Daniel Haczyk

Kryptowaluty – czy to bezpieczne?

Jak nie dać się okraść

Czy sieć bitcoin jest bezpieczna? Skąd można mieć pewność, że ktoś nas nie okradnie albo nie stracimy swoich pieniędzy w wyniku awarii sieci? W jaki sposób zabezpieczyć swoje oszczędności i jak nie dać się oszukać? Na te pytania postaram się odpowiedzieć w poniższym artykule.

Daniel Haczyk
Od 2013 r. właściciel i redaktor naczelny serwisu Cyfrowa Ekonomia. Właściciel firmy BitSky Multimedia, zawodowo zajmuje się marketingiem i produkcją wideo. Walutami cyfrowymi i technologią blockchain interesuje się od 2012 roku.

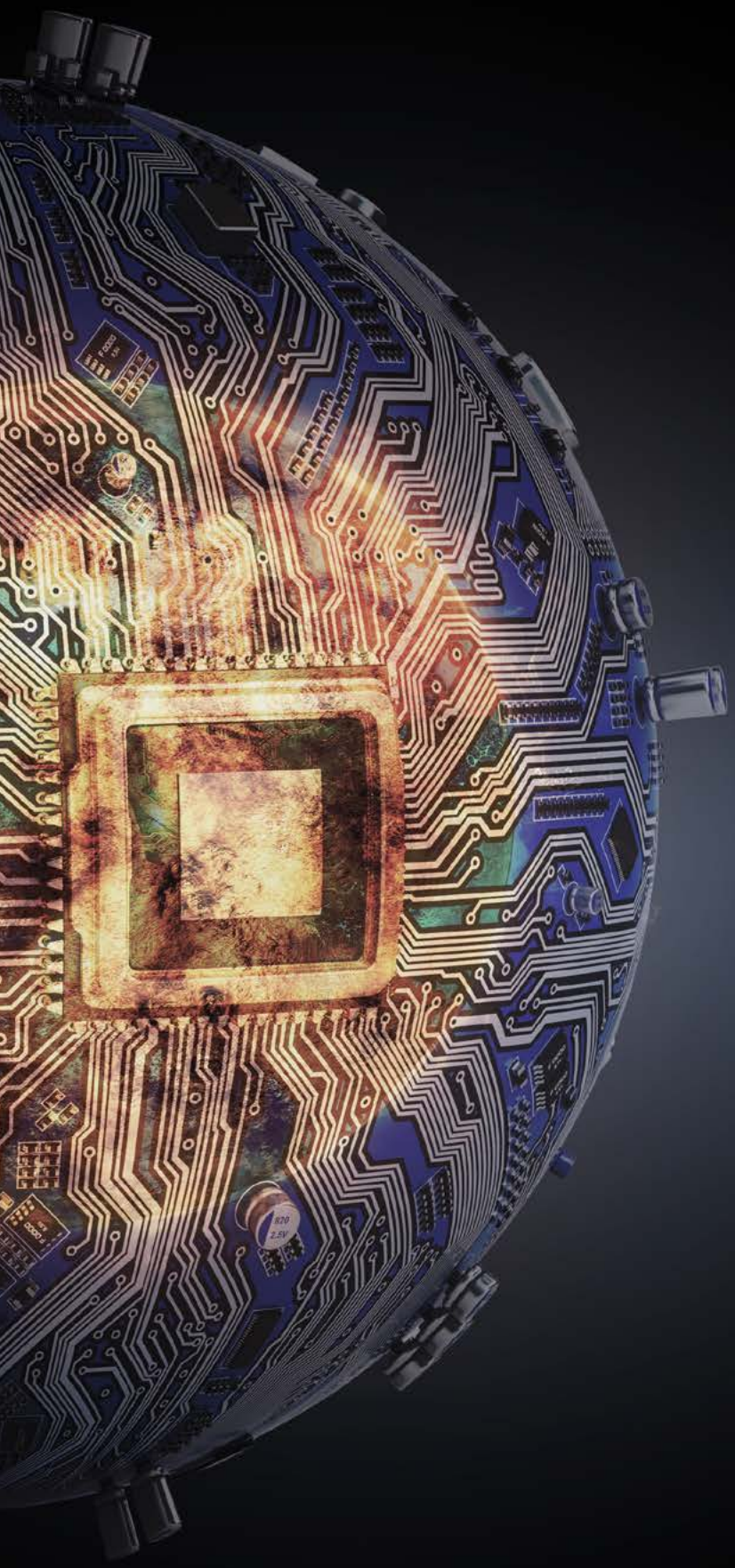
dhaczyk
daniel.haczyk1

Wiara w to, że wartość bitcoina wzrośnie, skłania do spekulacji. Kryptowaluty coraz częściej wzbudzają zainteresowanie osób, które nie przeżyły nigdy przygody z rynkami finansowymi. Wiele osób kupuje niewielkie ilości kryptowalut z wiarą, że za kilka lat będą one warte znacznie więcej. Mało kto jednak zna podstawowe zasady bezpieczeństwa i potrafi odpowiednio zadbać o swoje cyfrowe monety.

Nie można mieć bitcoinów

Można mieć tylko klucze do "bitcoinowych sejfów" i to nimi wymieniamy się, dokonując transakcji. Wynika to z zasad działania sieci. Blockchain to technologia, która pozwala na zapisanie informacji. Dzięki zabezpieczeniom kryptograficznym i znacznikom czasu, w bazie danych można zapisać nowe informacje, ale nie istnieje techniczna możliwość, żeby zmienić już istniejące zapisy. Bitcoiny tak naprawdę są tylko zapisem cyfrowym w rozproszonej bazie danych.

Blockchain rozwiązuje problem zaufania w publicznej sieci. Przesyłając bitcoiny na inny adres, sieć każdorazowo sprawdza historię pochodzenia wysyłanych monet, śledząc wszystkie transakcje, aż do momentu ich wygenerowania. Jeśli nie ma wątpliwości co do pochodzenia środków, do rejestru dodawany jest nowy zapis. Tylko właściciel klucza do danego adresu może dokonać kolejnej transakcji.



