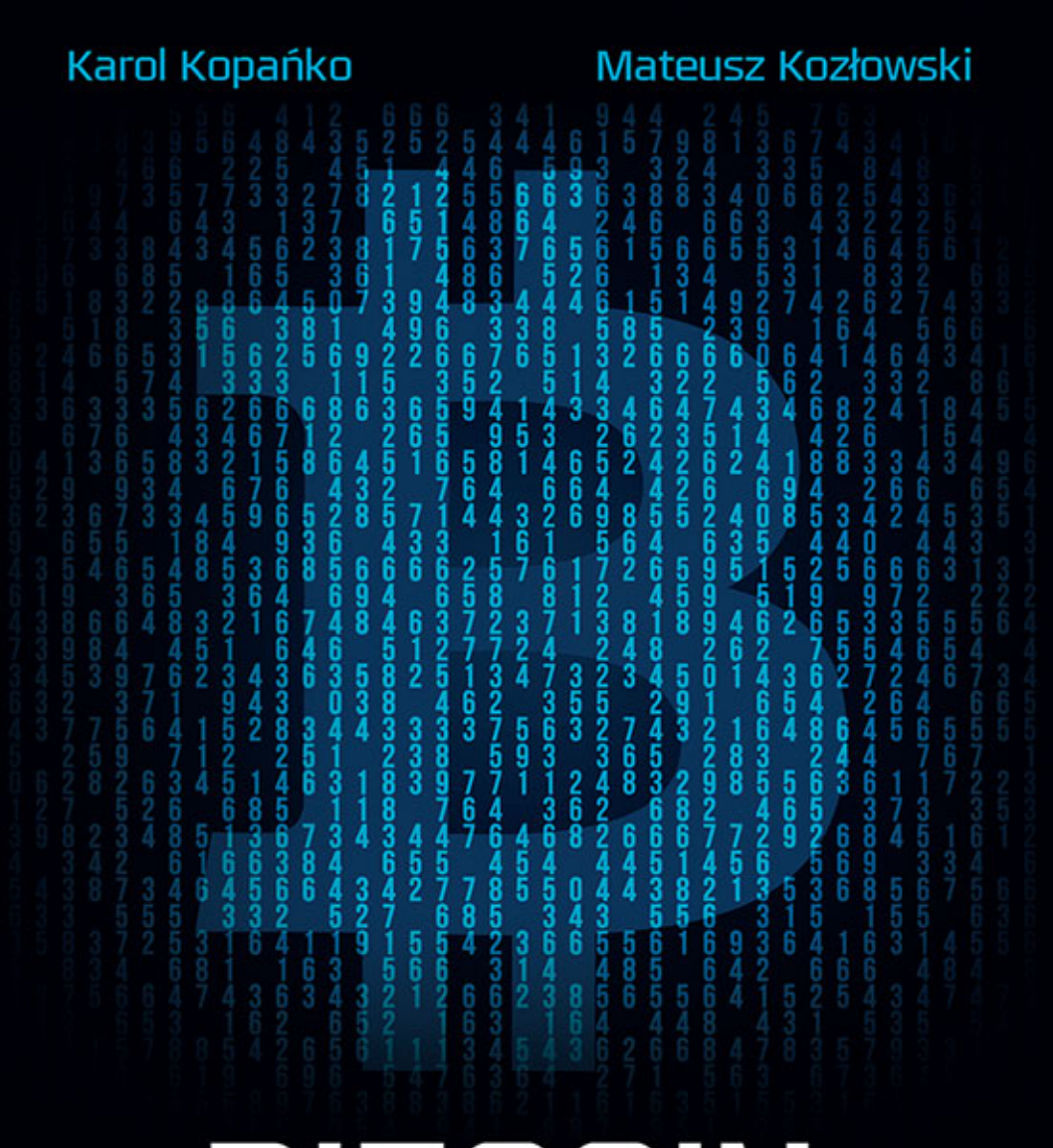
Karol Kopańko Mateusz Kozłowski



BITCOIN

ZŁOTO XXI WIEKU

one press

Redaktor prowadzący: Barbara Gancarz-Wójcicka
Projekt okładki: Jan Paluch

Fotografia na okładce została wykorzystana za zgodą Shutterstock.

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *onepress@onepress.pl*
WWW: *http://onepress.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://onepress.pl/user/opinie/bitzlo
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-246-9748-9

Printed in Poland.

Spis treści

Zakładamy portfel

Jednym z pierwszych kroków osoby aspirującej do posiadania Bitcoina może być ściągnięcie klienta (choć można się bez niego obyć, zakładając konto w chmurze — o czym dalej).

