KRYPTOWALUTY NA BIURKU

Jak czytać cyfrowe ślady i nie zgubić tropu?

Michał Królik

Akademia Informatyki Śledczej Mediarecovery

Zdj. Mediarecovery

Michał Królik – Crypto Product Area Manager w Mediarecovery – były funkcjonariusz Zarządu w Krakowie Centralnego Biura Zwalczania Cyberprzestępczości. Posiada międzynarodowe certyfikaty (m.in. TRM, Chainalysis, Europol, FBI), a w swojej karierze przeszkolił setki funkcjonariuszy i prokuratorów. Ponadto jest współtwórcą procedur zabezpieczania kryptowalut w Polsce i Europolu. Od 2017 r. kształtuje krajową praktykę analizy *blockchain* i wspiera rozwój kompetencji śledczych. Jest odpowiedzialny za rozwój portfolio produktów do analizy *blockchain* i śledzenia transakcji kryptowalutowych oraz usługi i prowadzenie szkoleń z serii *Kryptowaluty i analiza blockchain* w ramach Akademii Informatyki Śledczej Mediarecovery.

Autor artykułu w przejrzysty sposób przedstawia specyfikę czynności operacyjnych i procesowych, które należy wykonać w sprawach dotyczących przestępstw związanych z wykorzystywaniem kryptowalut. Podkreśla rolę analizy przepływów i zwraca uwagę na zabezpieczanie właściwych śladów w tego typu sprawach. Wskazuje na najczęstsze błędy popełniane przez funkcjonariuszy oraz wyjaśnia ich znaczenie dla prowadzonych postępowań.

Zwykłe przeszukanie i wirtualny sejf: zderzenie z nową rzeczywistością

Szósta rano. Wejście na adres. Klasyczna realizacja u figuranta. Przewracacie mieszkanie do góry nogami. Szukacie gotówki ukrytej w szafkach, rachunków bankowych, wartościowych przedmiotów. I nic. Pusto. Zabezpieczacie telefony i laptopy, technik wpisuje je do protokołu, a wy powoli zbieracie się do wyjścia.

Tymczasem na biurku, tuż obok kluczyków do samochodu, leży niewielkie urządzenie przypominające pendrive, a pod nim zwykła kartka z zapisanymi 24 angielskimi słowami. Dla osoby niewtajemniczonej to bezwartościowe przedmioty. Mijacie je obojętnie.

W rzeczywistości ten „pendrive” (czyli portfel sprzętowy) oraz kartka (tzw. *seed phrase*, czyli fraza odzyskiwania) to klucz do cyfrowego sejfu, w którym sprawca może

przechowywać równowartość setek tysięcy, a czasem milionów złotych. Zostawiając je na miejscu, przechodzicie obok jednego z najważniejszych dowodów w sprawie i majątku, który mógłby zostać zabezpieczony na poczet roszczeń pokrzywdzonych.
Jeszcze kilka lat temu takie znaleziska można było potraktować jako ciekawostkę. Dziś kryptowaluty stały się narzędziem wykorzystywanym w bardzo przyziemnych przestępstwach, od oszustw inwestycyjnych, przez obrót środkami odurzającymi, aż po pranie pieniędzy. Zrozumienie, na co patrzymy w trakcie przeszukania czy analizy materiału dowodowego, przestało być wyborem. Stało się rzemieślniczym obowiązkiem.

Mit pełnej anonimowości. Czym (operacyjnie) jest *blockchain*?

W wielu sprawach, które trafiają na nasze biurka, widać jedno: sprawcy traktują kryptowaluty jak cyfrową, w pełni anonimową gotówkę, niemożliwą do prześledzenia. Co istotne, często my sami również tak o nich myślimy. Gdy w materiałach pojawia się informacja, że środki trafiły na giełdę kryptowalut, łatwo uznać, że dalsze ustalenia będą niemożliwe.
To jeden z najczęstszych błędów na początku postępowania. W praktyce jest dokładnie odwrotnie.
Żeby skutecznie prowadzić tego typu sprawy, warto na chwilę odciąć się od technicznego żargonu. Nie trzeba rozumieć szczegółów kryptografii ani procesu „kopania". Z operacyjnego punktu widzenia blockchain to po prostu publiczny rejestr transakcji, swoista księga rachunkowa dostępna dla każdego.

> Różnica w stosunku do systemu bankowego jest zasadnicza. Przelew bankowy widzi wyłącznie bank, a dostęp do tych danych uzyskujemy dopiero po przeprowadzeniu odpowiednich czynności procesowych. Przelew w *blockchainie* jest widoczny publicznie 24 godziny na dobę, bez konieczności uzyskiwania zgód czy kierowania wniosków. Każda operacja pozostaje tam zapisana w sposób trwały.

