Kryptowaluty na celowniku

Największe kradzieże krypto w historii oraz poradnik ochrony Twoich wirtualnych pieniędzy

Antoni Kurek

Spis treści

Rozdział 1. Cyfrowe złoto, cyfrowi złodzieje 5

1.1. Pieniądz bez banku: krótka historia kryptowalut.....5

1.2. Klucz prywatny, czyli wszystko, co masz 10

1.3. Gorące i zimne portfele 15

1.4. Dlaczego kradzież w blockchainie jest nieodwracalna.....19

1.5. Anatomia skoku: od włamania do pralni 24

Rozdział 2. Mt. Gox: upadek giganta .. **Błąd! Nie zdefiniowano zakładki.**

2.1. Od kart do gry do największej giełdy świata**Błąd! Nie zdefiniowano zakładki.**

2.2. Znikające bitcoiny ..... **Błąd! Nie zdefiniowano zakładki.**

2.3. Bankructwo i 850 tysięcy BTC. **Błąd! Nie zdefiniowano zakładki.**

2.4. Śledztwo, które trwało latami ... **Błąd! Nie zdefiniowano zakładki.**

2.5. Dekada czekania na zwrot pieniędzy**Błąd! Nie zdefiniowano zakładki.**

Rozdział 3. Bitfinex i Coincheck: giełdy na celowniku**Błąd! Nie zdefiniowano zakładki.**

3.1. Bitfinex 2016: dziura w multisigu**Błąd! Nie zdefiniowano zakładki.**

3.2. Para z Nowego Jorku i odzyskane miliardy**Błąd! Nie zdefiniowano zakładki.**

3.3. Coincheck 2018: NEM w gorącym portfelu**Błąd! Nie zdefiniowano zakładki.**

3.4. Japonia zaostrza zasady ..... **Błąd! Nie zdefiniowano zakładki.**

3.5. Czego nauczyły się giełdy (a czego nie)**Błąd! Nie zdefiniowano zakładki.**

Rozdział 4. Ronin i Poly Network: mosty pod ostrzałem**Błąd! Nie zdefiniowano zakładki.**

4.1. Czym są mosty między blockchainami**Błąd! Nie zdefiniowano zakładki.**

4.2. Ronin: pięć kluczy i jedna fałszywa oferta pracy**Błąd! Nie zdefiniowano zakładki.**

4.3. Poly Network: haker, który oddał łup**Błąd! Nie zdefiniowano zakładki.**

4.4. Wormhole, Nomad i inne pęknięte mosty**Błąd! Nie zdefiniowano zakładki.**

4.5. Dlaczego mosty są najsłabszym ogniwem**Błąd! Nie zdefiniowano zakładki.**

Rozdział 5. Bybit: rekord, który przetrwał półtora roku**Błąd! Nie zdefiniowano zakładki.**

5.1. Luty 2025: 1,5 miliarda w kilka minut**Błąd! Nie zdefiniowano zakładki.**

5.2. Podmieniony interfejs portfela . **Błąd! Nie zdefiniowano zakładki.**

5.3. Wyścig o zamrożenie środków. **Błąd! Nie zdefiniowano zakładki.**

5.4. Jak giełda przetrwała szturm na wypłaty**Błąd! Nie zdefiniowano zakładki.**

Rozdział 6. Binance: skok stulecia..... **Błąd! Nie zdefiniowano zakładki.**

6.1. 29 października 2026: alarm o 20:20**Błąd! Nie zdefiniowano zakładki.**

6.2. Laptop, od którego wszystko się zaczęło**Błąd! Nie zdefiniowano zakładki.**

6.3. 6,3 miliarda dolarów w ruchu... **Błąd! Nie zdefiniowano zakładki.**

6.4. Zamrożone miliardy: Tether, Circle i partnerzy**Błąd! Nie zdefiniowano zakładki.**

6.5. Ślad prowadzący do Bitget i Bybit**Błąd! Nie zdefiniowano zakładki.**

6.6. Binance płaci za wszystko..... **Błąd! Nie zdefiniowano zakładki.**

6.7. Co ten skok zmienia w branży.. **Błąd! Nie zdefiniowano zakładki.**

Rozdział 7. Lazarus: hakerzy na usługach państwa**Błąd! Nie zdefiniowano zakładki.**

7.1. Kim są i dla kogo pracują ..... **Błąd! Nie zdefiniowano zakładki.**

7.2. TraderTraitor i fałszywi rekruterzy**Błąd! Nie zdefiniowano zakładki.**

7.3. Od Sony Pictures do kryptowalut**Błąd! Nie zdefiniowano zakładki.**

7.4. Pralnia: miksery, mosty i OTC . **Błąd! Nie zdefiniowano zakładki.**

7.5. Kradzież jako źródło finansowania programu zbrojeniowego **Błąd! Nie zdefiniowano zakładki.**

7.6. Czy da się ich zatrzymać?..... **Błąd! Nie zdefiniowano zakładki.**

Rozdział 8. Twój portfel pod kluczem: praktyczny poradnik ochrony ..... **Błąd! Nie zdefiniowano zakładki.**

8.1. Giełda czy własny portfel? ..... **Błąd! Nie zdefiniowano zakładki.**

8.2. Portfele sprzętowe w praktyce.. **Błąd! Nie zdefiniowano zakładki.**

8.3. Fraza odzyskiwania: jak ją przechowywać**Błąd! Nie zdefiniowano zakładki.**

8.4. Phishing, fałszywe airdropy i podrobione aplikacje**Błąd! Nie zdefiniowano zakładki.**

8.5. Oszustwa „na inwestycję" i „na romans"**Błąd! Nie zdefiniowano zakładki.**

8.6. Uwierzytelnianie dwuskładnikowe bez SMS-ów**Błąd! Nie zdefiniowano zakładki.**

8.7. Podpisuj świadomie: zatwierdzenia i smart kontrakty**Błąd! Nie zdefiniowano zakładki.**

8.8. Co robić, gdy już zostałeś okradziony**Błąd! Nie zdefiniowano zakładki.**

8.9. Lista kontrolna bezpieczeństwa **Błąd! Nie zdefiniowano zakładki.**

Rozdział 1. Cyfrowe złoto, cyfrowi złodzieje

1.1. Pieniądz bez banku: krótka historia kryptowalut

Zanim pojawił się bitcoin, kilka pokoleń kryptografów próbowało zbudować pieniądz elektroniczny, który działałby bez banku. Żadna z tych prób nie przetrwała, a powody ich upadku warto znać, bo tłumaczą, dlaczego konstrukcja Satoshiego Nakamoto wyglądała tak, jak wygląda.

David Chaum, amerykański kryptograf, opisał w latach osiemdziesiątych system cyfrowej gotówki opartej na podpisach ślepych, czyli metodzie pozwalającej bankowi poświadczyć banknot bez poznania, kto go wydał. W 1989 roku założył firmę DigiCash, która wdrożyła ten pomysł pod nazwą eCash. Rozwiązanie było technicznie dobre i chroniło prywatność lepiej niż cokolwiek, co dziś używamy. Miało jedną wadę: wymagało banku, który emituje jednostki. Banki nie były zainteresowane, użytkowników nie przybywało, a DigiCash ogłosił upadłość w 1998 roku.

E-gold, uruchomiony w 1996 roku przez Douglasa Jacksona, poszedł inną drogą. Jednostki były pokryte złotem przechowywanym w skarbcach, a konta dało się zakładać praktycznie bez formalności. System urósł do milionów rachunków i obsługiwał przelewy międzynarodowe tańsze i szybsze niż banki. Przyciągnął też oszustów i piramidy finansowe, bo przelewów nie dało się cofnąć, a tożsamości nie weryfikowano. W 2007 roku amerykańskie władze postawiły firmie zarzuty prowadzenia nielicencjonowanej działalności transferu pieniędzy i prania pieniędzy, a e-gold przestał działać.

Dwie propozycje z 1998 roku poszły dalej i usunęły z układu centralnego emitenta. Wei Dai opisał b-money, w którym grupa uczestników prowadzi wspólny rejestr sald, a nowe jednostki powstają za wykonanie kosztownej pracy obliczeniowej. Nick Szabo opisał Bit Gold, w którym jednostki powstają z rozwiązywania zagadek kryptograficznych, a ich kolejność jest poświadczana przez rozproszoną sieć. Żadna z tych konstrukcji nie została wdrożona, bo obie zatrzymywały się na tym samym problemie: co zrobić, gdy uczestnicy rejestru nie zgadzają się co do tego, która wersja historii jest prawdziwa.