Zgadnięcie klucza prywatnego to kosmiczna abstrakcja

Bitcoin nie jest zarządzany przez żadną firmę ani instytucję. Wszystkie zabezpieczenia sieci wynikają z praw matematyki i zastosowania zaawansowanych rozwiązań kryptograficznych oraz „magii" wielkich liczb. Wygenerowanie dwóch takich samych kluczy bitcoin graniczy z cudem. Udowadnia to ten przykład:

Wyobraź sobie, że zbudowałeś komputer doskonały. Komputer, który korzysta z teoretycznego minimum energii koniecznej do zanotowania zmiany przy pojedynczym bicie (z 1 na 0 lub 0 na 1). Ograniczenia termodynamiki sprawiają, że dalsze usprawnienia nie są możliwe.

Teraz wyobraź sobie, że, korzystając z większości surowców naturalnych dostępnych w naszym układzie gwiezdnym, udało Ci się stworzyć Sferę Dysona. Powierzchnię sfery pokrywasz pojedynczym superkomputerem wielkości całego układu gwiezdnego.

Następnie wyobraź sobie, że możliwe jest utrzymanie temperatury superkomputera na poziomie zera absolutnego bez wykorzystania dodatkowej energii.

Gdybyś dysponował takim rozwiązaniem i udałoby Ci się wychwycić całość energii generowanej przez naszą gwiazdę, przez cały okres jej życia, niemożliwe byłoby doliczenie do 2^256 przed wyczerpaniem energii.

Pamiętajmy, że mowa tu wyłącznie o liczeniu. Wyłącznie – bez hashowania, porównywania, wyszukiwania; tylko liczymy: 1..2..3?.2^256-1.

Działania te nie mają nic wspólnego z technologią urządzeń – są to maxima, na które pozwala termodynamika.

Wynika z nich, że brutalne ataki na klucze 256-bitowe będą nieopłacalne tak długo, jak komputery będą składać z czegoś innego niż materia i zajmować coś innego niż przestrzeń.

Bitcoin – Twoich pieniędzy strzegą prawa wszechświata.

Dzięki temu rozwiązany jest problem „podwójnego wydania" środków. Nie można dwa razy wydać tych samych monet, w taki sposób, jak można skopiować plik na komputerze – ta cecha czyni kryptowaluty wyjątkowymi.

