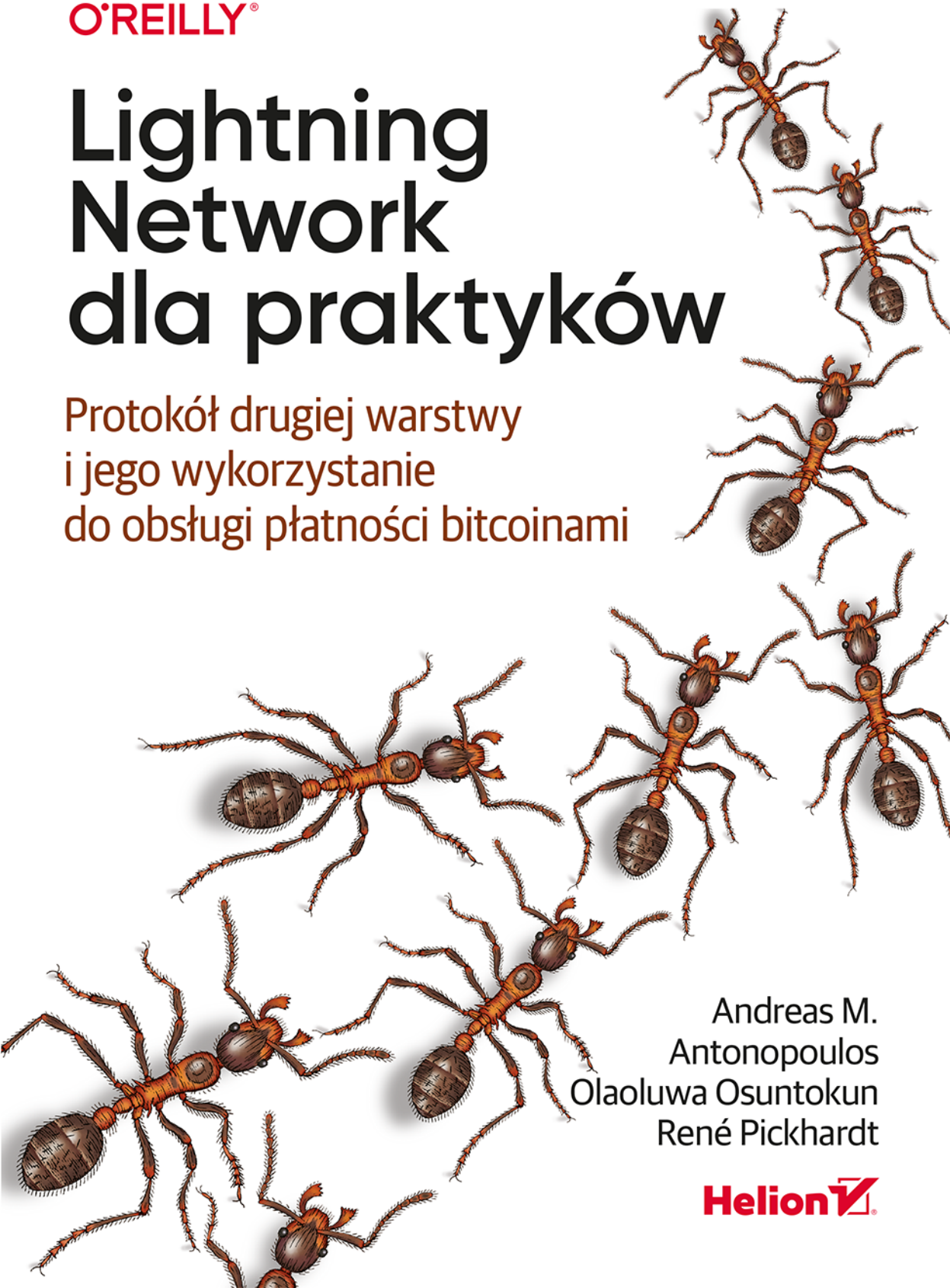
O'REILLY®

Lightning Network dla praktyków

Protokół drugiej warstwy i jego wykorzystanie do obsługi płatności bitcoinami



Andreas M. Antonopoulos
Olaoluwa Osuntokun
René Pickhardt

Helion

Tytuł oryginału: Mastering the Lightning Network: A Second Layer Blockchain Protocol for Instant Bitcoin Payments

Tłumaczenie: Radosław Meryk

ISBN: 978-83-283-9322-6

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

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

Część II. Lightning Network w szczegółach

ROZDZIAŁ 2.