Problem ten ma w informatyce nazwę i długą literaturę. Chodzi o uzgodnienie stanu przez grupę, w której część uczestników może kłamać, a

nikt nie ma władzy rozstrzygającej. Bez jego rozwiązania pieniądz elektroniczny bez banku pozostaje pomysłem, bo nic nie powstrzymuje posiadacza przed wydaniem tej samej jednostki dwa razy w dwóch różnych miejscach.

31 października 2008 roku, w szczycie kryzysu finansowego, na liście dyskusyjnej poświęconej kryptografii pojawił się dziewięciostronicowy dokument zatytułowany „Bitcoin: A Peer-to-Peer Electronic Cash System". Podpisał go Satoshi Nakamoto, osoba lub grupa, której tożsamości do dziś nie ustalono.

Kontekst miał znaczenie. Sześć tygodni wcześniej upadł bank Lehman Brothers, rządy ratowały instytucje finansowe publicznymi pieniędzmi, a zaufanie do bankowości było najniższe od dziesięcioleci. Dokument Nakamoto nie zawierał publicystyki, lecz jego pierwsze zdanie opisywało system płatności pozwalający przesyłać pieniądze bezpośrednio, bez pośrednictwa instytucji finansowej.

Rozwiązanie problemu uzgodnienia było proste i kosztowne. Uczestnicy sieci konkurują o prawo dopisania kolejnej porcji transakcji, rozwiązując zadanie wymagające ogromnej liczby prób. Zwycięzca ogłasza wynik, pozostali go sprawdzają, a historia, za którą stoi najwięcej wykonanej pracy, jest uznawana za obowiązującą. Podmiana zapisu wymagałaby powtórzenia całej pracy wykonanej od tego momentu przez resztę sieci, a to przy odpowiedniej skali przestaje być opłacalne.

3 stycznia 2009 roku Nakamoto wykopał pierwszy blok, nazywany blokiem genezy. W jego treści zapisał nagłówek z gazety „The Times" z tego samego dnia: „Chancellor on brink of second bailout for banks", czyli „Kanclerz skarbu o krok od drugiego planu ratunkowego dla banków". Zapis pełni dwie funkcje: dowodzi, że blok nie powstał wcześniej, i wskazuje, w czym twórca upatrywał wady istniejącego systemu.

Rejestr, który wtedy powstał, nazywamy blockchainem. Jest to lista bloków, z których każdy zawiera zestaw transakcji i skrót matematyczny poprzedniego bloku. Zmiana czegokolwiek w starym bloku zmienia jego skrót, a przez to unieważnia wszystkie bloki następujące po nim.

Rejestr ten nie jest przechowywany w jednym miejscu. Kopię trzymają tysiące niezależnych komputerów, zwanych węzłami, rozsianych po świecie. Każdy z nich sprawdza samodzielnie, czy przychodzące transakcje są poprawne, i odrzuca te, które łamią reguły. Nie ma operatora, który mógłby

dopisać jednostki, zamrozić konto albo odwrócić przelew, i jest to cecha zamierzona, a nie niedopatrzenie.

Konsekwencje tej konstrukcji przewijają się przez całą tę książkę. Brak operatora oznacza brak infolinii, brak reklamacji i brak instancji odwoławczej. System, który nikomu nie pozwala cofnąć twojej transakcji, nie pozwala też cofnąć transakcji złodzieja.

Nowe bitcoiny powstają w procesie nazywanym kopaniem. Komputery kopiące wykonują miliardy prób na sekundę, szukając wartości, przy której skrót bloku spełni warunek narzucony przez sieć. Pierwszy, któremu się to uda, dopisuje blok i otrzymuje nagrodę w nowych monetach oraz opłaty z zawartych w bloku transakcji. Mechanizm ten nazywa się proof of work, czyli dowód wykonanej pracy.

Trudność zadania jest automatycznie korygowana, tak by blok powstawał średnio co dziesięć minut, niezależnie od tego, ile mocy obliczeniowej pracuje w sieci. Nagroda za blok zmniejsza się o połowę mniej więcej co cztery lata. Na początku wynosiła 50 bitcoinów, dziś jest wielokrotnie mniejsza, a suma wszystkich monet, które kiedykolwiek powstaną, została ograniczona do 21 milionów.

Limit ten jest zapisany w regułach, które sprawdza każdy węzeł, i jego zmiana wymagałaby zgody przeważającej części sieci. Jest to przeciwieństwo pieniądza państwowego, którego podaż ustala bank centralny, i właśnie ta cecha zjednała bitcoinowi określenie cyfrowego złota.

Przez pierwsze półtora roku bitcoin nie miał ceny, bo nikt nim nie handlował. 22 maja 2010 roku programista Laszlo Hanyecz z Florydy zapłacił 10 000 BTC za dwie pizze zamówione przez pośrednika. Była to pierwsza znana transakcja, w której bitcoiny wymieniono na rzecz materialną, a dzień ten obchodzony jest w środowisku jako Bitcoin Pizza Day.

Wartość tych dziesięciu tysięcy monet zmieniała się od tamtej pory o kilka rzędów wielkości. Przy cenie rzędu osiemdziesięciu tysięcy dolarów za monetę, zbliżonej do notowań z jesieni 2026 roku, odpowiadałaby ona około ośmiuset milionom dolarów. Liczba ta bywa przytaczana jako anegdota o straconej fortunie, choć w maju 2010 roku bitcoin nie miał rynku, na którym dałoby się te monety sprzedać.

W 2015 roku ruszył Ethereum, projekt zapoczątkowany przez Vitalika Buterina, który dodał do rejestru coś, czego bitcoin nie miał: możliwość

uruchamiania programów. Program taki, nazywany smart kontraktem, jest zapisany w blockchainie i wykonuje się automatycznie, gdy ktoś wyśle do niego transakcję spełniającą zapisane warunki.

Smart kontrakt nie jest umową w sensie prawnym ani niczym inteligentnym. Jest kodem, który robi to, co w nim napisano, niezależnie od intencji autora. Jeśli kod zawiera błąd pozwalający wypłacić cudze środki, to wypłata jest wykonaniem programu, a nie jego złamaniem. Rozdziały o Poly Network i o mostach pokazują, co z tego wynika w praktyce.

Na Ethereum i na podobnych sieciach powstała cała warstwa aplikacji finansowych: giełdy działające bez operatora, protokoły pożyczkowe, rynki instrumentów pochodnych. Wartość zablokowana w tych programach liczona jest w dziesiątkach miliardów dolarów, a ich kod jest jawny, co oznacza, że każdy, kto szuka w nim błędu, ma pełny wgląd.

Osobną i dziś bardzo dużą kategorią są stablecoiny, czyli tokeny utrzymujące stały kurs wobec waluty tradycyjnej, najczęściej dolara. Dwa największe to USDT emitowany przez spółkę Tether i USDC emitowany przez Circle. Ich kurs utrzymuje się dzięki rezerwom, które emitent deklaruje jako pokrycie wyemitowanych tokenów.

Różnica między nimi a bitcoinem jest zasadnicza i stanie się tematem kilku rozdziałów tej książki. Stablecoin ma centralnego emitenta, a emitent ma w kodzie tokena uprawnienie pozwalające zamrozić środki na wskazanym adresie. Nikt nie może zablokować twoich bitcoinów, ale Tether i Circle mogą zablokować twoje USDT i USDC, i robią to na wniosek organów ścigania oraz z własnej inicjatywy.

Dla posiadacza oznacza to, że stablecoin jest wygodny i jednocześnie nie jest aktywem na okaziciela. Dla złodzieja oznacza to, że ukradziony stablecoin bywa bezużyteczny. W rozdziale o kradzieży z Binance zobaczysz, jak ta jedna właściwość zadecydowała o losie miliardów dolarów.

Rynek kryptowalut przeszedł od 2009 roku kilka pełnych cykli wzrostu i załamania, a każdy z nich przebiegał podobnie. W 2013 roku cena bitcoina wzrosła z kilkunastu do ponad tysiąca dolarów, po czym spadła o ponad osiemdziesiąt procent, w czym udział miał upadek giełdy Mt. Gox opisany w następnym rozdziale.

W 2017 roku bitcoin zbliżył się do dwudziestu tysięcy dolarów, napędzany falą zbiórek na nowe tokeny, z których większość okazała się bezwartościowa. Rok 2018 przyniósł spadek o około osiemdziesiąt pięć

procent. W 2021 roku szczyt wypadł w okolicach sześćdziesięciu dziewięciu tysięcy dolarów, a kolejny rok przyniósł upadek giełdy FTX i spadek porównywalny z poprzednimi.

Każdy cykl zostawiał po sobie więcej użytkowników niż poprzedni. Zmieniał się też ich profil: od entuzjastów kryptografii, przez spekulantów, po zwykłych ludzi kupujących niewielkie kwoty przez aplikację w telefonie. Ta ostatnia grupa jest najliczniejsza i najsłabiej przygotowana, a rozdział ósmy jest napisany przede wszystkim dla niej.