Właśnie dlatego nie można mieć bitcoinów – można mieć tylko klucz dostępu, który pozwala na zamianę cyfrowego zapisu. Klucz ten jest na tyle długi i unikatowy, że nikt nie jest w stanie go podrobić.

Gdyby ktoś mimo wszystko był ciekawy dokładnej liczby, zgadnięcie 256-bitowego klucza prywatnego to prawdopodobieństwo: 1:115 792 089 237 316 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000, czyli odpowiednik wyrzucenia 256 razy z rzędu reszki podczas rzutu monetą (1 bit to zawsze jedynka lub zero, dlatego porównanie do rzutu monetą jest bardzo adekwatne).

Przypominam, że trafienie szóstki w totolotka to prawdopodobieństwo mniej więcej 1:14 000 000, natomiast np. zgadnięcie numeru karty kredytowej to około 1:9 007 199 254 740 990.

Najsłabszy element to człowiek

Kod źródłowy bitcoina jest jawny, a użyta w nim kryptografia i zastosowanie wielkich liczb gwarantują bezpieczeństwo sieci. Cytując prof. Mariana Srebrnego z Państwowej Akademii Nauk: „rozwiązania kryptograficzne (w bitcoinie) są na najwyższym możliwym poziomie". Taka sama kryptografia zabezpiecza nie tylko domeny internetowe i systemy bankowe, ale właściwie całą sieć Internetu.

Bitcoin jest najstarszą kryptowalutą, która w styczniu 2019 roku skończyła 10 lat. Fakt, że rejestr transakcji jest przechowywany na tysiącach komputerów w sieci i każdy może zrobić swoją kopię tej bazy danych, sprawia, że nie trzeba się obawiać awarii sieci. W przeciwieństwie do systemów bankowych, aktualizacje sieci bitcoin nie wiążą się z koniecznością zatrzymania sieci.

Rozproszenie gwarantuje bezpieczeństwo rejestru również w momencie awarii Internetu albo blokady regionalnej, a moc obliczeniowa koparek (urządzeń zabezpieczających działanie sieci), jest wielokrotnie wyższa od mocy obliczeniowej wszystkich superkomputerów z listy top 500 razem wziętych. Sprawia to, że próba przejęcia kontroli nad siecią kosztowałaby więcej niż wynosi kapitalizacja całego rynku.

Przez dziesięć lat działania sieci bitcoin miała miejsce tylko jedna awaria – w sierpniu 2010 roku. Trwała ona około 8 godzin, pomiędzy blokami 74638 a 74691. W wyniku błędu w implementacji stworzonych zostało 184 mld nowych bitcoinów. Błąd został natychmiast wykryty i załatany. 8 godzin trwało upewnienie się, że cała sieć jest w łańcuchu nieakceptującym wadliwej transakcji.

Najsłabszym ogniwem zarówno w tym, jak i we wszystkich innych systemach zabezpieczeń okazał się człowiek. Największym zagrożeniem dla użytkowników kryptowalut jest niestosowanie się do podstawowych zasad bezpieczeństwa w sieci.

Trzymasz oszczędności na giełdzie? Odważnie!

Większość niedoświadczonych użytkowników kryptowalut przechowuje swoje środki na giełdach. Jest to wygodne rozwiązanie, ponieważ w każdym momencie można dokonać wymiany na inną walutę i wypłacić swoje oszczędności.

Mało osób jednak zdaje sobie sprawę z tego, że trzymając pieniądze na giełdzie, powierzamy je opiece prywatnej firmy, podobnie jak w sytuacji, w której zdeponowalibyśmy środki w banku. Różnica jest taka, że giełdy nie są bankami.

"Not your keys, not your bitcoin!"

Andreas M. Antonopoulos

To giełda zazwyczaj przechowuje klucze prywatne do adresów i giełda zarządza tymi adresami. Każda z giełd posiada wypracowane przez siebie procedury bezpieczeństwa. Większość środków przechowywana jest na tak zwanych 'zimnych portfelach', bez połączenia z Internetem. W takim przypadku, w sytuacji ataku hakerskiego na giełdę większość kryptowalut powinna być bezpieczna.

