wykonana, musi zostać podpisana przez odpowiedni klucz prywatny. Za bezpieczne przechowywanie tego klucza prywatnego i wygodne podpisywanie nim transakcji odpowiada użytkownik korzystający z portfela. Przykład generowania par kluczy oraz adresu waluty Bitcoin przedstawiono na rysunku 1.

Rysunek 1. Generowanie par kluczy oraz adresu waluty Bitcoin



Źródło: <https://asecuritysite.com/encryption/bit_keys?__cf_chl_managed_tk__=pmd_0mThnfO6XY_Ae2KScelYn1KfmjfXGP9FPSAMed1hIFk-1632399879-0-gqNtZGzNAvujcnBszQh9/>, dostęp: 17 czerwca 2021 r.

[11] P. Rodwald, *Kryptowaluty z perspektywy…*, wyd. cyt., s. 17.

Z przedstawionego powyżej schematu wynika, że klucz prywatny (ang. *private key*): 904081f45a6890ae6070c4ca0c6231720546c3c6ad53f26c6b6c2e61f5892141 generowany jest jako losowy 256-bitowy ciąg. Utworzony klucz prywatny jest następnie konwertowany za pomocą funkcji Base-58 do postaci klucza WiF (ang. *Wallet Interchange Format*): 5JupJddAVbKB8Fa8T1SP999kzePLiQFYG39Kk3XjZgWf8VKDTcr. Taki format klucza prywatnego jest przechowywany w portfelu.

Przekształcając klucz prywatny algorytmem Elliptic Curve Digital Signature Algorithm (ang. *ECDSA*) otrzymuje się 512-bitowy klucz publiczny w postaci: 04f94454315341f0dc0700329d7c7cca833bf29a722df04c1ce7f88d85c88a80b49777d30372ec71e44dc6ffb7059c4e2f29ad30a69021f576594c170eabc4d314. Funkcja haszująca działająca na kluczu publicznym wyznacza jego funkcję skrótu (ang. *Public Key Hash*): 66276E465A08B20D9A51CBC43A5A56F489304BED. Następnie w wyniku konwersji wartość klucza publicznego za pomocą funkcji Base-58, uzyskuje się adres kryptowaluty 1EsPD1GVW3eyshZG8bJ1dydWPc7Abic4V2, który można porównać do numeru rachunku bankowego. Przechowywanie klucza prywatnego w portfelu jest wystarczające do wyznaczenia klucza publicznego i adresu. Warto dodać, że dla sieci Ethereum adresy tworzone są w inny, nieco prostszy sposób.

Portfele kryptowalutowe

Portfel to miejsce przechowywania par kluczy (prywatnego i publicznego), niewymagające jednak składowania samych adresów, gdyż są one generowane na podstawie klucza publicznego. Niektórzy autorzy rozszerzają definicję portfela o pełną kontrolę znajdujących się na nim środków. W takim ujęciu portfel, poza przechowywaniem kluczy i zarządzaniem nimi, pozwala śledzić stan konta, a także tworzyć i podpisywać transakcje. Wyróżnia się kilka typów portfeli:

— portfel papierowy stanowiący wydruk pary kluczy (prywatny i publiczny);
— portfel sprzętowy będący wyspecjalizowanym urządzeniem najczęściej w postaci klucza USB;
— portfel w postaci aplikacji, będący oprogramowaniem przeznaczonym na konkretną platformę (komputer, smartfon);
— portfel przeglądarkowy, stanowiący udostępniany przez określony podmiot zewnętrzny serwis, do którego obsługi wystarczy przeglądarka internetowa.

Bezpieczeństwo środków przechowywanych na poszczególnych typach portfeli maleje zgodnie z kolejnością, w której zostały przedstawione: największy poziom bezpieczeństwa posiadają portfele papierowe (bądź stalowe), w których klucz prywatny (ewentualnie ziarno) znajduje się tylko na wydrukowanej kartce (stalowej tabliczce) i powinien być znany jedynie jej posiadaczowi. Najniższy poziom bezpieczeństwa posiadają portfele przeglądarkowe, w których klucze prywatne użytkowników przechowywane są na zewnętrznych serwerach[12].

[12] Tamże, s. 131.

Fizyczne monety

Monety fizyczne (ang. *physical coins*) nie spełniają definicji portfela, gdyż znajdują się na nich tylko klucze prywatne. Dostęp do klucza prywatnego jest jednak wystarczający, aby wygenerować na jego podstawie klucz publiczny, a co za tym idzie również adres oraz dysponować środkami znajdującymi się pod tym adresem. Projekty fizycznych kryptowalut, zwłaszcza bitcoinów, nie mieszczą się w głównym nurcie zainteresowań użytkowników kryptowalut. Stanowią raczej ciekawostkę, mają element kolekcjonerski, cechują się pewnymi walorami estetycznymi i należą do zbiorów nielicznej grupy pasjonatów tej formy przechowywania walut internetowych[13].