Co do obecnej skali, podaję liczby z ostrożnością, bo zmieniają się z miesiąca na miesiąc i różnią się zależnie od źródła. Łączna kapitalizacja rynku kryptowalut liczona jest w bilionach dolarów, z czego bitcoin odpowiada zwykle za mniej więcej połowę. Szacunki liczby posiadaczy na świecie wahają się od kilkuset milionów w górę, zależnie od tego, czy liczy się konta na giełdach, czy osoby.

W Polsce, według badań prowadzonych w ostatnich latach, doświadczenie z kryptowalutami deklaruje kilkanaście procent dorosłych, przy czym większość z nich trzyma niewielkie kwoty na giełdach, a nie w portfelach własnych. Liczba ta rośnie, a wraz z nią rośnie liczba poszkodowanych, bo przestępcy idą tam, gdzie są pieniądze ludzi, którzy dopiero się uczą.

Jedna uwaga techniczna, zanim przejdziemy dalej. W tej książce podaję wartości skradzionych środków w dolarach według kursu z chwili kradzieży, chyba że zaznaczam inaczej. Jest to konwencja stosowana przez firmy analityczne, ale trzeba pamiętać, że kurs zmienia się o dziesiątki procent w ciągu miesięcy, więc te same monety bywają w różnych źródłach wyceniane różnie. Rozbieżności, na które natrafisz w opisach poszczególnych spraw, wynikają najczęściej właśnie z tego, a nie z błędu któregoś ze źródeł.

Warto jeszcze powiedzieć, czego ta książka nie jest, żeby nie było nieporozumień co do jej zamiaru.

Nie jest poradnikiem inwestycyjnym i nie zawiera żadnych zaleceń dotyczących tego, czy kupować kryptowaluty, które i kiedy. Nie oceniam, czy bitcoin jest dobrą lokatą ani czy rynek ten ma przed sobą przyszłość. Są to pytania, na które każdy musi odpowiedzieć sobie sam, uwzględniając własną sytuację, a ja nie jestem doradcą inwestycyjnym.

Nie jest też podręcznikiem technicznym. Opisuję ataki na tyle dokładnie, by było jasne, co zawiodło i czego to uczy, i nie dalej. Nie znajdziesz tu

instrukcji, kodu ani szczegółów, które przydałyby się komuś, kto chciałby powtórzyć opisane operacje. Wszystko, co podaję, pochodzi z publikacji firm analitycznych, z komunikatów poszkodowanych podmiotów i z dokumentów organów ścigania.

Jest natomiast dwiema rzeczami naraz. Po pierwsze, opisem tego, jak znikały największe sumy w historii tej branży, bo historie te są pouczające i rzadko bywają opowiedziane w całości. Po drugie, poradnikiem dla osoby, która trzyma kryptowaluty i chce, żeby jej nie zniknęły.

Te dwie części są ze sobą związane ściślej, niż mogłoby się wydawać. Prawie każdy mechanizm, który pozbawił giełdę miliardów, ma swój odpowiednik w skali pojedynczego użytkownika, różniący się wyłącznie rozmiarem. Dlatego rozdział ósmy raz po raz odsyła do konkretnych spraw z rozdziałów wcześniejszych, a wcześniejsze rozdziały kończą się wnioskami dla ciebie.

1.2. Klucz prywatny, czyli wszystko, co masz

Zacznę od sprostowania, które jest podstawą całej reszty tej książki: w twoim portfelu nie ma kryptowalut. Nie ma ich też w telefonie, w portfelu sprzętowym ani na giełdzie. Są zapisane w blockchainie, czyli w rejestrze powielonym na tysiącach komputerów, i nigdzie indziej nie istnieją.

To, co nazywamy portfelem, jest programem albo urządzeniem przechowującym klucze. Klucz pozwala udowodnić sieci, że to ty rozporządzasz środkami przypisanymi do określonego adresu. Gdy wysyłasz komuś bitcoiny, nic fizycznie nie wędruje; rejestr odnotowuje, że od tej pory środki przypisane do twojego adresu są przypisane do adresu odbiorcy.

Różnica ta ma skutki praktyczne. Zniszczenie portfela sprzętowego nie niszczy środków, bo rejestr pozostaje nietknięty i wystarczy odtworzyć klucze z kopii zapasowej. Zgubienie klucza bez kopii oznacza natomiast, że środki zostają w rejestrze na zawsze, widoczne dla wszystkich i niedostępne dla nikogo.

Klucz prywatny w bitcoinie i w Ethereum jest liczbą o długości 256 bitów, wylosowaną spośród wszystkich liczb z tego zakresu. Zapisany szesnastkowo ma postać ciągu sześćdziesięciu czterech znaków i nie zawiera żadnej struktury, którą dałoby się odgadnąć.

Warto wyobrazić sobie skalę tego zbioru, bo od niej zależy bezpieczeństwo całej konstrukcji. Liczb 256-bitowych jest około 1,16 razy 10 do potęgi 77. Liczbę atomów w obserwowalnym wszechświecie szacuje się na mniej więcej 10 do potęgi 80. Zbiór możliwych kluczy jest zatem porównywalny z liczbą atomów we wszechświecie podzieloną przez kilkaset.

Z tego wynika, że zgadywanie kluczy jest bezcelowe. Komputer sprawdzający bilion kluczy na sekundę, działający od Wielkiego Wybuchu, przeszedłby znikomy ułamek tego zbioru. Dlatego w żadnej z kradzieży opisanych w tej książce nikt nie łamał kryptografii. Klucze zdobywano inaczej: z komputera pracownika, z serwera, z pliku kopii zapasowej, z podstawionego ekranu albo przez nakłonienie właściciela do podpisania czegoś, czego nie rozumiał.

Z klucza prywatnego wylicza się klucz publiczny, a z klucza publicznego adres portfela. Operacja ta jest jednokierunkowa: mając klucz prywatny, otrzymasz adres w ułamku sekundy, mając adres, nie odtworzysz klucza żadną znaną metodą.

Jednokierunkowość opiera się na matematyce krzywych eliptycznych. Nie musisz jej rozumieć, by korzystać z portfela, ale warto wiedzieć, na czym polega zaufanie, które jej udzielasz. Mnożenie punktu na krzywej przez dużą liczbę jest łatwe, a odtworzenie tej liczby z wyniku jest zadaniem, dla którego nie znamy szybkiego algorytmu. Gdyby ktoś taki algorytm znalazł, runęłoby wszystko, co opisuję w tej książce, łącznie z zabezpieczeniami banków.

Praktyczny wniosek jest taki, że adres możesz pokazywać bez ryzyka. Każdy, kto go zna, zobaczy twoje saldo i historię transakcji, ale nie dowie się z niego niczego, co pozwoliłoby wydać środki. Klucz prywatny jest dokładnie odwrotnością: nie wolno go pokazać nikomu i nigdy.

Każda transakcja wychodząca z twojego adresu musi być podpisana cyfrowo kluczem prywatnym. Podpis powstaje z treści transakcji i z klucza, więc jest ważny tylko dla tej jednej transakcji; skopiowanie go do innej nic nie da.

Węzły sieci sprawdzają podpis przy użyciu klucza publicznego. Jeśli się zgadza, transakcja jest poprawna i zostaje wykonana. Sieć nie pyta przy tym, kim jesteś, skąd masz klucz ani czy go nie ukradłeś. Nie ma takiego pytania w protokole i nie ma nikogo, kto mógłby je zadać.

Tu leży źródło całej nieodwracalności, o której piszę w podrozdziale 1.4. Z punktu widzenia sieci właścicielem jest ten, kto ma klucz. Nie istnieje odrębna kategoria prawowitego właściciela ani sposób, by sieć ją rozpoznała.

Zapisywanie i wprowadzanie 256-bitowej liczby jest w praktyce nie do wykonania bez błędów, więc wymyślono zapis czytelny dla człowieka. Standard BIP-39 koduje losowe ziarno jako ciąg 12 lub 24 słów pochodzących z ustalonej listy 2048 słów.

Z tej frazy, nazywanej frazą odzyskiwania albo seed phrase, portfel wylicza nie jeden klucz, lecz całe drzewo kluczy dla wszystkich obsługiwanych sieci i wszystkich kont. Dlatego dwanaście słów wystarcza, by odtworzyć portfel z bitcoinami, ethereum i kilkunastoma innymi aktywami naraz, na dowolnym urządzeniu dowolnego producenta obsługującego ten standard.

Wygoda ta ma swoją cenę i trzeba ją powiedzieć wprost: fraza odzyskiwania jest ważniejsza od pojedynczego klucza, bo jest kluczem do wszystkiego. Kto ją pozna, przejmie całą zawartość portfela, we wszystkich sieciach, bez względu na to, gdzie fizycznie znajduje się urządzenie i czy jest włączone.