Pierwszy rodzaj klientów reprezentuje oficjalny program tworzony przez społeczność Bitcoina. Nazywa się on Bitcoin Core i jego instalacja jest bardzo czasochłonna, gdyż musi się on zsynchronizować z całą siecią, co oznacza pobranie wielogigabajtowej paczki danych. Paczka zawiera informacje o transakcjach przeprowadzonych od samego początku istnienia tej wirtualnej waluty[44]. Synchronizacja informacji o transakcjach dokonywana jest później codziennie, jednak wtedy nie trwa to już długo, ponieważ pobierana jest mniejsza ilość danych. Co istotne, zakończenie procesu synchronizacji nie jest wymagane do otrzymywania bitcoinów, gdyż nasz adres jest generowany odpowiednio wcześniej. Jeśli natomiast chcemy bitmonety wysyłać, musimy cierpliwie poczekać na zakończenie całej synchronizacji lub skorzystać z innego rodzaju portfeli.

Bitcoin nie jest do końca wolny od opłat transakcyjnych. Stała opłata za dokonanie transakcji wynosi 0,0001 BTC, a jej wysokość możemy wedle uznania powiększać. Zapewne możesz się w tej chwili poczuć nieco zdezorientowany, ponieważ wedle standardowego myślenia zwiększanie opłaty po prostu nie

[44] *http://www.coindesk.com/bitcoin-core-developers-bitcoin-side-chains/*

ma sensu. Jednak w przypadku Bitcoina opłata ta jest jednocześnie swoistą nagrodą oferowaną innym klientom w sieci za jak najszybszą weryfikację transakcji. Dlatego im jest większa, tym szybciej zachodzi autoryzacja danej transakcji i tym szybciej jej odbiorca może się cieszyć wpływem wirtualnej waluty do swojej „kieszeni".

Sejf

Jeśli pragniemy większej dozy bezpieczeństwa, to możemy się również zaopatrzyć w oprogramowanie Armory[45]. Jest to klient, który posiada dużą liczbę zaawansowanych funkcji, dzięki którym możemy łatwo wykonywać kopie bezpieczeństwa swojego portfela, a także przechowywać portfele na komputerach niepodłączonych do sieci. Działa on razem z Bitcoin Core.

Jeśli zaś nie mamy czasu albo nie chcemy korzystać z zaawansowanych funkcji oficjalnego klienta, to możemy zadowolić się portfelem takim jak Multibit[46]. Nie przechowuje on bloków na dysku i dlatego działa od razu po uruchomieniu. Jest on szczególnie polecany osobom rozpoczynającym przygodę z Bitcoinem, które odstrasza pobieranie wielu gigabajtów danych, aby spokojnie korzystać z Bitcoin Core.

Na smartfonie

W związku z tym, że coraz więcej spraw załatwiamy przy użyciu smartfona, pojawiła się potrzeba stworzenia aplikacji mobilnej, która mogłaby obsługiwać nasz portfel. Jedną z takich aplikacji jest Bitcoin Wallet, działający na Androidzie i BlackBerry. Apple początkowo usunęło wszystkie aplikacje portfele ze swojego App Store'a[47]. Są one już ponownie dostępne. Wielu użytkowników iPhone'ów mocno protestowało przeciwko takiej cenzurze i firma

[45] *https://bitcoinarmory.com/*

[46] *https://multibit.org/*

[47] *http://www.businessinsider.com/why-apple-is-anti-bitcoin-apps-right-now-2014-2*

z Cupertino przywróciła możliwość pobierania aplikacji do obsługi BTC. Organizacja stworzona przez wizjonera najwyraźniej doszła do wniosku, że zakazywanie Bitcoinów nie było najlepszym pomysłem.[48] Dzięki niemu możemy dokonywać szybkich płatności, używając aparatu jako skanera kodów QR. Pod ich postacią można zapisać adresy bitcoinowych portfeli. Dodatkowo, jeśli nasz telefon wyposażony jest w łączność NFC (*Near Field Communication*), wystarczy, abyś zbliżył telefon do czytnika sprzedawcy, a urządzenia zostaną sparowane i odpowiedni algorytm samodzielnie dokona płatności. Wadą Bitcoin Wallet jest to, że zapisuje on klucze prywatne w telefonie, dlatego jeśli ktoś zgubi telefon, to może się pożegnać ze swoimi bitcoinami… (o ile oczywiście nie zrobił sobie zawczasu kopii bezpieczeństwa). Ludzie dzielą się na tych którzy robią backupy i na tych, którzy będą robili.

CZY WIESZ, ŻE...

Kiedy Apple usunęło z App Store'a aplikację najpopularniejszego bitcoinowego portfela, rozwścieczyło to internautów do tego stopnia, że jeden z użytkowników portalu *reddit.com* zaoferował, iż sprezentuje telefon Nexus 5 osobom, które nagrają film wideo pokazujący, jak niszczą swojego iPhone'a. Przynajmniej kilka osób przystało na jego propozycję, a relacje z niszczenia iPhone'ów można teraz oglądać na YouTube.