Pierwsze kroki

W tym rozdziale zaczniemy od tego, od czego zaczyna większość osób, gdy po raz pierwszy spotyka się z Lightning Network — wyboru oprogramowania do korzystania z ekonomii LN. Przeanalizujemy wybory dwóch użytkowników reprezentujących powszechny przypadek użycia Lightning Network i będziesz uczyć się na ich przykładzie. Alicja, klientka kawiarni, będzie używać portfela Lightning na swoim urządzeniu mobilnym, aby płacić za kawę z „Kawiarni u Bogdana". Bogdan, handlowiec, będzie używał węzła Lightning i portfela do utrzymywania systemu punktów sprzedaży w swojej kawiarni, dzięki czemu będzie mógł akceptować płatności za pośrednictwem Lightning Network.

Pierwszy portfel Lightning Alicji

Alicja od dawna korzysta z sieci Bitcoin. Po raz pierwszy spotkaliśmy się z nią w rozdziale 1. książki *Mastering Bitcoin*[1], gdy za pomocą transakcji Bitcoin kupowała filiżankę kawy w kawiarni u Bogdana. Jeśli jeszcze nie wiesz, jak działają transakcje Bitcoin, lub potrzebujesz przypomnienia, przeczytaj książkę *Mastering Bitcoin* lub podsumowanie w dodatku A.

Alicja niedawno się dowiedziała, że w „Kawiarni u Bogdana" zaczęto akceptować płatności LN! Alicja bardzo by chciała poznać technologię Lightning Network i poeksperymentować z nią. Postanowiła stać się jednym z pierwszych klientów Bogdana korzystających z LN. Aby to zrobić, Alicja musi najpierw wybrać portfel Lightning, który spełnia jej potrzeby.

Alicja nie chce powierzać opieki nad swoimi bitcoinami podmiotom zewnętrznym. Dowiedziała się o kryptowalutach wystarczająco dużo, aby wiedzieć, w jaki sposób korzystać z portfela. Potrzebuje również portfela mobilnego, umożliwiającego dokonywanie niewielkich płatności w podróży. Dlatego wybrała portfel Eclair, popularny *niepowierniczy* (ang. *non custodial*) mobilny portfel Lightning. Zaraz powiemy więcej o tym, jak i dlaczego dokonała takiego wyboru.

[1] Andreas M. Antonopoulos, *Mastering Bitcoin*, wydanie drugie, O'Reilly, rozdział 1. (*https://github.com/bitcoinbook/bitcoin book/blob/develop/ch01.asciidoc*).

Węzły Lightning

Dostęp do sieci Lightning Network można uzyskać za pośrednictwem aplikacji, które mogą się komunikować za pomocą protokołu LN. Węzeł Lightning Network (zwany również węzłem LN lub po prostu węzłem) to aplikacja, która ma trzy ważne funkcje. Po pierwsze, węzły Lightning są portfelami, więc wysyłają i odbierają płatności za pośrednictwem sieci Lightning Network, a także w sieci Bitcoin. Po drugie, węzły muszą się komunikować z innymi węzłami Lightning tworzącymi sieć na zasadach *peer-to-peer*. Na koniec, węzły Lightning potrzebują dostępu do sieci blockchain Bitcoina (lub sieci blockchain innych kryptowalut) w celu zabezpieczenia środków używanych w płatnościach.

Użytkownicy mogą uzyskać najwyższy stopień kontroli dzięki uruchomieniu własnego węzła Bitcoin i węzła Lightning. Do interakcji z siecią blockchain Bitcoin węzły Lightning mogą jednak również korzystać z prostego klienta Bitcoin, powszechnie określanego jako SPV (ang. *simplified payment verification*).

Eksploratory Lightning

Eksploratory LN są przydatnymi narzędziami do wyświetlania statystyk węzłów, kanałów oraz monitorowania możliwości sieci.