Dodam dwie uwagi techniczne, przydatne później. Kolejność słów ma znaczenie, a lista słów jest tak dobrana, że pierwsze cztery litery jednoznacznie identyfikują słowo. Ostatnie słowo frazy zawiera sumę kontrolną, więc przypadkowo wymyślona fraza prawie na pewno zostanie odrzucona jako niepoprawna.

W środowisku kryptowalut krąży zdanie, które jest jednocześnie hasłem i streszczeniem całej nauki płynącej z tej książki: not your keys, not your coins. Nie twoje klucze, nie twoje monety.

Gdy trzymasz środki na giełdzie, nie masz kluczy. Masz wpis w bazie danych firmy, stwierdzający, że jesteś jej wierzycielem na określoną kwotę. Kluczami zarządza giełda, w swoim imieniu, i to ona decyduje, czy i kiedy wykona twoje zlecenie wypłaty.

W normalnych warunkach różnica jest niewidoczna, bo wypłaty działają. Staje się widoczna, gdy giełda zostanie okradziona, zbankrutuje, zablokuje konto albo wstrzyma wypłaty. Wtedy okazuje się, że byłeś wierzycielem, a nie właścicielem, i że twoje miejsce jest w kolejce wierzycieli, co przy Mt. Gox oznaczało dekadę oczekiwania.

Rozwiązanie przeciwne, czyli samodzielne trzymanie kluczy, przenosi całe ryzyko na ciebie. Nikt nie ukradnie twoich monet z giełdy, bo ich tam nie ma, ale nikt też nie pomoże ci, gdy zgubisz frazę albo podpiszesz złośliwą transakcję. Wybór między tymi dwoma modelami jest tematem podrozdziału 8.1 i nie ma jednej dobrej odpowiedzi.

O tym, jak nieodwracalna jest utrata klucza, najlepiej świadczy to, ile bitcoinów przestało być dostępnych. Szacunki firm analizujących blockchain mówią o kilku milionach monet, które nie poruszyły się od wielu lat i prawdopodobnie nie poruszą się nigdy, co odpowiada kilkunastu procentom całej podaży.

Liczby te są szacunkami, bo z rejestru nie da się odczytać, czy ktoś zgubił klucz, czy po prostu nie wydaje monet. Analitycy wyciągają wnioski z wieku środków, z historii adresów i z monet wykopanych w pierwszych latach, kiedy nie miały ceny i nikt nie dbał o kopie zapasowe.

Najczęściej przytaczanym przykładem jest sprawa Jamesa Howellsa z Newport w Walii. W 2009 roku wykopał on około ośmiu tysięcy bitcoinów, a dysk twardy z kluczami wyrzucił w 2013 roku przy porządkach, nie pamiętając, co na nim jest. Dysk trafił na miejskie wysypisko.

Howells od tamtej pory próbuje uzyskać zgodę władz miasta na przekopanie składowiska, oferując udział w wartości odzyskanych monet i przedstawiając kolejne plany wykopalisk. Miasto odmawia, powołując się na pozwolenia środowiskowe i ryzyko skażenia, a sprawa trafiła do sądu, który w 2025 roku oddalił jego pozew. Wartość tych ośmiu tysięcy monet liczona jest dziś w setkach milionów dolarów.

Historia ta bywa opowiadana jako ciekawostka, a zawiera konkretną lekcję. Howells nie padł ofiarą żadnego ataku. Nie zawiodła kryptografia, nie było włamania ani oszustwa. Wystarczyło, że jeden przedmiot trafił do niewłaściwego worka.

Na koniec zdanie, które jest najważniejsze w całym tym podrozdziale i do którego będę wracał w rozdziale ósmym. Kto zdobędzie twój klucz prywatny albo twoją frazę odzyskiwania, ma pełną kontrolę nad środkami. Pełną, natychmiastową i nieodwracalną.

Nie ma znaczenia, w jaki sposób je zdobył. Czy wykradł je złośliwym oprogramowaniem, czy podejrzał kartkę na biurku, czy przekonał cię przez telefon, że jest pracownikiem obsługi, czy znalazł zdjęcie frazy w kopii

zapasowej twojego telefonu w chmurze. Dla sieci wszystkie te drogi są identyczne, bo sieć widzi wyłącznie poprawny podpis.

Nie ma też znaczenia, czy wiesz o kradzieży. Osoba, która zna twoją frazę, może poczekać miesiąc albo rok, obserwując adres i wybierając moment, w którym saldo będzie najwyższe. Zdarza się to częściej, niż można przypuszczać, i jest jednym z powodów, dla których fraza raz wprowadzona na zainfekowanym urządzeniu jest spalona na zawsze, nawet jeśli nic się nie stało przez pół roku.

Z tych dwóch zdań wynika praktycznie cały poradnik z rozdziału ósmego. Wszystko, co tam opisuję — portfele sprzętowe, przechowywanie frazy, uwierzytelnianie dwuskładnikowe, czytanie transakcji przed podpisaniem — służy jednemu celowi: żeby ta jedna informacja nie trafiła do nikogo poza tobą.

Na zakończenie warto wyjaśnić jeszcze jedno nieporozumienie, które powraca w rozmowach o bezpieczeństwie kryptowalut: obawę przed komputerami kwantowymi.

Teza, którą się słyszy, brzmi tak: komputer kwantowy złamie kryptografię zabezpieczającą bitcoina, więc całość jest tymczasowa. Teza ta jest uproszczeniem na tyle dużym, że warto ją rozłożyć.

Zagrożenie dotyczy nie kluczy prywatnych jako takich, lecz algorytmu, który wiąże klucz prywatny z publicznym. Znany algorytm kwantowy pozwalałby, przy dostatecznie dużym i stabilnym komputerze kwantowym, wyliczyć klucz prywatny z publicznego. Funkcje skrótu, na których opierają się adresy, są na to znacznie odporniejsze.

Z tego wynika rzecz praktyczna. Adres, z którego nigdy nie wysłano transakcji, nie ujawnia klucza publicznego, bo ten pojawia się dopiero przy pierwszym wydatku. Środki na takich adresach są bezpieczniejsze niż na adresach używanych wielokrotnie.

Co do skali zagrożenia: obecne komputery kwantowe są wiele rzędów wielkości za małe, a szacunki czasu potrzebnego do osiągnięcia wymaganej skali wahają się od kilkunastu lat do nigdy. Równolegle trwają prace nad algorytmami odpornymi na ataki kwantowe, a sieci kryptowalutowe mogą je wdrożyć, zanim zagrożenie stanie się realne.

Dla ciebie wniosek jest taki, że to nie jest ryzyko, którym warto się dziś zajmować. Twoje środki są wielokrotnie bardziej zagrożone przez phishing,

przez zgubioną frazę i przez podpisanie niewłaściwej transakcji, czyli przez wszystko, co opisuję w rozdziale ósmym.

1.3. Gorące i zimne portfele

Podział portfeli na gorące i zimne jest najprostszym i najużyteczniejszym rozróżnieniem w całym bezpieczeństwie kryptowalut. Kryterium jest jedno: czy klucz prywatny znajduje się na urządzeniu mającym kontakt z internetem.

Portfel gorący to taki, którego klucze przechowywane są na urządzeniu stale podłączonym do sieci. Należą tu aplikacje w telefonie, rozszerzenia przeglądarki, programy na komputerze i serwery giełd obsługujące bieżące wypłaty. Zaletą jest natychmiastowa dostępność: podpisanie transakcji zajmuje sekundę i nie wymaga żadnych dodatkowych czynności.

Wadą jest to, że klucz znajduje się w zasięgu wszystkiego, co może zaatakować to urządzenie. Złośliwe oprogramowanie, luka w systemie, przejęte konto, zainfekowane rozszerzenie przeglądarki, dostęp zdalny udzielony przez nieuważnego użytkownika. Każda z tych dróg prowadzi do klucza, a klucz jest wszystkim.

Portfel zimny to taki, którego klucze nigdy nie miały i nie mają kontaktu z siecią. Klucz powstaje na urządzeniu odciętym od internetu i nigdy go nie opuszcza. Transakcja jest przygotowywana na komputerze podłączonym do sieci, przenoszona do urządzenia zimnego, tam podpisywana, a z powrotem wraca sam podpis.

Przewaga tego rozwiązania polega na tym, że napastnik, który przejął twój komputer, nadal nie ma klucza. Może zobaczyć twoje salda, może podmienić adres odbiorcy w przygotowywanej transakcji, ale nie podpisze niczego bez urządzenia, które masz w szufladzie. To ograniczenie jest fizyczne, a nie programowe, i dlatego trudne do obejścia.