Gdzie jest zatem ograniczenie? W tym rejestrze nie ma danych osobowych. Zamiast nazwisk i numerów PESEL widzimy jedynie adresy, czyli ciągi znaków przypisane do portfeli.

> Dlatego podstawowa zasada analizy kryptowalut brzmi: blockchain pokazuje przepływy, nie pokazuje osób.
> Z tego punktu widzenia nie jest to dziedzina zarezerwowana wyłącznie dla specjalistów IT. To w dużej mierze klasyczna praca operacyjna przeniesiona do środowiska cyfrowego: mamy ślad, który należy zabezpieczyć i powiązać z konkretną osobą.

Co faktycznie widać w analizie i… dlaczego nie zawsze ktoś zrobi to za nas?

Kiedy już wiemy, że *blockchain* to jawny rejestr, pojawia się naturalne pytanie: co tak naprawdę w nim widzimy? Nie ma tu efektownych wizualizacji rodem z filmów. Analiza *on-chain* to w praktyce żmudne łączenie kropek.
Widzimy ciągi znaków, czyli adresy (odpowiedniki kont), transakcje (przelewy), powiązania między nimi oraz powtarzalne wzorce zachowań. Możemy prześledzić, jak środki wyłudzone na „pewną inwestycję" trafiają na portfel sprawcy, są dzielone na mniejsze części, przechodzą przez kolejne adresy, a następnie trafiają na konto dużej giełdy kryptowalutowej. I tu pojawia się kluczowy element, jakim jest giełda. To nasz pierwszy realny punkt zaczepienia.
Zanim jednak do tego dojdziemy, warto zwrócić uwagę na pewien schemat myślowy. Gdy w sprawie pojawia się wątek kryptowalut, często pojawia się pokusa, aby przekazać ją w całości do wyspecjalizowanych jednostek.
W rzeczywistości zajmują się one najbardziej złożonymi sprawami, dotyczącymi zorganizowanych grup, zaawansowanej infrastruktury czy działań o dużej skali. Natomiast wiele podstawowych czynności, takich jak zabezpieczenie danych czy wstępne prześledzenie przepływu środków, może zostać wykonanych na poziomie jednostki prowadzącej postępowanie.
To właśnie ten etap często decyduje o powodzeniu dalszych działań. Zabezpieczenie cyfrowego śladu i jego wstępna analiza stają się dziś elementem podstawowego warsztatu.

Gdzie kończy się analiza *on-chain*, czyli operacyjne złoto

Wróćmy do naszego przykładu. Środki po kilku transferach trafiają na giełdę kryptowalutową. Co dzieje się dalej?
W tym miejscu dochodzimy do kluczowego momentu. Zgodnie z zasadą, że *blockchain* pokazuje przepływy, a nie osoby, ślad w publicznym rejestrze kończy się w momencie wejścia środków na scentralizowaną platformę.
Z punktu widzenia analizy *on-chain* oznacza to przerwę. Dalsze operacje nie są już widoczne w *blockchainie*, lecz zapisywane w wewnętrznych systemach giełdy.
I co ważne, to dobra wiadomość.
W tym miejscu kończy się analiza techniczna, a zaczynają się klasyczne czynności procesowe. Większe platformy kryptowalutowe oraz operatorzy usług podlegają regulacjom związanym z przeciwdziałaniem praniu pieniędzy i stosują procedury identyfikacji użytkowników.
Dla prowadzącego sprawę oznacza to możliwość uzyskania konkretnych danych: od informacji identyfikacyjnych, przez historię logowań, po szczegóły aktywności na koncie. W praktyce często pozwala to powiązać adres z konkretną osobą.
Od tego momentu ciężar działań przenosi się na znane obszary: analizę danych, pracę operacyjną, ustalenia osobowe i czynności terenowe. Kluczową rolę zaczyna odgrywać biały wywiad (OSINT – *Open Source Intelligence*). Aktywność w mediach społecznościo-

wych, powiązania z adresami e-mail, wpisy na forach czy ślady pozostawione w innych usługach często pozwalają powiązać adres kryptowalutowy z konkretną osobą lub środowiskiem. W praktyce dopiero połączenie analizy *on-chain* z działaniami poza *blockchainem* obejmującymi m.in. OSINT, dane pozyskane od podmiotów rynku kryptowalutowego oraz klasyczne czynności procesowe i operacyjne, umożliwia pełne odtworzenie przebiegu zdarzeń i identyfikację sprawcy.

Najczęstsze błędy w sprawach z wykorzystaniem kryptowalut

Przejdźmy do praktyki. Gdzie najczęściej popełniane są błędy już na początku postępowania? Z doświadczenia wynika, że powtarzają się trzy podstawowe schematy.