Oto kilka przykładów eksploratorów Lightning:

- 1ML (*https://1ml.com*),
- ACINQ (*https://explorer.acinq.co*), z wyszukanymi wizualizacjami,
- Amboss Space (*https://amboss.space*), z metrykami społeczności i intuicyjnymi wizualizacjami,
- Fiatjaf (*https://ln.bigsun.xyz*), z wieloma wykresami,
- hashXP (*https://hashxp.org/lightning/node*).

Należy pamiętać, że podczas korzystania z eksploratorów Lightning, podobnie jak innych eksploratorów bloków, może dojść do naruszeń prywatności. Jeśli użytkownicy są nieostrożni, witryna może śledzić ich adresy IP i zbierać zapis ich zachowania (na przykład uzyskiwać informacje o węzłach, którymi użytkownicy są zainteresowani).

Należy również zapamiętać, że ze względu na brak zgody co do obecnego grafu sieci Lightning lub obecnego stanu polityki kanału użytkownicy nie powinni polegać na eksploratorach Lightning w uzyskiwaniu możliwie aktualnych informacji. Co więcej, gdy użytkownicy otwierają, zamykają i aktualizują kanały, graf się zmienia, a poszczególne eksploratory Lightning mogą być nieaktualne. Korzystaj z eksploratorów Lightning do wizualizacji sieci lub zbierania informacji, ale nie stosuj ich jako autorytatywnego źródła informacji na temat tego, co się dzieje w sieci Lightning Network. Aby uzyskać autorytatywny widok sieci Lightning Network, uruchom własny węzeł Lightning, który zbuduje graf kanału i zbierze różne statystyki dostępne do przeglądania w interfejsie webowym.

Portfele Lightning

Termin *portfel Lightning* jest nieco mylący, ponieważ może opisywać szeroką gamę komponentów w połączeniu z wybranymi interfejsami użytkownika. Do najbardziej powszechnych składników oprogramowania portfela Lightning należą:

- magazyn kluczy zawierający poufne informacje (ang. *secrets*), takie jak klucze prywatne,
- węzeł LN (węzeł Lightning), który komunikuje się w sieci *peer-to-peer*, tak jak opisano powyżej,
- węzeł Bitcoin, który przechowuje dane sieci blockchain i komunikuje się z innymi węzłami Bitcoin,
- „mapa" bazy danych i kanałów, które są rozgłaszane w sieci Lightning Network,
- menedżer kanałów, który może otwierać i zamykać kanały LN,
- system „przybliżania" (ang. *close-up*), który pozwala znaleźć ścieżkę połączonych kanałów od źródła płatności do jej miejsca docelowego.

Portfel Lightning może zawierać wszystkie te funkcje. Dzięki temu może być wykorzystywany jako „pełnoprawny" portfel, niewymagający korzystania z jakichkolwiek usług zewnętrznych. Jeden lub większa liczba tych składników może polegać (częściowo lub całkowicie) na usługach innych firm, pośredniczących w dostarczaniu potrzebnych funkcji.

Kluczową cechą wyróżniającą jest to, czy funkcja magazynu kluczy jest wewnętrzna czy zewnętrzna. W sieciach typu blockchain zarządzanie kluczami określa opiekę nad funduszami, co upamiętnia fraza „twoje klucze, twoje monety, nie twoje klucze, nie twoje monety". Każdy portfel, w którym zarządzanie kluczami zostało zlecone na zewnątrz, jest nazywany *powierniczym* (ang. *custodial*), ponieważ to podmiot zewnętrzny, a nie użytkownik, ma kontrolę nad funduszami użytkownika. Dla porównania, portfel *niepowierniczy* (ang. *noncustodial* lub *self-custody*) to taki, w którym magazyn kluczy jest częścią portfela, a klucze są zarządzane bezpośrednio przez użytkownika. Termin portfel niepowierniczy oznacza, że magazyn kluczy jest lokalny i pod kontrolą użytkownika. Jednak jeden lub więcej innych komponentów portfela może, ale nie musi, pochodzić z zewnątrz i polegać na zaufanych podmiotach zewnętrznych.