Dla użytkownika indywidualnego dostępne są cztery podstawowe rodzaje portfeli i warto znać ich właściwości, zanim przejdziemy do praktyki w rozdziale ósmym.

Aplikacje mobilne są portfelami gorącymi. Klucz leży w pamięci telefonu, chroniony przez mechanizmy systemu operacyjnego, które w nowszych urządzeniach są dobre, ale nie są nie do przejścia. Zaletą jest

wygoda, wadą to, że telefon jest urządzeniem, na którym instalujesz dziesiątki aplikacji, klikasz w linki i łączysz się z przypadkowymi sieciami.

Rozszerzenia przeglądarki są portfelami gorącymi o podwyższonym ryzyku. Działają w środowisku, które z założenia wykonuje kod pobrany z internetu, i są najczęstszym celem podrobionych wersji oraz złośliwych stron. Jednocześnie są niezbędne do korzystania z aplikacji zdecentralizowanych, więc rzecz nie w tym, by ich nie używać, lecz by trzymać w nich tylko tyle, ile można stracić.

Portfele sprzętowe to urządzenia wielkości pendrive'a, przeznaczone wyłącznie do przechowywania kluczy i podpisywania transakcji. Klucz powstaje wewnątrz, nie opuszcza układu i nie jest dostępny dla komputera, do którego urządzenie podłączasz. Są najpopularniejszą formą zimnego przechowywania dla osób prywatnych i poświęcam im osobny podrozdział.

Portfele papierowe to wydrukowany lub zapisany ręcznie klucz albo fraza. Są skrajnie odporne na ataki sieciowe, bo nie mają żadnego styku z siecią, i skrajnie podatne na ogień, wodę, wyblaknięcie druku oraz przypadkowe wyrzucenie. Dziś stosuje się je raczej jako kopię zapasową frazy niż jako główny portfel.

Giełdy stosują ten sam podział, tylko w innej skali. Nie trzymają wszystkich środków klientów w jednym miejscu, bo byłoby to równoznaczne z pozostawieniem całego majątku firmy na jednym serwerze.

Typowy układ wygląda tak: niewielka część środków, zwykle rzędu kilku procent, leży w portfelach gorących i służy do obsługi bieżących wypłat. Reszta jest w zimnych magazynach, do których dostęp wymaga udziału kilku osób, często fizycznej obecności i procedur trwających godziny. Gdy gorący portfel się opróżnia, przeprowadza się uzupełnienie z magazynu zimnego.

Układ ten jest rozsądny i ogranicza skalę pojedynczego włamania. Ma jednak dwa punkty, w których zawodzi, i oba opisuję w tej książce. Pierwszy to sam moment uzupełnienia, gdy środki przechodzą z zimnego do gorącego i ktoś musi je podpisać; tak wyglądał atak na Bybit. Drugi to sytuacja, w której napastnik nie kradnie kluczy, lecz zmusza systemy giełdy, by same podpisały to, czego chce; tak wyglądał atak na Binance.

Osobnym zabezpieczeniem, stosowanym zarówno przez firmy, jak i przez zamożniejszych użytkowników indywidualnych, są portfele wielopodpisowe, w skrócie multisig. Zasada jest prosta: do wykonania transakcji potrzeba kilku podpisów z wcześniej ustalonego zbioru kluczy.

Typowe układy zapisuje się jako dwa z trzech albo trzy z pięciu. W pierwszym istnieją trzy klucze, a do wykonania transakcji wystarczają dowolne dwa. Zaletą jest odporność na dwie przeciwne sytuacje naraz: utrata jednego klucza nie blokuje środków, a przejęcie jednego klucza nie wystarcza do kradzieży.

Dla osoby prywatnej taki układ ma sens przy większych kwotach. Klucze można rozłożyć na różne urządzenia i różne lokalizacje, a jeden powierzyć zaufanej osobie albo usłudze zewnętrznej. Dla firmy multisig jest standardem, bo rozdziela odpowiedzialność i wymusza udział kilku osób przy każdej wypłacie.

Nowszym rozwiązaniem stosowanym w instytucjach jest MPC, czyli obliczenia wielostronne. Różnica wobec multisigu jest subtelna, a istotna. W multisigu istnieje kilka pełnoprawnych kluczy, a blockchain widzi kilka podpisów. W MPC istnieje jeden klucz, który nigdy nie zostaje złożony w całość: jest podzielony na fragmenty przechowywane przez różne strony, a podpis powstaje przez wspólne obliczenie, w którym żadna strona nie poznaje fragmentów pozostałych.

Zaletą jest to, że nie ma momentu ani miejsca, w którym kompletny klucz istnieje i mógłby zostać wykradziony. Zaletą jest też to, że dla blockchaina wygląda to jak zwykły pojedynczy podpis, więc działa w każdej sieci i nie zdradza struktury zabezpieczeń. Wadą jest złożoność: poprawność implementacji trudniej sprawdzić, a cała konstrukcja opiera się na oprogramowaniu dostawcy.

Teraz rzecz, która tłumaczy większość kradzieży opisanych w tej książce: nikt nie trzyma wszystkiego w zimnym magazynie, bo zimny magazyn nie pozwala prowadzić działalności.

Giełda musi realizować wypłaty w minutach, a nie w godzinach, bo klienci odejdą do konkurencji. Protokół pożyczkowy musi móc automatycznie likwidować pozycje. Firma płacąca dostawcom musi wykonywać przelewy codziennie. Każde z tych wymagań oznacza, że jakaś część środków i jakaś część uprawnień musi być dostępna bez udziału człowieka albo z udziałem minimalnym.

Kompromis ten nie jest niedbalstwem, lecz warunkiem działania. Pytanie, które zadaje sobie każdy dobry zespół bezpieczeństwa, nie brzmi, jak go uniknąć, lecz jak ograniczyć szkodę, gdy gorąca część zostanie przejęta: jakie limity nałożyć na pojedynczą wypłatę, jakie opóźnienia wprowadzić dla

nowych adresów, jakie progi wymagają udziału człowieka i jak szybko da się odciąć kompromitowany system.

Dokładnie to samo pytanie dotyczy ciebie, tylko w mniejszej skali. Nie chodzi o to, by trzymać wszystko w zimnym portfelu, bo wtedy przestaniesz go używać i w końcu zrobisz coś niebezpiecznego ze zniecierpliwienia. Chodzi o to, by rozdzielić środki według tego, jak często ich używasz, i żeby kwota dostępna z telefonu była kwotą, której strata byłaby przykra, a nie katastrofalna.

Na koniec ostrzeżenie, bez którego cały ten podrozdział byłby mylący. Portfel zimny chroni przed wykradzeniem klucza. Nie chroni przed sytuacją, w której sam podpiszesz transakcję przygotowaną przez napastnika.

Mechanizm jest następujący. Napastnik nie potrzebuje twojego klucza, jeśli zdoła sprawić, że użyjesz go sam w sposób, którego nie zamierzałeś. Pokazuje ci na ekranie komputera jedną treść, a do urządzenia podpisującego wysyła inną. Albo pokazuje treść prawdziwą, lecz tak zapisaną, że nie da się jej odczytać ze znaczeniem na małym wyświetlaczu.

W obu przypadkach urządzenie zachowuje się poprawnie: dostaje do podpisania dane, prosi o potwierdzenie i podpisuje. Klucz nie wycieka. Środki znikają.

Zjawisko to nazywa się ślepym podpisywaniem i jest dziś najpoważniejszym pojedynczym zagrożeniem dla użytkowników portfeli sprzętowych. Przy kradzieży z Bybit, opisanej w rozdziale piątym, dotknęło zespołu zawodowców korzystających z najlepszych dostępnych narzędzi, a mimo to podpisali oni przejęcie własnego portfela, widząc na ekranie zwyczajny przelew.

Wniosek dla ciebie jest praktyczny i wracam do niego w podrozdziale 8.7. Sprzęt odpowiada za ochronę klucza i robi to dobrze. Za to, co podpisujesz, odpowiadasz ty, a to jest ta część zabezpieczenia, której nie da się kupić.

Warto jeszcze powiedzieć o rozwiązaniu, które w ostatnich latach zyskuje popularność i mieści się pomiędzy portfelem gorącym a zimnym: o portfelach z kontrolą społeczną i z odzyskiwaniem dostępu.

Pomysł wziął się z obserwacji, że najczęstszą przyczyną utraty środków przez zwykłych ludzi nie jest kradzież, lecz zgubienie frazy. Jeśli tak, to rozwiązaniem nie jest kolejne zabezpieczenie, lecz mechanizm pozwalający odzyskać dostęp bez frazy.