Tworzenie monet fizycznych ma przede wszystkim na celu zwiększenie rozpoznawalności samych kryptowalut. Wykorzystanie metafory monety sprawia, że zwykłym użytkownikom bardzo łatwo jest je wizualizować i identyfikować jako pieniądze, a po drugie, ich fizyczna natura oznacza, że możemy wykorzystać technologie opracowane na przestrzeni wieków, aby je zabezpieczyć[14]. Przykład waluty wirtualnej w postaci monet fizycznych przedstawiono na rysunku 2.

Rysunek 2. Przykład fizycznych monet waluty wirtualnej

Źródło: <https://en.bitcoin.it/wiki/Casascius_physical_bitcoins>, dostęp: 17 czerwca 2021 r.

Portfele papierowe (stalowe)

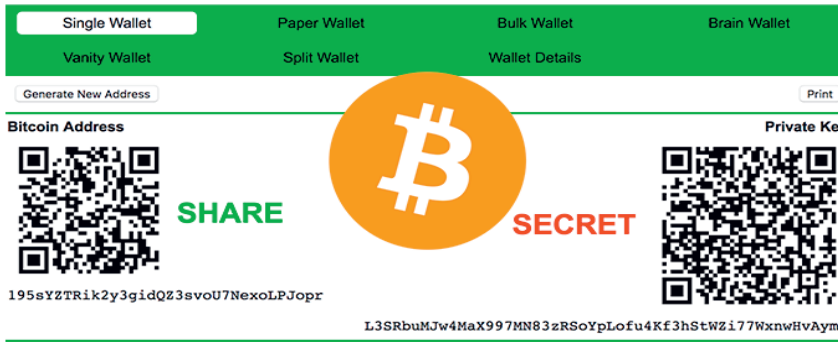
Portfel papierowy (ang. *paper wallet*) to kartka papieru z wydrukowanymi informacjami niezbędnymi do zarządzania portfelem — kluczem prywatnym oraz adresem. Portfele papierowe nie są w pełni funkcjonalne, ponieważ nie możemy za ich pomocą bezpośrednio przesyłać kryptowalut. Portfele takie często zawierają kod QR ułatwiający dokonywanie transakcji (zob. rysunek 3).

Istotną wadą portfeli papierowych jest ich nietrwałość. W razie ewentualnego zniszczenia kartki papieru dostęp do portfela zostaje bezpowrotnie utracony.

[13] Tamże.

[14] A. Femenias-Hermida, C.R. Munteanu, J.M. Vázquez-Naya, *Design and Implementation of a Physical Bitcoin Coin*, „Proceedings 54", nr 21, <https://doi.org/10.3390/proceedings2020054021>, dostęp: 17 czerwca 2021 r.

Rysunek 3. Portfel papierowy

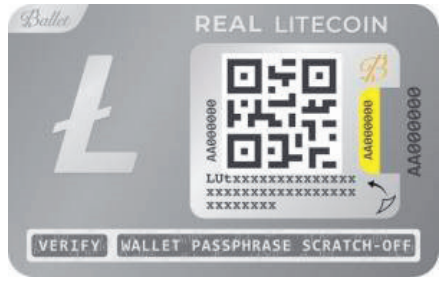


Źródło: opracowano na podstawie strony internetowej <https://block-builders.net/>, dostęp: 18 czerwca 2021 r.

Rozwiązaniem zwiększającym trwałość są nieśmiertelniki, czyli stalowe płytki, na których umieszcza się najczęściej frazę do odzyskiwania dostępu do portfela. Nic nie stoi jednak na przeszkodzie, aby w portfelu takim umieszczać klucz prywatny[15].

Kolejne rozwiązanie portfela papierowego to "Ballet Real Bitcoin", zaprezentowane we wrześniu 2019 r. Jego główną cechą jest to, że klucz prywatny jest generowany na etapie produkcji portfela. Jest to nieelektroniczny portfel w fizycznej postaci, wielkości karty kredytowej, z ukazanym adresem portfela i ukrytym pod specjalną warstwą kluczem prywatnym. Portfel działa na zasadzie magazynu zawierającego klucze prywatne, którego właściciele kryptowalut mogą użyć, aby odblokować swoje portfele online[16] (zob. rysunek 4).

Rysunek 4. Portfel Ballet



Źródło: J. Walewski, *Ballet: twórca pierwszej chińskiej giełdy kryptowalut wraca na rynek z nowym pomysłem,* <https://comparic.pl/tworca-pierwszej-chinskiej-gieldy-kryptowalut-wraca-na-rynek-z-nowym-pomyslem/>, dostęp: 18 czerwca 2021 r.

[15] P. Rodwald, *Kryptowaluty z perspektywy…*, wyd. cyt., s. 134.

[16] J. Walewski, *Ballet: twórca pierwszej chińskiej giełdy kryptowalut wraca na rynek z nowym pomysłem,* <https://comparic.pl/tworca-pierwszej-chinskiej-gieldy-kryptowalut-wraca-na-rynek-z-nowym-pomyslem/>, dostęp: 18 czerwca 2021 r.