Sieci blockchain, a zwłaszcza otwarte sieci blockchain, takie jak Bitcoin, próbują zminimalizować lub wyeliminować zaufanie do podmiotów zewnętrznych i wzmocnić pozycję użytkowników. Taki model działania często jest nazywany modelem „niezaufanym" (ang. *trustless*), chociaż lepszym określeniem byłoby „model o minimalnej potrzebie zaufania" (ang. *trust-minimized*). W takich systemach użytkownik ufa regułom oprogramowania, a nie podmiotom zewnętrznym. Dlatego przy wyborze portfela Lightning głównym czynnikiem jest kwestia kontroli nad kluczami.

Do wszystkich innych elementów portfela Lightning mają zastosowanie podobne względy zaufania. Jeśli wszystkie komponenty są pod kontrolą użytkownika, wtedy stopień zaufania do podmiotów zewnętrznych jest zminimalizowany, co daje użytkownikom maksymalne możliwości. Oczywiście jest z tym związany bezpośredni kompromis, ponieważ z Tymi możliwościami wiąże się odpowiedzialność za zarządzanie złożonym oprogramowaniem.

Każdy użytkownik przed podjęciem decyzji o wyborze rodzaju portfela Lightning musi wziąć pod uwagę własne umiejętności techniczne. Osoby z obszerną wiedzą techniczną powinny korzystać z portfela Lightning, w którym wszystkie komponenty znajdują się pod bezpośrednią kontrolą użytkownika. Osoby, które mają mniejsze umiejętności techniczne, ale chcą kontrolować własne fundusze, powinny wybrać niepowierniczy portfel Lightning. Często w takich przypadkach zaufanie jest powiązane z prywatnością. Jeśli użytkownicy decydują się zlecić niektóre funkcje podmiotom zewnętrznym, zwykle rezygnują z prywatności, ponieważ podmioty zewnętrzne uzyskają o nich pewne informacje.

Na koniec, osoby poszukujące prostoty i wygody, nawet kosztem kontroli i bezpieczeństwa, powinny wybrać powierniczy portfel Lightning. Jest to najmniej trudna technicznie opcja, ale *podważa model zaufania kryptowaluty* i dlatego powinna być traktowana jedynie jako krok w kierunku uzyskania większej kontroli i samodzielności.

Istnieje wiele sposobów, na jakie można charakteryzować lub kategoryzować portfele. Oto najważniejsze pytania na temat konkretnego portfela, które należy zadać:

1. Czy portfel Lightning zawiera kompletny węzeł Lightning, czy też używa węzła Lightning firmy zewnętrznej?
2. Czy portfel Lightning zawiera kompletny węzeł Bitcoin, czy też korzysta z węzła Bitcoin za pośrednictwem innej firmy?
3. Czy portfel Lightning przechowuje własne klucze, które są pod kontrolą użytkownika (samoopieka), czy też klucze są przechowywane u zewnętrznego opiekuna?

Jeśli portfel Lightning korzysta z węzła zewnętrznej firmy, to ten węzeł decyduje o sposobie komunikowania się z siecią Bitcoin. W związku z tym korzystanie z węzła Lightning należącego do firmy zewnętrznej oznacza również korzystanie z jej węzła Bitcoin. Wybór między pełnoprawnym węzłem Bitcoin a węzłem Bitcoin firmy zewnętrznej istnieje tylko wtedy, gdy portfel Lightning używa własnego węzła Lightning.

Na najwyższym poziomie abstrakcji najbardziej podstawowe są pytania 1. i 3. Na podstawie odpowiedzi na te dwa pytania możemy wyodrębnić cztery możliwe kategorie. Te cztery kategorie można umieścić w kwadrancie, co pokazano w tabeli 2.1. Należy jednak pamiętać, że jest to tylko jeden ze sposobów kategoryzacji portfeli Lightning.