Portfele tego rodzaju są smart kontraktami, a nie zwykłymi adresami, i mają wbudowane reguły. Jedną z nich bywa odzyskiwanie dostępu przy udziale wskazanych wcześniej osób albo urządzeń: jeśli stracisz klucz, odpowiednia ich liczba może po upływie okresu oczekiwania przypisać do portfela nowy.

Zaletą jest to, że utrata jednego urządzenia przestaje być katastrofą. Wadą jest zaufanie do osób, które wskazałeś, oraz zależność od poprawności kodu kontraktu, czyli od ryzyka, którego zwykły portfel nie ma.

Do tej samej rodziny należą portfele z wbudowanymi limitami: dzienną kwotą, którą można wypłacić bez dodatkowego potwierdzenia, oraz opóźnieniem przy wypłatach powyżej progu. Jest to przeniesienie na poziom użytkownika rozwiązań, które giełdy stosują od lat i które opisuję w rozdziale szóstym.

Nie polecam ani nie odradzam konkretnych produktów tego rodzaju, bo rynek zmienia się zbyt szybko. Warto natomiast wiedzieć, że wybór nie sprowadza się do pary gorący albo zimny i że przy większych kwotach rozwiązania pośrednie bywają rozsądniejsze od obu skrajności.

1.4. Dlaczego kradzież w blockchainie jest nieodwracalna

Gdy wykonujesz przelew bankowy, uruchamiasz procedurę, w której uczestniczy kilka instytucji, a każda z nich ma możliwość ingerencji. Bank nadawcy może wstrzymać przelew przed jego wysłaniem. Bank odbiorcy może zablokować środki na rachunku. Przy zgłoszeniu oszustwa banki mogą uruchomić procedurę odzyskania, a w Polsce istnieje system szybkich zastrzeżeń międzybankowych, który pozwala zatrzymać pieniądze, jeśli zgłoszenie nastąpi dostatecznie wcześnie.

Skuteczność tych narzędzi jest ograniczona i każdy, kto padł ofiarą oszustwa bankowego, wie, że odzyskanie pieniędzy bywa trudne. Istotne jest jednak to, że istnieje ktoś, kto może działać: instytucja z obowiązkami, adresem i nadzorem.

W blockchainie nie ma takiej instytucji. Transakcja, która została włączona do bloku i potwierdzona przez sieć, jest faktem zapisanym w rejestrze powielonym na tysiącach komputerów. Nie istnieje podmiot, do którego można złożyć reklamację, bo nie istnieje podmiot, który tę transakcję wykonał. Wykonały ją reguły protokołu, a reguły nie mają obsługi klienta.

Nie pomaga tu zgłoszenie na policję ani wyrok sądu, przynajmniej nie bezpośrednio. Sąd może nakazać komuś zwrot środków, ale żaden wyrok nie zmieni zapisu w rejestrze. Egzekucja takiego wyroku wymaga, by osoba zobowiązana istniała, była znana, podlegała jurysdykcji i miała z czego zapłacić, a przy kradzieżach opisanych w tej książce żaden z tych warunków zwykle nie jest spełniony.

Osobno warto wymienić to, czego w kryptowalutach nie ma: odpowiednika chargebacku. Przy płatności kartą masz prawo zakwestionować transakcję u wydawcy karty, który w razie uznania reklamacji obciąża zwrotnie sprzedawcę. Mechanizm ten istnieje, ponieważ w systemie kartowym jest pośrednik ponoszący ryzyko i czerpiący z tego zysk.

W płatności kryptowalutą pośrednika nie ma, więc nie ma też nikogo, kto mógłby obciążyć drugą stronę. Dla sprzedawcy jest to zaleta, bo nie grożą mu nieuczciwe reklamacje. Dla kupującego jest to wada, bo jeśli zapłaci i nie dostanie towaru, pozostaje mu wyłącznie droga sądowa wobec konkretnej osoby, o ile wie, kim ona jest.

Nieodwracalność nie pojawia się w jednej chwili, lecz narasta. Transakcja wysłana do sieci trafia najpierw do puli oczekujących i w tym momencie nadal można ją zastąpić inną, płacąc wyższą opłatę. Gdy zostanie włączona do bloku, mówimy o jednym potwierdzeniu.

Teoretycznie blok może zostać odrzucony, jeśli w sieci powstanie konkurencyjne rozgałęzienie o większej skumulowanej pracy. W praktyce prawdopodobieństwo maleje wykładniczo z każdym kolejnym blokiem. W bitcoinie za praktycznie nieodwracalne przyjmuje się sześć potwierdzeń, czyli mniej więcej godzinę. Przy dużych kwotach giełdy wymagają więcej.

Ethereum po przejściu na mechanizm oparty na depozytach wprowadziło pojęcie ostateczności w sensie ścisłym: po dwóch epokach, czyli mniej więcej po trzynastu minutach, odwrócenie bloku wymagałoby utraty depozytów o wartości liczonej w miliardach dolarów. Nie jest to niemożliwe matematycznie, lecz jest nieopłacalne w sposób, który czyni je praktycznie wykluczonym.

Dla ofiary kradzieży oznacza to, że okno reakcji liczy się w minutach, a nie w godzinach, i że w praktyce zwykle już go nie ma, bo kradzież zauważa się po fakcie. Dlatego w rozdziale o Binance tak duże znaczenie ma to, że emitenci stablecoinów zamrozili główne adresy w ciągu godziny.

W całej historii kryptowalut skutki jednej kradzieży cofnięto, zmieniając reguły sieci. Warto tę sprawę znać, bo bywa przywoływana jako dowód, że odwrócenie jest możliwe, a wnioski z niej są odwrotne.

W kwietniu 2016 roku na Ethereum uruchomiono The DAO, zdecentralizowany fundusz inwestycyjny w postaci smart kontraktu. Zebrał równowartość ponad 150 milionów dolarów, co stanowiło wówczas znaczną część wszystkich eterów w obiegu. W czerwcu ktoś wykorzystał błąd w kodzie funkcji wypłaty i wyprowadził około jednej trzeciej zgromadzonych środków.

Kod zadziałał zgodnie z tym, co w nim napisano, i w tym sensie nie został złamany. Społeczność Ethereum stanęła przed wyborem: uznać wynik za obowiązujący albo zmienić reguły sieci, by go unieważnić. Po gorącym sporze w lipcu 2016 roku przeprowadzono hard fork, czyli rozgałęzienie, w którym nowa wersja protokołu przenosiła środki z kontraktu napastnika do kontraktu umożliwiającego zwrot.

Część uczestników uznała to za złamanie fundamentalnej zasady i kontynuowała pracę na starym łańcuchu, w którym kradzież pozostała w mocy. Ten łańcuch istnieje do dziś pod nazwą Ethereum Classic.

Z tej sprawy płyną dwa wnioski. Pierwszy: cofnięcie jest możliwe tylko wtedy, gdy przeważająca część sieci zgodzi się zmienić reguły, co wymaga, by kradzież zagrażała istnieniu całego projektu. Drugi: koszt takiej operacji jest ogromny, bo rozbija społeczność i podważa założenie, na którym opiera się cała konstrukcja. Od 2016 roku nie powtórzono tego ani razu, mimo kradzieży wielokrotnie większych.

Przeciwwagą dla nieodwracalności jest jawność. Blockchain jest pseudonimowy, a nie anonimowy, i różnica ta jest zasadnicza.

Każda transakcja w bitcoinie i w Ethereum jest publiczna. Każdy może zobaczyć, z jakiego adresu na jaki poszły środki, kiedy i ile. Nie trzeba do tego żadnych uprawnień ani narzędzi: wystarczy przeglądarka bloków, czyli zwykła strona internetowa.

Czego nie widać, to powiązania adresu z nazwiskiem. Adres jest ciągiem znaków i sam z siebie nie mówi nic o właścicielu. Dopóki nie zrobisz niczego, co połączy adres z twoją tożsamością, pozostaje on niepowiązany.

Przez pierwsze lata uważano, że czyni to kryptowaluty narzędziem idealnym dla przestępców. Praktyka okazała się inna: trwały, publiczny i kompletny rejestr wszystkich przepływów jest dla śledczych materiałem,

jakiego nie mają w żadnym innym systemie finansowym. W bankowości trzeba wnioskować o dane do każdej instytucji z osobna, w różnych krajach. Tutaj wszystko jest od razu widoczne, na zawsze.

Na tej jawności wyrosła osobna branża. Firmy analizy blockchaina — największe to Chainalysis, Elliptic i TRM Labs — zajmują się przypisywaniem adresów do podmiotów i śledzeniem przepływów.

Metody opierają się na kilku prostych obserwacjach. Adresy używane razem w jednej transakcji należą zwykle do tego samego właściciela. Giełdy mają rozpoznawalne wzorce wpłat i wypłat. Kwoty, godziny i kolejność operacji tworzą ślady. Do tego dochodzą dane spoza łańcucha: adresy ujawnione w postępowaniach, dane od giełd, informacje z forów i z wycieków.