PO PIERWSZE: ZAŁOŻENIE, ŻE „JEDEN ADRES = JEDNA OSOBA".

Często myślimy schematem bankowym: skoro dana osoba ma jedno konto, to w świecie kryptowalut również korzysta z jednego adresu. W rzeczywistości jest inaczej. Nowoczesne portfele automatycznie generują nowe adresy dla kolejnych transakcji.

Błędne powiązanie kilku adresów tylko dlatego, że „wydają się podobne", może prowadzić do połączenia zupełnie niezwiązanych ze sobą wątków i skierowania postępowania na niewłaściwe tory.

PO DRUGIE: NIEUWAGA PODCZAS PRZESZUKANIA.

Wracając do sytuacji ze wstępu, w trakcie realizacji skupiamy się na gotówce, sprzęcie elektronicznym i oczywistych dowodach. Tymczasem kluczowe znaczenie mogą mieć rzeczy niepozorne: kartka z zapisanymi słowami lub niewielkie urządzenie przypominające pendrive.

Fraza odzyskiwania (tzw. *seed phrase*), najczęściej składająca się z 12 lub 24 słów, nie jest zwykłym hasłem. To w praktyce klucz do środków zgromadzonych w portfelu.

Zabezpieczenie samego urządzenia lub komputera nie gwarantuje dostępu do tych środków ani ich ochrony. Jeżeli sprawca posiada kopię frazy lub zapamiętał ją, może odzyskać dostęp do środków na dowolnym urządzeniu.

Dlatego w sprawach związanych z kryptowalutami kluczowe jest nie tylko zabezpieczenie sprzętu, ale również odnalezienie i zabezpieczenie frazy odzyskiwania.

PO TRZECIE: CZAS REAKCJI.

W odróżnieniu od systemu bankowego kryptowaluty funkcjonują bez przerw. Transakcje realizowane są przez całą dobę, niezależnie od dnia tygodnia.

Oznacza to, że środki mogą zostać przeniesione wielokrotnie w bardzo krótkim czasie. Zwłoka w podjęciu działań znacząco zmniejsza szanse na ich prześledzenie lub zabezpieczenie.

Co zabezpieczyć już na etapie zawiadomienia

W wielu sprawach kluczowe informacje znajdują się już po stronie pokrzywdzonego. Problem polega na tym, że często nie są one właściwie zabezpieczane na samym początku postępowania.

Z punktu widzenia analizy kryptowalut szczególne znaczenie mają:

- adres portfela, na który zostały przesłane środki,
- identyfikator transakcji (tzw. TXID),
- data i kwota transferu,
- nazwy wykorzystanych platform (giełd, kantorów),
- korespondencja ze sprawcą (np. komunikatory, e-mail),
- zrzuty ekranu z przebiegu „inwestycji".

Już na podstawie tych danych możliwe jest wstępne prześledzenie przepływu środków i określenie dalszego kierunku czynności.
Brak tych informacji lub ich niepełne zabezpieczenie na początku znacząco utrudnia dalszą analizę, a w niektórych przypadkach może uniemożliwić odtworzenie pełnego przebiegu zdarzeń.
Należy również zwrócić szczególną uwagę na poprawność zapisywanych danych. Adresy portfeli oraz identyfikatory transakcji (TXID) są ciągami znaków, w których nawet pojedyncza literówka lub pominięcie znaku może uniemożliwić ich odnalezienie w systemie. W praktyce oznacza to konieczność ponownego zbierania danych, a w niektórych przypadkach utratę możliwości odtworzenia pełnego przebiegu transferu środków.

Jak działają sprawcy, czyli mechanika z lotu ptaka

Kryptowaluty pojawiają się w różnych rodzajach przestępstw, od obrotu środkami odurzającymi po rozliczenia za nielegalne towary. Obecnie jednak najczęściej wykorzystywane są w oszustwach związanych z fałszywymi inwestycjami.
Sprawcy wykorzystują wizerunki znanych firm, instytucji publicznych lub osób rozpoznawalnych, często posługując się materiałami generowanymi przy użyciu sztucznej

inteligencji. Pokrzywdzony, przekonany o wiarygodności „inwestycji", sam kupuje kryptowaluty na legalnej platformie, a następnie przekazuje je na wskazany adres.
Z perspektywy sprawcy jest to rozwiązanie bardzo wygodne, ponieważ środki omijają tradycyjny system bankowy. Jednocześnie sprawca zdaje sobie sprawę, że przepływy w *blockchainie* są publiczne, dlatego podejmuje działania mające na celu ich ukrycie.