Tabela 2.1. Kwadrant portfeli Lightning

	Pełnoprawny węzeł Lightning	Zewnętrzny węzeł Lightning
Niepowierniczy	Q1: Wysokie umiejętności techniczne, najmniejsze zaufanie do podmiotów zewnętrznych, w większości nie wymaga żadnych uprawnień	Q2: Poziom techniczny poniżej średniego, zaufanie do podmiotów zewnętrznych, wymaga pewnych uprawnień
Powierniczy	Q3: Poziom techniczny powyżej średniego, zaufanie do podmiotów zewnętrznych, wymaga pewnych uprawnień	Q4: Niski poziom techniczny, wysokie zaufanie do podmiotów zewnętrznych, wymaga uprawnień

Kwadrant 3 (Q3), w którym korzysta się z pełnoprawnego węzła Lightning, ale klucze przechowywane są u opiekuna, nie jest powszechne używany. Przyszłe portfele w tym kwadrancie mogą wymagać od użytkownika dbania o operacyjne aspekty swojego węzła, ale wymagać przekazywania dostępu do kluczy podmiotowi zewnętrznemu, który przede wszystkim używa magazynowania w trybie *cold storage*.

Portfele Lightning można zainstalować na wielu urządzeniach, w tym na laptopach, serwerach i urządzeniach mobilnych. Aby uruchomić pełnoprawny węzeł Lightning, należy użyć serwera lub komputera stacjonarnego. Urządzenia mobilne i laptopy zwykle nie są wystarczająco mocne pod względem pojemności, mocy obliczeniowej, żywotności akumulatora czy też możliwości komunikacyjnych. Kategorię zewnętrznych węzłów Lightning można podzielić dalej na następujące podkategorie:

Lekkie (ang. *lightweight*)

Oznacza, że portfel nie obsługuje węzła Lightning, a zatem informacje o Lightning Network musi pobrać przez internet z węzła należącego do podmiotu zewnętrznego.

Brak

Oznacza to, że nie tylko węzeł Lightning jest obsługiwany przez podmiot zewnętrzny, ale także większość portfela jest obsługiwana przez podmiot zewnętrzny w chmurze. Jest to portfel powierniczy, w którym ktoś inny ma kontrolę nad funduszami.

Wspomniane podkategorie zostały wymienione w tabeli 2.2.

Tabela 2.2. Przykłady popularnych portfeli Lightning

Aplikacja	Urządzenia	Węzeł Lightning	Węzeł Bitcoin	Magazyn kluczy
Blue Wallet	mobilne	Brak	Brak	powierniczy
Breez Wallet	mobilne	Pełnoprawny węzeł	Neutrino	niepowierniczy
Eclair Mobile	mobilne	lekki	Electrum	niepowierniczy
Intxbot	mobilne	Brak	Brak	powierniczy
Muun	mobilne	lekki	Neutrino	niepowierniczy
Phoenix Wallet	mobilne	lekki	Electrum	niepowierniczy
Zeus	mobilne	Pełnoprawny węzeł	Bitcoin Core (btcd)	niepowierniczy
Electrum	desktop	Pełnoprawny węzeł	Bitcoin Core (Electrum)	niepowierniczy
Zap Desktop	desktop	Pełnoprawny węzeł	Neutrino	niepowierniczy
c-lightning	serwery	Pełnoprawny węzeł	Bitcoin Core	niepowierniczy
Eclair Server	serwery	Pełnoprawny węzeł	Bitcoin Core/Electrum	niepowierniczy
lnd	serwery	Pełnoprawny węzeł	Bitcoin Core (btcd)	niepowierniczy

Oto inne terminy z kolumny *Węzeł Bitcoin* z tabeli 2.2 wymagające omówienia:

Neutrino

Ten portfel nie obsługuje węzła Bitcoin. Zamiast tego węzłem Bitcoin zarządza ktoś inny (podmiot zewnętrzny). Dostęp do niego uzyskuje się za pośrednictwem protokołu Neutrino.

Electrum

Ten portfel nie obsługuje węzła Bitcoin. Zamiast niego dostęp do węzła Bitcoin obsługiwanego przez kogoś innego (podmiot zewnętrzny) uzyskuje się za pośrednictwem protokołu Electrum.

Bitcoin Core

Implementacja węzła Bitcoin.

btcd

Inna implementacja węzła Bitcoin.

Kilka przykładów popularnych aplikacji węzłów Lightning oraz portfeli dla różnych typów urządzeń zestawiono w tabeli 2.2. Lista została posortowana najpierw według typu urządzenia, a następnie alfabetycznie.