Źródło: ***http://www.reddit.com/r/Bitcoin/comments/1x62we/for_every_100_upvotes_this_post_receives_i_will***

Portfel w obłokach

Do tej pory rozpatrywaliśmy programy, które zapisują dane na posiadanych przez nas pamięciach. Co jednak z portfelami działającymi w chmurze? Istnieje ich kilka, a najpopularniejsze to Blockchain.info i Coinbase. W jaki sposób użytkowanie obu portfeli przebiega w praktyce?

[48] *http://www.wired.com/2014/07/blockchain-back/*

Ich założenie i prowadzenie jest darmowe, a także nie wymaga żadnej technologicznej wiedzy. Jeśli posiadasz internetowe konto w banku, to i tu odnajdziesz się prawie jak u siebie w domu. Podstawowa funkcjonalność obu portfeli to oczywiście wysyłanie i odbieranie bitcoinów. Zawierają one także książki adresowe, dzięki czemu nie musimy za każdym razem kopiować adresu, na jaki chcemy przesłać cyfrowe pieniądze.

Tu jednak zaczynają się różnice. Coinbase jako jedyny umożliwia też transfery z wykorzystaniem tylko i wyłącznie adresu e-mail zamiast klucza — wtedy adresat otrzymuje link do założenia portfela, w którym znajdzie od razu przygotowaną dla niego kwotę. Coinbase wydaje się także portfelem bardziej skonsolidowanym, gdyż ma on wbudowany kantor wymiany na inne waluty, a także posiada gotowe rozwiązania dla przedsiębiorców chcących rozliczać się z klientami w bitcoinach. Coinbase udostępnia po prostu swoje API, które administratorzy mogą włączyć w kod strony. To rozwiązanie sprawia, że dokonanie płatności jest bardzo łatwe w obsłudze, gdyż z punktu widzenia płacącego w sklepie internetowym sprowadza się do kliknięcia widocznych przycisków takich jak *Kup* czy *Ofiaruj*, zupełnie jak w przypadku PayPala. Dodatkowo do tego portfela możemy podłączyć swoje konto bankowe (tylko w USD) i bez przeszkód przelewać pomiędzy nimi środki. Korzystanie z usług Coinbase to w rzeczywistości powierzenie im kontroli nad swoimi bitcoinami. Bardziej rozsądnym rozwiązaniem jest korzystanie z portfela w formie aplikacji.

Apple nie lubi Bitcoina

Centrum dowodzenia obu serwisów jest strona internetowa, ale jeśli wolimy korzystanie ze smartfona, to, o ile go macie, możecie także skorzystać z dostępnych aplikacji.

Do tej pory jedyną przewagą Blockchain.info wydawała się prostota, ale prawda jest taka, iż jest to również zdecydowanie większa otwartość platformy w porównaniu z Coinbase. Z jej

poziomu możemy przeglądać wszystkie transakcje zapisywane w Blockchainie, a także dowolnie ściągać swój portfel, przesyłać go do Dropboxa, Google Drive albo nawet wydrukować. Coinbase natomiast przechowuje wszystkie te informacje i klucze publiczne na swoich serwerach.

Można więc z tego wysnuć wniosek, że Coinbase nastawia się bardziej na zbudowanie pozycji bitcoinowego banku. Podobnie jak w przypadku tradycyjnych instytucji finansowych, Coinbase przeznacza tylko 1% posiadanych środków na bieżącą obsługę klientów (*hot wallet*), a pozostałą część funduszy trzyma w bezpiecznym cyfrowym skarbcu (*cold wallet*). Zapewnia też wiele dodatkowych usług, a także jest bardziej przyjazny użytkownikowi.

Blockchain.info można za to polecić już nieco bardziej zaawansowanym użytkownikom, ze względu na jego elastyczność i komplet analitycznych danych o handlu bitcoinami. Jest to także lepsze rozwiązanie dla osób, które boją się niestabilności i tego, że jakiś serwis może z dnia na dzień wyparować z internetu. W przypadku usługi Blockchaina panem sytuacji przez cały czas pozostaje klient, który ze swoimi kluczami (prywatnym i publicznym) może robić, co chce. Dlatego nawet jeśli z jakichś niewyjaśnionych przyczyn usługa Blockchain przestanie istnieć, to to samo nie stanie się z Twoimi pieniędzmi.