W tym celu wykorzystywane są m.in.:

- giełdy działające bez weryfikacji tożsamości,
- usługi mieszające środki (tzw. miksery),
- przenoszenie środków pomiędzy różnymi sieciami (*chain-hopping*).

Celem tych działań jest utrudnienie prześledzenia przepływu i zerwanie ciągłości analizy.
Końcowy etap często odbywa się już w świecie fizycznym. Środki trafiają do systemów umożliwiających ich wypłatę w gotówce, np. poprzez wpłatomaty kryptowalutowe. Wypłaty dokonują podstawione osoby, co dodatkowo utrudnia identyfikację sprawcy.
To właśnie na tych etapach, przy błędach popełnianych przez sprawców lub w punktach styku ze światem rzeczywistym, pojawia się największa szansa na skuteczne działania.

Dlaczego to nie jest proste

Skoro *blockchain* jest publiczny, a wiemy już, czego szukać na miejscu zdarzenia, pojawia się naturalne pytanie: dlaczego nie da się po prostu uruchomić ogólnodostępnego narzędzia i prześledzić przepływu środków?
Odpowiedź jest prosta: przestępcy również się uczą, a technologia rozwija się bardzo dynamicznie.
Nie operujemy już wyłącznie na jednej sieci, takiej jak Bitcoin. W praktyce mamy do czynienia z wieloma różnymi *blockchainami* (np. Ethereum czy Tron), które działają w odmienny sposób. Różnią się także modele zapisu transakcji, od modelu UTXO w Bitcoinie po model kont stosowany w innych sieciach.
W efekcie analiza szybko przestaje być intuicyjna. Próba śledzenia przepływów wyłącznie przy użyciu podstawowych narzędzi może być czasochłonna i obarczona ryzykiem błędnej interpretacji.

Kluczowym elementem są tzw. heurystyki, czyli reguły analityczne pozwalające na łączenie adresów i identyfikację wzorców działania. Bez ich znajomości łatwo o błędne wnioski, które mogą prowadzić do utraty czasu i skierowania postępowania na niewłaściwe tory.
Dlatego analiza kryptowalut nie polega na „zgadywaniu", lecz na uporządkowanym łączeniu danych. W praktyce wymaga to zarówno odpowiedniego przygotowania, jak i dostępu do specjalistycznych narzędzi analitycznych.

Zakończenie: nowa rzeczywistość

Kryptowaluty przestały być zjawiskiem niszowym. Stały się stałym elementem przestępczości gospodarczej i kryminalnej, z którym funkcjonariusze spotykają się coraz częściej.
Widać to również po zmianach w strukturach, od 1 marca 2026 r. we wszystkich komendach wojewódzkich Policji funkcjonują wydziały do walki z przestępczością cyfrową, których zakres obejmuje m.in. analizę informacji dostępnych w sieci (OSINT), zwalczanie oszustw internetowych oraz wsparcie lokalnych jednostek w sprawach technicznych. Zagadnienia związane z kryptowalutami stanowią już integralny element tego obszaru działań, obejmujący w szczególności zabezpieczenie materiału dowodowego, analizę przepływów oraz ich wstępną interpretację, a także transfer zabezpieczonych środków.
To wyraźny sygnał, że nie jest to już wiedza specjalistyczna zarezerwowana dla wąskiej grupy, lecz kompetencja, która staje się elementem codziennej pracy.
Jednocześnie w bardziej złożonych sprawach niezbędne pozostaje wsparcie wyspecjalizowanych jednostek. W praktyce oznacza to uzupełniający się model działania: od wstępnej analizy po zaawansowane działania operacyjne.
Doświadczenie pokazuje jednak, że wiele spraw, w szczególności dotyczących oszustw inwestycyjnych, można skutecznie ukierunkować już na etapie podstawowych czynności, pod warunkiem właściwego zabezpieczenia śladów i ich wstępnej analizy.
Środowisko pracy zmienia się dynamicznie, a wraz z nim rosną wymagania wobec funkcjonariuszy. Zrozumienie specyfiki kryptowalut oraz umiejętność właściwego zabezpieczenia cyfrowych śladów stają się dziś elementem podstawowego warsztatu.
Im szybciej zostanie to uwzględnione w codziennej praktyce, tym większe będą szanse na skuteczne prowadzenie postępowań i realne odzyskiwanie środków na rzecz pokrzywdzonych.

Summary

Cryptocurrencies. How to read digital footprints and avoid losing trail?

The author of this article presents the specific operational and procedural steps that must be taken in cases involving crimes related to the use of cryptocurrencies. The article highlights the role of flow analysis and draws attention to securing appropriate traces in such cases. The article also points out the most common mistakes made by officers and explains their importance for the proceedings conducted.

Tłumaczenie: Beata Pepłowska