Bitcoin Testnet

System Bitcoin oferuje alternatywny blockchain do celów testowych, o nazwie *testnet*, w odróżnieniu od „normalnego" łańcucha Bitcoin, określanego jako *mainnet*. Walutą w *testnecie* jest *testnet bitcoin* (*tBTC*) — bezwartościowa imitacja bitcoina używana wyłącznie w celach testowych. Wszystkie funkcje Bitcoina w testnecie zostały dokładnie odtworzone. Te pieniądze nie są jednak nic warte, zatem dosłownie nie masz nic do stracenia!

W testnecie mogą również działać niektóre portfele Lightning, co umożliwia dokonywanie płatności Lightning za pomocą testowych bitcoinów, bez ryzyka utraty prawdziwych pieniędzy. Sieć testnet zapewnia świetny sposób na bezpieczne eksperymentowanie z Lightning Network. Jednym z przykładów portfela Lightning obsługującego sieć testnet jest Eclair Mobile, którego Alicja używa w tym rozdziale.

Pewną kwotę tBTC do testów możesz pobrać z portfeli *testnet bitcoin faucet*, które dostarczają na żądanie darmowej waluty tBTC. Oto kilka z nich:

- *https://coinfaucet.eu/en/btc-testnet*,
- *https://testnet-faucet.mempool.co*,
- *https://bitcoinfaucet.uo1.net*,
- *https://testnet.help/en/btcfaucet/testnet*.

Wszystkie przykłady w tej książce można dokładnie odtworzyć w sieci testnet z wykorzystaniem waluty tBTC. Dzięki temu możesz śledzić przykłady bez ryzyka utraty prawdziwych pieniędzy.

Równoważenie złożoności i kontroli

W portfelach Lightning należy zachowywać właściwą równowagę pomiędzy złożonością a poziomem kontroli sprawowanej przez użytkownika. Portfele dające użytkownikowi największą kontrolę nad funduszami, zapewniające najwyższy stopień prywatności i największą niezależność od usług podmiotów zewnętrznych są z konieczności bardziej złożone i trudne w obsłudze. Wraz

z rozwojem technologii niektóre z tych kompromisów stają się mniej restrykcyjne, a użytkownicy mogą uzyskać większą kontrolę bez większej złożoności. Na razie jednak liczne firmy, w różnych projektach, badają rozmaite rozwiązania spektrum kontrola-złożoność, licząc na znalezienie „idealnego punktu" dla docelowych użytkowników.

Gdy wybierasz portfel, pamiętaj, że zastosowano w nim wspomniane kompromisy, nawet jeśli ich nie dostrzegasz. Na przykład w wielu portfelach podjęto próbę zdjęcia z użytkowników obowiązków związanych z zarządzaniem kanałami. W tym celu w tych portfelach zastosowano węzły centralne, do których automatycznie łączą się wszystkie portfele. Zaletą tego kompromisu jest uproszczony interfejs i wrażenie łatwiejszej obsługi, wprowadza on jednak pojedynczy punkt awarii (ang. *single point of failure* — SPoF), ponieważ do działania portfela stają się niezbędne węzły centralne. Co więcej, poleganie na takim „centralnym węźle" może pogorszyć prywatność użytkownika, „centrala" zna bowiem nadawcę i potencjalnie (jeśli wykonuje płatności w imieniu użytkownika) również odbiorcę każdej płatności dokonanej z wykorzystaniem portfela użytkownika.

W następnym podrozdziale powrócimy do Alicji i spróbujemy wykonać wraz z nią pierwszą konfigurację portfela Lightning. Wybrała portfel, który jest bardziej zaawansowany od prostszych portfeli powierniczych. Pozwoliło to nam zaprezentować część związanej z tym złożoności i wprowadzić w tematykę niektórych z wewnętrznych działań zaawansowanego portfela. Może się okazać, że Twój pierwszy idealnie dopasowany portfel został zaprojektowany pod kątem łatwości obsługi i zostały w nim przyjęte pewne kompromisy związane z poziomem kontroli i prywatnością. A być może jesteś bardziej zaawansowanym użytkownikiem i chcesz uruchomić własne węzły Lightning i Bitcoin w ramach rozwiązania takiego portfela?