Na koniec otwarta pozostaje jeszcze kwestia, czy lepiej skorzystać z usług świadczonych w chmurze, czy może tradycyjnie pozostawiać bitcoiny na dysku komputera. Na komputerze zwykle bez naszej wiedzy mogą grasować szkodliwe wirusy, dla których pozyskanie naszych kluczy czy nawet zorientowanie się w hasłach dostępowych i loginach nie jest problemem. Ba, niebezpieczne są nawet wtyczki nieznanego pochodzenia instalowane w przeglądarkach, których zadaniem jest na przykład śledzenie tego, co wpisujemy na klawiaturze i jakie strony odwiedzamy. Aby się przed tym ustrzec należy przestrzegać tzw. higieny komputerowej, polegającej na posiadaniu zawsze aktualnego systemu operacyjnego i antywirusowego a także na nie klikaniu

w podejrzane linki. Chmura może być dobrym rozwiązaniem na przechowywanie niewielkich, „testowych" ilości BTC. Pełne bezpieczeństwo zapewnia tylko i wyłącznie portfel offline.

Ty to Ty?

Aby zwiększyć bezpieczeństwo korzystania z Bitcoina, należy także koniecznie skorzystać z uwierzytelniania dwuskładnikowego. W przypadku tradycyjnego banku działa ono tak, że kiedy chcemy wykonać przelew, to nie dość, że musimy się zalogować na konto, podając identyfikator i hasło (pierwszy składnik uwierzytelniania), to jeszcze jesteśmy proszeni o potwierdzenie transakcji z wykorzystaniem drugiego składnika — na przykład otrzymujemy kod SMS-em. Bardziej zaawansowani użytkownicy (a może raczej tacy, którzy bardziej obawiają się o swoje środki) mają do dyspozycji także tokeny. Mogą to być zarówno zewnętrzne urządzenia podpinane do sieci, jak i aplikacje na smartfony. Jeszcze inną metodą weryfikacji tożsamości jest zastosowanie biometryki, w ramach której możemy skorzystać na przykład ze skanerów linii papilarnych bądź siatkówki. Specjalne aplikacje służące do tego celu pojawiły się już w Google Play i App Store.

Przyjrzyjmy się więc, jak wygląda taka dwuskładnikowa weryfikacja w przypadku Blockchain.info. Możemy tu oczywiście skorzystać z wiadomości przesyłanej SMS-em albo mailem. Ciekawą metodą jest także użycie Google Authenticatora, darmowej aplikacji na Androida, która generuje kody potwierdzające, że to właśnie my znajdujemy się w posiadaniu telefonu. Jeszcze większą dozę bezpieczeństwa zapewnia Yubikey. Jest to specjalne urządzenie, które wygląda jak pendrive i jest podłączane do komputera przez wejście USB. Logując się, wpisujemy hasło, a strona sama weryfikuje informacje i autentyczność Yubikeya. Ta metoda chroni nas dodatkowo przed trojanami oraz hakerami, co jest chyba największą zaletą dla osób dbających o bezpieczeństwo.

Wirtualny pieniądz — praktyczne zastosowanie

Bitcoin to fenomen. Mówią o nim media, sprzeczają się o niego politycy, spekulanci upatrują w nim szansy na błyskawiczne wzbogacenie się. Czasem jakaś gazeta pochyli się nad technologicznym geniuszem bitcoina, jednak znacznie częściej wybierze temat o kradzieżach i wykorzystywaniu cyfrowej waluty do nabywania narkotyków lub broni.

Czym tak naprawdę jest bitcoin?

Nie każdy musi angażować się w społeczność bitcoina albo śledzić na bieżąco kursy jego wymiany na złotówki. Jednak każdy, kto nie chce przegapić prawdziwej rewolucji, powinien rozumieć, czym jest i w jaki sposób działa ta wirtualna waluta. Ta książka to kompendium wiedzy o bitcoinie, które pomoże poznać i zrozumieć jego istotę osobom spoza branży finansowej czy branży nowoczesnych technologii.

Świat bitcoina to dla nas wciąż nowość, mimo że w niektórych krajach ten twór funkcjonuje już jako waluta. Tak jest na przykład w Niemczech, w krajach skandynawskich i na Cyprze, gdzie bitcoiny można wypłacić z bankomatu. W tym tkwi piękno bitcoina — nie jest narzucany z góry, a jego zastosowanie to kwestia wolnego wyboru.

Bitcoin to jednak nie tylko rewolucja w płatnościach — to mechanizm, który może kompletnie wywrócić naszą rzeczywistość i zmienić zasady gry.

To złoto XXI wieku!

książkiklasybusiness

Nr katalogowy: 23780

Księgarnia internetowa: http://onepress.pl

Zamówienia telefoniczne: 0 801 339900 0 601 339900

one press

Sprawdź najnowsze promocje: http://onepress.pl/promocje
Książki najchętniej czytane: http://onepress.pl/bestsellery
Zamów informacje o nowościach: http://onepress.pl/nowosci

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: onepress@onepress.pl
http://onepress.pl

Cena 31,90 zł
ISBN 978-83-246-9748-9
9 788324 697489