Skuteczność tych narzędzi jest realna, choć łatwo ją przecenić. Przy kradzieży z Binance analitycy oznaczyli adresy odbiorcze w ciągu minut, co pozwoliło emitentom zamrozić miliardy. Przy kradzieży z Bybit po roku około dwóch trzecich środków pozostawało możliwych do prześledzenia, a mimo to niemożliwych do odzyskania, bo śledzenie i odzyskanie to dwie różne rzeczy.

Możliwości odzyskania środków są trzy i wszystkie mają poważne ograniczenia.

Pierwsza to zamrożenie przez emitenta. Dotyczy wyłącznie tokenów mających centralnego emitenta, czyli przede wszystkim stablecoinów. Tether, Circle, Ripple i inni mogą zablokować środki na wskazanym adresie, i robią to szybko, gdy dostaną wiarygodne zgłoszenie. Jest to dziś najskuteczniejsze narzędzie w całym zestawie, i to ono uratowało znaczną część łupu przy kradzieży z Binance.

Druga to blokada na giełdzie. Jeśli napastnik spróbuje wypłacić środki przez giełdę stosującą weryfikację tożsamości i monitorującą adresy, operacja zostanie zatrzymana, a konto zablokowane. Dlatego zorganizowane grupy unikają takich giełd i korzystają z pośredników, którzy o tożsamość nie pytają.

Trzecia to konfiskata przez organy ścigania. Zdarza się i bywa skuteczna, o czym świadczy odzyskanie przez amerykański Departament Sprawiedliwości bitcoinów skradzionych z Bitfinex w 2016 roku. Wymaga jednak dotarcia do kluczy, czyli zwykle do urządzenia podejrzanego, a to oznacza, że podejrzany musi być zidentyfikowany i osiągalny.

Ostatnie zastrzeżenie jest najpoważniejsze i prowadzi do problemu, na którym rozbija się większość spraw. Przy kradzieżach prowadzonych przez grupy działające z terytorium państw niewspółpracujących z zachodnimi organami ścigania żadna z tych dróg nie prowadzi do sprawcy.

Akt oskarżenia wobec osoby, która nie opuszcza swojego kraju, jest dokumentem bez praktycznych skutków. Wniosek o pomoc prawną do państwa, które tego nie zrobi, pozostaje bez odpowiedzi. Nakaz aresztowania działa tylko wtedy, gdy podejrzany przekroczy granicę do kraju, który go wykona, i właśnie tak zatrzymano Aleksandra Winnika, o czym piszę w rozdziale drugim.

Pozostaje droga cywilna, równie trudna. Ustalenie właściwego sądu przy transakcji między adresem a adresem bywa samo w sobie sporne. Doręczenie pozwu osobie, której nazwiska nie znasz, jest niewykonalne. Nawet przy korzystnym wyroku egzekucja wymaga majątku w zasięgu komornika.

Dlatego praktyczny wniosek z tego podrozdziału jest taki, że w kryptowalutach nie ma skutecznej drogi odzyskania po fakcie i że całą uwagę trzeba przenieść na to, co dzieje się przed. Rozdział ósmy jest poświęcony właśnie temu, a podrozdział 8.8 opisuje, co robić po kradzieży, zachowując przy tym realistyczne oczekiwania co do wyniku.

Dla pełnego obrazu trzeba dodać, że nieodwracalność bywa przerywana również w inny sposób niż przez zmianę reguł sieci, i że zdarza się to częściej, niż się przypuszcza.

Chodzi o sieci warstwy drugiej i o sieci o ograniczonej liczbie uczestników, w których istnieją mechanizmy nadzwyczajne. Rada Bezpieczeństwa sieci Arbitrum, o której piszę w podrozdziale 6.4, przeniosła poza zasięg napastnika środki warte około trzydziestu milionów dolarów, korzystając z uprawnień wbudowanych w tę sieć.

Podobne uprawnienia istnieją w kilku innych sieciach, zwłaszcza nowszych i wciąż rozwijanych. Ich twórcy uzasadniają to koniecznością reagowania na błędy w okresie, gdy konstrukcja nie jest jeszcze w pełni dojrzała, i jest to uzasadnienie rozsądne.

Dla użytkownika wynika stąd jednak wniosek, o którym rzadko się mówi: nie wszystkie sieci są równie nieodwracalne, a różnice te wynikają z tego, kto ma w nich uprawnienia nadzwyczajne. Sieć, w której grupa osób może przenieść cudze środki, ma inny model zaufania niż bitcoin, choć wygląda z zewnątrz podobnie.

Działa to w obie strony. Taka sieć może uratować twoje środki po kradzieży i może je odebrać wskutek decyzji, na którą nie masz wpływu. Przed przeniesieniem większych kwot do sieci, której nie znasz, warto sprawdzić, kto i w jakim zakresie ma w niej takie uprawnienia.

1.5. Anatomia skoku: od włamania do pralni

Duże kradzieże kryptowalut nie są dziełem przypadku ani pojedynczego geniusza przy klawiaturze. Są operacjami planowanymi tygodniami, prowadzonymi przez zespoły z podziałem ról, i przebiegają według schematu, który powtarza się na tyle wiernie, że da się go opisać etapami. Ten podrozdział jest mapą dla całej reszty książki: w kolejnych rozdziałach zobaczysz te same etapy w konkretnych sprawach.

Zaczyna się od rozpoznania. Napastnicy zbierają informacje o celu: kto tam pracuje i na jakich stanowiskach, jakiego oprogramowania używa firma, kto jest jej dostawcą, jak wygląda infrastruktura, gdzie leżą portfele i jakie są procedury wypłat.

Źródła są w większości jawne. Profile zawodowe pracowników w serwisach rekrutacyjnych, ogłoszenia o pracę opisujące używane technologie, wystąpienia konferencyjne inżynierów, publiczne repozytoria kodu, dokumentacja techniczna, adresy portfeli widoczne w blockchainie. Firma działająca jawnie i zatrudniająca ludzi nie ma sposobu, by te informacje ukryć.

Etap ten trwa najdłużej i jest najmniej widoczny. W sprawie Bybit przygotowania sięgały kilku tygodni, w sprawie Binance analitycy ustalili, że sama faza operacyjna zaczęła się co najmniej trzydzieści sześć godzin przed kradzieżą, a poprzedzało ją rozpoznanie trwające znacznie dłużej.

Potem następuje uzyskanie pierwszego dostępu i tutaj drogi są cztery, przy czym pierwsza jest zdecydowanie najczęstsza.

Socjotechnika, czyli nakłonienie człowieka do zrobienia czegoś, co otworzy drzwi. Najskuteczniejszą jej odmianą w tej branży okazała się fałszywa rekrutacja: pracownik dostaje ofertę atrakcyjnej pracy, prowadzi kilka rozmów, a potem otrzymuje zadanie techniczne do wykonania na własnym komputerze. Uruchomienie tego zadania instaluje oprogramowanie dające dostęp do maszyny. Metoda ta stoi za kradzieżą z Ronin i za kradzieżą z DMM Bitcoin, a opisuję ją szczegółowo w podrozdziale 7.2.

Złośliwe oprogramowanie dostarczane innymi kanałami: zainfekowane biblioteki programistyczne, fałszywe aktualizacje, załączniki. W środowisku, w którym programiści codziennie pobierają setki zewnętrznych pakietów, podstawienie jednego z nich jest drogą realną i wielokrotnie wykorzystaną.

Przejęcie kont pracowników: wykradzione hasła, przechwycone kody jednorazowe, przejęcie numeru telefonu, a także zmęczenie powiadomieniami, czyli zasypywanie pracownika prośbami o potwierdzenie logowania, aż któreś zatwierdzi przez pomyłkę.

Atak na dostawcę zewnętrznego. Zamiast włamywać się do giełdy, napastnik włamuje się do firmy, której oprogramowanie giełda uruchamia u siebie. Tak przebiegał atak na Bybit, w którym punktem wyjścia był komputer dewelopera dostawcy interfejsu portfela, a nie żaden system samej giełdy.

Osobną drogą, nieprzypominającą żadnej z powyższych, są luki w smart kontraktach. Nie wymagają one włamania do czyjegokolwiek komputera, bo kontrakt jest publiczny i każdy może wysłać do niego transakcję.

Napastnik czyta kod, znajduje w nim błąd pozwalający osiągnąć stan, którego autor nie przewidział, i wysyła transakcję, która ten stan wywołuje. Wszystko odbywa się jawnie, zgodnie z regułami sieci. Z punktu widzenia protokołu nic nielegalnego się nie dzieje, co jest dokładnie tym, co stało się przy The DAO i przy Poly Network.