Historia pokazała jednak, że błędy w oprogramowaniu giełd się zdarzają. Giełdy są także celem hakerów, a zgromadzone na nich duże pieniądze prowokują oszustów. Najbardziej znanym przykładem jest historia giełdy Mt.Gox. która straciła 750 000 bitcoinów swoich klientów i zniknęła z sieci.

Jeśli w Polsce upadnie bank, to Bankowy Fundusz Gwarancyjny gwarantuje zazwyczaj zwrot wszystkich depozytów do równowartości 100 000 euro. Giełdy zwykle nie są zabezpieczone na takie ewentualności.

Rok	Giełda	Kwota
lipiec 2011	Mt.Gox	30 000 USD
październik 2011	Bitcoin7	50 000 USD
wrzesień 2012	BitFloor	250 000 USD
maj 2013	Vircurex	50 000 000 USD
listopad 2013	Inputs.io	1 200 000 USD
listopad 2013	BIPS	1 000 000 USD
listopad 2013	PicoStocks.com	6 000 000 USD
luty 2014	Mt.Gox	460 000 000 USD
marzec 2014	Poloniex	50 000 USD
lipiec 2014	Cryptsy	9 500 000 USD
lipiec 2014	Mintpal	2 000 000 USD
październik 2014	BitPay	1 800 000 USD
październik 2014	Mintpal	1 500 000 USD
styczeń 2015	796 Exchange	230 000 USD
styczeń 2015	Bitstamp	5 100 000 USD
luty 2015	Bter.com	1 750 000 USD
sierpień 2016	Bitfinex	72 000 000 USD
kwiecień 2017	Yapizon	5 300 000 USD
kwiecień 2017	YouBit	17% zasobów w krypto
grudzień 2017	NiceHash	60 000 000 USD
styczeń 2018	Coincheck	534 800 000 USD
luty 2018	BitGrail	195 000 000 USD
kwiecień 2018	CoinSecure	3 300 000 USD
czerwiec 2018	Coinrail	40 000 000 USD
czerwiec 2018	BitHumb	31 500 000 USD
wrzesień 2018	Zaif	60 000 000 USD

▲ *Przypadki utracenia funduszy przez giełdy*

W przypadku utraty pieniędzy przez giełdę nikt nie pokryje strat klientów.

Giełdom zależy jednak na zaufaniu, dlatego w Polsce powstał już podobny fundusz gwarancyjny – Crypto Security Fund. Niestety jest to dość młody projekt i nie obejmuje swoją gwarancją największych giełd – jest to jednak krok w dobrą stronę.

Warto podkreślić jednak, że nawet jeśli kiedyś giełdy zostaną objęte gwarancją depozytów, to wciąż pozostaną inne zagrożenia. Atakujący może przejąć kontrolę nad komputerem i telefonem użytkownika, a następnie wyprowadzić bitcoiny z giełdy. Sieć bitcoin chroni prawo własności, dlatego transakcji nie można cofnąć – skradzione pieniądze są nie do odzyskania.

Bezpieczeństwo na poziomie portfela

Portfele kryptowalutowe służą do przechowywania wszystkich naszych kluczy – a te dają dostęp do naszych adresów kryptowalutowych. Każdy klucz to nic innego jak ciąg znaków. Jest on długi i trudny do zapamiętania.

Istnieje wiele rodzajów portfeli kryptowalutowych – portfele online, do których można zalogować się przez przeglądarkę, oraz takie instalowane bezpośrednio na smartfonie lub komputerze. Złośliwe oprogramowanie może próbować ukraść nasze oszczędności. Zabezpieczenie portfela hasłem albo korzystanie z dwuskładnikowego uwierzytelniania na giełdach nie daje gwarancji, że nikt nas nie okradnie.

Najlepiej jest przechowywać swoje klucze offline, z dala od komputera.

Teoretycznie można przechowywać klucze we własnej pamięci i, kiedy jest to konieczne, przepisać ciąg znaków do komputera.

Takie rozwiązanie jest popularne wśród wyjeżdzających z upadającej gospodarczo Wenezueli - pozwala przewieźć swoje środki przez granicę i uniknąć konfiskaty dużych zasobów gotówki i złota.