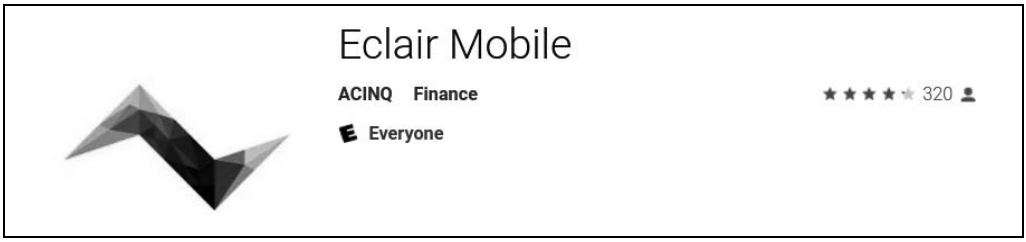
Pobieranie i instalowanie portfela Lightning

Gdy szukasz nowego portfela kryptowalut, musisz bardzo uważnie wybrać bezpieczne źródło oprogramowania.

Niestety, istnieje wiele fałszywych aplikacji portfelowych, które mogą skraść Twoje pieniądze. Niektóre z nich znajdują się nawet na renomowanych i rzekomo sprawdzonych stronach z oprogramowaniem, takich jak sklepy Apple i Google. Niezależnie od tego, czy instalujesz swój pierwszy czy dziesiąty portfel, zawsze zachowuj szczególną ostrożność. Fałszywa aplikacja może nie tylko ukraść wszystkie powierzone jej pieniądze, ale również, dzięki przejęciu kontroli nad systemem operacyjnym urządzenia mobilnego, ukraść klucze i hasła z innych aplikacji.

Alicja korzysta z urządzenia z systemem Android. Zamierza pobrać i zainstalować aplikację portfela Eclair ze sklepu Google Play. Szukając aplikacji w Google Play, znalazła pozycję „Eclair Mobile", co pokazano na rysunku 2.1.

Dzięki wykorzystaniu testowych bitcoinów sieci testnet możliwe jest eksperymentowanie i testowanie oprogramowania Bitcoin bez żadnego ryzyka (z wyjątkiem utraty własnego czasu). Aby wypróbować Lightning Network (w sieci testnet), możesz także pobrać ze sklepu Google Play testowy portfel Eclair.



Rysunek 2.1. Eclair Mobile w sklepie Google Play

Alicja zauważyła na tej stronie kilka różnych elementów, które pomogły jej zyskać pewność, że ten portfel „Eclair Mobile" jest tym, którego szuka. Po pierwsze, jako twórcę tego mobilnego portfela wymieniono organizację ACINQ[2]. Alicja na podstawie przeprowadzonego własnego rozpoznania wie, że to właściwa firma. Po drugie, portfel został zainstalowany ponad 10 tysięcy razy i ma ponad 320 pozytywnych komentarzy. Jest mało prawdopodobne, aby była to nieuczciwa aplikacja, która przypadkiem wkradła się do Sklepu Google Play. W trzecim kroku Alicja przeszła na stronę internetową ACINQ (*https://acinq.co*). Sprawdziła, czy strona internetowa jest bezpieczna. W tym celu zweryfikowała, czy adres strony zaczyna się od *https* oraz czy jest poprzedzony w niektórych przeglądarkach kłódką. Na stronie internetowej przeszła do sekcji *Download*, a potem poszukała odnośnika do serwisu *Google App Store*. Znalazła odpowiedni odnośnik i go kliknęła. Porównała, że ten odnośnik przenosi ją do tej samej aplikacji w Google App Store. Zadowolona z tych odkryć, Alicja zainstalowała na swoim urządzeniu mobilnym aplikację Eclair.

Podczas instalowania oprogramowania na dowolnym urządzeniu zawsze zachowuj szczególną ostrożność. Istnieje wiele fałszywych portfeli kryptowalut, które mogą nie tylko przejąć Twoje pieniądze, ale również zagrozić wszystkim innym aplikacjom na Twoim urządzeniu.

Tworzenie nowego portfela

Kiedy Alicja po raz pierwszy otworzyła aplikację Eclair Mobile, wyświetliła się w niej prośba o wybranie opcji „Utwórz nowy portfel" (*Create a New Wallet*) lub „Zaimportuj istniejący portfel" (*Import an Existing Wallet*). Alicja zdecydowała się utworzyć nowy portfel. Najpierw jednak opowiemy, dlaczego te opcje zostały jej przedstawione i co to znaczy „zaimportować istniejący portfel".