Z perspektywy obrony oznacza to inny rodzaj pracy. Nie pomogą tu szkolenia pracowników ani kontrola dostępu, bo atak nie przechodzi przez żadne z tych miejsc. Pomagają audyty kodu, programy nagród za znalezione błędy, ograniczenia kwot i opóźnienia przy dużych wypłatach.

Niezależnie od drogi wejścia, moment przełomowy jest zawsze ten sam: napastnik uzyskuje możliwość podpisania transakcji wychodzącej. Do tej chwili ma dostęp do systemów, a od tej chwili ma pieniądze.

Warto zauważyć, że nie zawsze oznacza to zdobycie klucza prywatnego. W sprawie Bybit klucze pozostały bezpieczne, a napastnik doprowadził do tego, że uprawnieni ludzie podpisali transakcję o innej treści niż ta, którą widzieli. W sprawie Binance klucze również nie wyciekły, a napastnik uzyskał dostęp do systemów, które wydają polecenia podpisywania, i zmusił je do wykonania swojego polecenia.

Jest to zmiana, na którą branża zwróciła uwagę dopiero po tych dwóch sprawach. Przez lata ochrona kluczy była głównym zadaniem

bezpieczeństwa. Okazało się, że chronić trzeba całą ścieżkę prowadzącą do podpisu, bo klucz doskonale zabezpieczony podpisze wszystko, co dostanie.

Samo wyprowadzenie środków trwa minuty. Przy kradzieży z Binance większość majątku opuściła giełdę w ciągu około dwudziestu minut, a pojedyncza transakcja w sieci Ethereum przekroczyła dwa i pół miliarda dolarów.

Tempo nie jest przypadkiem, lecz wymogiem. Od chwili pierwszego podejrzanego przelewu zaczyna się wyścig: analitycy oznaczają adresy, emitenci stablecoinów przygotowują zamrożenia, giełda próbuje odciąć dostęp. Każda minuta zwłoki zmniejsza łup.

Z tego samego powodu ataki przeprowadza się nocą albo w weekend, licząc na to, że zespoły dyżurne są mniejsze, decydenci niedostępni, a procedury kryzysowe wymagają kontaktu z ludźmi, którzy śpią. Kradzież z Binance nastąpiła w czwartkowy wieczór czasu uniwersalnego, co w Azji, gdzie mieści się znaczna część zespołów giełdy, oznaczało noc z czwartku na piątek.

Gdy środki są już poza zasięgiem właściciela, zaczyna się druga część operacji, trwająca znacznie dłużej niż pierwsza. Jej celem jest doprowadzenie do stanu, w którym środki da się wydać, a tego nie da się zrobić z pieniędzmi, których każdy ruch jest publicznie widoczny i oznaczony.

Pierwszym krokiem jest rozdrobnienie. Łup zostaje rozbity na setki albo tysiące adresów, w kwotach różnej wielkości, przesyłanych w różnych odstępach czasu. Celem nie jest ukrycie środków, bo każdy ruch i tak jest widoczny, lecz zwiększenie kosztu analizy i rozmycie obrazu.

Drugim jest zamiana wszystkiego, co da się zamrozić, na to, czego zamrozić nie można. Stablecoiny i tokeny z centralnym emitentem zamieniane są na ether i bitcoiny, które nie mają emitenta i których nikt nie zablokuje.

Krok ten wykonuje się natychmiast, bo każda minuta zwłoki zwiększa szansę, że emitent zdąży pierwszy. Przy kradzieży z Binance napastnik sprzedał około 325 milionów USDT wyspecjalizowanym kupcom, godząc się na zniżkę przekraczającą dziesięć procent, byle zamienić je na ether, zanim zostaną zablokowane. Reszta tej partii została zamrożona, zanim zdążył ją sprzedać.

Trzecim krokiem jest przenoszenie środków między blockchainami, nazywane chain hopping. Napastnik zamienia ether na bitcoiny, bitcoiny na

aktywa w kolejnej sieci, i tak dalej, korzystając z protokołów wymiany międzysieciowej działających bez weryfikacji tożsamości. Każde przejście między sieciami zrywa ciągłość śladu, bo wymaga od analityka połączenia dwóch odrębnych rejestrów na podstawie kwot i czasu.

Równolegle używa się mikserów, czyli usług mieszających środki wielu użytkowników, by rozerwać powiązanie między wpłatą a wypłatą. Najbardziej znanym jest Tornado Cash, a jego losy prawne opisuję w podrozdziale 7.4.

Ostatnim etapem jest wyjście do pieniądza tradycyjnego i jest on najtrudniejszy, bo w tym punkcie świat kryptowalut styka się ze światem rachunków bankowych, które mają właścicieli i nadzór.

Drogą najczęstszą są brokerzy działający poza giełdami, określani skrótem OTC. Przyjmują kryptowaluty i wypłacają gotówkę albo przelew, pobierając prowizję tym wyższą, im bardziej obciążone są środki. Część z nich działa świadomie, część nie zadaje pytań, a kilku takich pośredników objęto sankcjami.

Drugą drogą są giełdy o słabych procedurach weryfikacji klientów, działające w jurysdykcjach, które ich nie egzekwują, oraz konta zakładane na podstawione lub skradzione tożsamości. Przy sprawie Bybit istotną rolę odegrała platforma eXch, która nie weryfikowała tożsamości i odmówiła zablokowania środków mimo próśb giełdy. Ogłosiła zamknięcie działalności na 1 maja 2025 roku, a niemieckie organy ścigania przejęły jej infrastrukturę i zabezpieczyły aktywa o wartości około 38 milionów dolarów.

Charakterystyczne dla grup państwowych jest to, że nie spieszą się z ostatnim etapem. Środki potrafią leżeć na adresach miesiącami albo latami, czekając, aż uwaga opadnie, a wśród analityków pojawi się szum innych spraw. Cierpliwość jest tu przewagą, której zwykły przestępca nie ma, bo potrzebuje pieniędzy teraz.

Co do skali zjawiska, podaję liczby z podaniem źródeł, bo różnią się one między firmami w zależności od metodologii i momentu wyceny. Według TRM Labs łączne straty z włamań w kryptowalutach w całej historii wynoszą około 28 miliardów dolarów, a rok 2026 był pod tym względem najgorszy w historii: do października straty sięgnęły około 8,7 miliarda dolarów.

Dominacja jednego sprawcy jest w tych statystykach uderzająca. Według tej samej firmy Korea Północna odpowiada za około 85 procent wartości

wszystkich kradzieży kryptowalut w 2026 roku, a po wyłączeniu kradzieży z Binance nadal za około 45 procent. W 2025 roku udział ten wynosił 63 procent, w 2024 roku 39 procent, a w 2020 roku 7 procent.

Trzeci kwartał 2026 roku, który przed październikiem uchodził za wyjątkowo zły, przyniósł według firmy CertiK około 1,26 miliarda dolarów strat w 247 zdarzeniach. Pojedyncza kradzież z Binance przekroczyła tę kwotę pięciokrotnie, i to właśnie czyni ją wydarzeniem, od którego branża liczy nowy okres.

Na koniec warto zapisać jedną obserwację dotyczącą tego, jak zmieniał się w czasie najsłabszy punkt w całym tym łańcuchu, bo zmiana ta porządkuje całą resztę książki.

W pierwszym okresie, do mniej więcej 2016 roku, najsłabszym punktem był sposób przechowywania kluczy. Mt. Gox stracił środki przez skopiowanie niezaszyfrowanego pliku z serwera, a wiele mniejszych giełd z tamtych lat upadło z tego samego powodu.

W drugim okresie, mniej więcej do 2022 roku, najsłabszym punktem był kod. Mosty, protokoły i kontrakty pisano szybko, a każdy błąd w publicznym kodzie jest zaproszeniem. Rozdział czwarty tej książki opisuje właśnie ten okres.

W trzecim okresie, trwającym do dziś, najsłabszym punktem jest człowiek i proces. Klucze są dobrze chronione, kod jest poddawany audytom, a napastnicy wchodzą przez komputer pracownika, przez dostawcę oprogramowania i przez systemy wydające polecenia podpisu.

Prawidłowość ta nie jest przypadkiem. Każdy okres kończył się wtedy, gdy obrona po tej stronie stała się dostatecznie dobra, by koszt ataku przewyższył koszt znalezienia innej drogi. Napastnik idzie zawsze tam, gdzie jest taniej.

Wniosek dla ciebie jest ten sam co dla giełdy, tylko w mniejszej skali. Jeśli kupisz portfel sprzętowy i zabezpieczysz frazę, przestaniesz być celem opłacalnym dla ataków na klucze, a staniesz się celem dla ataków na to, co podpisujesz i w co klikasz. Rozdział ósmy jest ułożony dokładnie w tej kolejności.