Obecnie wiele portfeli jest w stanie wygenerować klucz na podstawie 12 do 24 słów (tzw. *seed*) ze specjalnie przygotowanego słownika. Co ciekawe, prawdopodobieństwo odgadnięcia 24 losowych słów ze słownika BIP39 (Bitcoin Improvement Proposal 0039) jest nawet mniejsze niż odgadnięcie 256-bitowego klucza, które opisałem już w artykule. Ponadto twórca portfela nie ma wpływu na wygenerowany *seed*, nie może go w żaden sposób przewidzieć ani podejrzeć. Zapisując te słowa zatem, nawet na zwykłej kartce, można w przyszłości, gdyby portfel przepadł, odzyskać dostęp do bitcoinów.

Jeśli jednak zapiszemy taki klucz na kartce papieru, to istnieje ryzyko, że kartka zamoknie albo się spali. Z tego powodu stworzono specjalny metalowy portfel, który pozwoli na zapisanie klucza albo słów pozwalających na jego odzyskanie. Cryptosteel to polski projekt, który podbił świat. Metalowy portfel jest w stanie przetrwać w ogniu, wodzie albo zakopany w ogrodzie.

Co, jeśli ktoś chciałby korzystać z sieci i dokonywać transakcji? W takiej sytuacji najlepszym uzupełnieniem dla metalowego portfela będą portfele sprzętowe, takie jak Trezor czy Ledger. Zapewniają one bezpieczeństwo nawet w sytuacji, kiedy komputer lub smartfon byłyby pod kontrolą przestępcy.

W momencie dokonywania transakcji konieczne jest podanie kodu PIN, który odblokuje dostęp. Dzięki temu, że cyfry wyświetlają się na ekranie urządzenia w losowej kolejności, osoba, która miałaby dostęp do komputera ofiary, nie byłaby w stanie podejrzeć kodu.

Każda transakcja musi zostać zatwierdzona manualnie na urządzeniu. Urządzenie najczęściej wyświetla sumę i adres, na który mają zostać przesłane środki. Dzięki temu użytkownik portfela ma pewność, że nikt nie podmienił adresu docelowego ani kwoty. Po zatwierdzeniu przez użytkownika, transakcja jest podpisywana i odsyłana do komputera. Klucze nigdy nie opuszczają portfela sprzętowego.

Tego typu urządzenie ma również inne zastosowania. Może służyć jako U2F, czyli uniwersalny drugi poziom zabezpieczenia kont w serwisach. Aplikacje do dwuskładnikowego uwierzytelniania, takie jak Google Authenticator, nie dają takiej gwarancji bezpieczeństwa.

Trezor ma jeszcze jedną zaletę, może bowiem służyć jako menedżer haseł. Ustawiając indywidualne hasła do każdego ze swoich kont, trudno je wszystkie zapamiętać. Zapisanie haseł na komputerze albo w przeglądarce nie jest bezpiecznym rozwiązaniem. Trezor pozwala na przechowywanie haseł w formie zaszyfrowanej, a dostęp do nich wymaga podania kodu PIN i zatwierdzenia na urządzeniu. Daje to gwarancję bezpieczeństwa danych.

Pojawiają się również nowe, coraz ciekawsze urządzenia. O niektórych z nich, jak na przykład Portfel Coldcard, przeczytasz pokrótce w stałym dziale **Kryptogadżety**, a obszerniej wtedy, kiedy dane będzie nam je przetestować.

Podsumowanie

Zabezpieczenia samej sieci bitcoin są bardzo dobre i najsłabszym punktem całego systemu jest użytkownik kryptowalut.

Warto pamiętać o tym, żeby odpowiednio zabezpieczyć swój kapitał, tak aby nie stracić dostępu do portfela albo nie zostać okradzionym.

Portfele na telefonie lub komputerze są wygodne, ale lepiej nie trzymać na nich więcej niż jest się w stanie stracić. Podobnie sytuacja ma się w przypadku giełd.

Sprzętowe portfele nie kosztują dużo, a pozwalają użytkownikom kryptowalut spać spokojnie. Na koniec warto też zadać sobie pytanie, co się stanie z twoimi bitcoinami po śmierci, w jaki sposób należałoby odpowiednio zabezpieczyć spadek – ale to już temat na osobny artykuł.