Odpowiedzialność związana z przechowywanymi kluczami

Jak wspomnieliśmy na początku tego rozdziału, Eclair jest portfelem niepowierniczym. Oznacza to, że Alicja ma wyłączną opiekę nad kluczami używanymi do kontrolowania jej bitcoinów. Oznacza to również, że Alicja jest odpowiedzialna za ochronę i tworzenie kopii zapasowych tych kluczy. Jeśli Alicja utraci klucze, nikt nie będzie mógł jej pomóc w odzyskaniu bitcoinów i zostaną one bezpowrotnie utracone.

[2] ACINQ: programiści portfela Eclair Mobile Lightning.

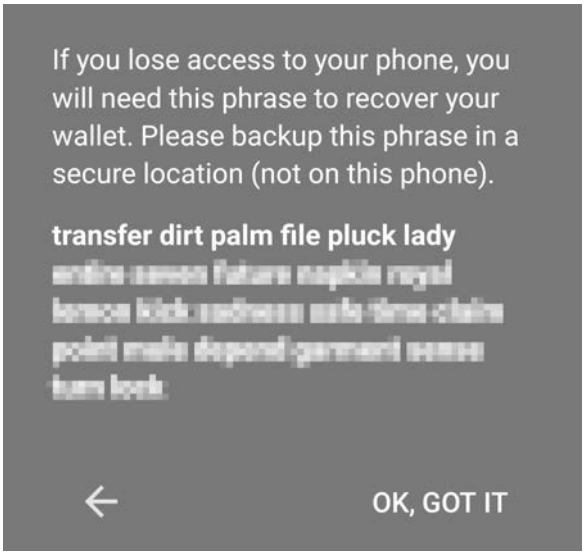
W przypadku portfela Eclair Mobile Alicja sprawuje opiekę i ma kontrolę nad kluczami, a zatem ponosi pełną odpowiedzialność za bezpieczeństwo kluczy i tworzenie k kopii zapasowych. Jeśli zgubi klucze, straci bitcoiny i nikt nie będzie w stanie pomóc jej w ich odzyskaniu!

Słowa mnemoniczne

Eclair Mobile, podobnie jak większość portfeli Bitcoina, zapewnia tzw. *frazę mnemoniczną* (czasami nazywaną również „ziarnem" — ang. *seed*, lub „frazą zalążkiem" — ang. *seed phrase*), której Alicja może użyć do odtworzenia klucza w warunkach awarii. Fraza mnemoniczna składa się z 24 angielskich słów, wybranych losowo przez oprogramowanie i stosowanych jako podstawa kluczy generowanych przez portfel. W razie zagubienia urządzenia mobilnego, wystąpienia błędu w oprogramowaniu lub uszkodzenia pamięci Alicja może skorzystać z frazy mnemonicznej, aby przywrócić wszystkie transakcje i środki w portfelu Eclair Mobile.

Poprawną nazwą słów zapewniających kopię zapasową jest „fraza mnemoniczna" (ang. *mnemonic phrase*). Unikamy używania terminu „ziarno" na określenie frazy mnemonicznej, ponieważ jego użycie, choć powszechne, jest błędne.

Kiedy Alicja podjęła decyzję o utworzeniu nowego portfela, zobaczyła ekran z frazą mnemoniczną, która ma postać pokazaną na rysunku 2.2.



Rysunek 2.2. Nowa fraza mnemoniczna portfela

Na rysunku 2.2 celowo zamazaliśmy część frazy mnemonicznej, aby uniemożliwić czytelnikom tej książki jej wykorzystanie.

Bezpieczne przechowywanie frazy mnemonicznej

Alicja musi być ostrożna przy przechowywaniu frazy mnemonicznej. Powinna przechowywać ją tak, aby zapobiec jej kradzieży, a jednocześnie uniknąć przypadkowej utraty. Zalecanym sposobem zrównoważenia wymienionych zagrożeń jest zapisanie dwóch kopii frazy mnemonicznej na papierze i ponumerowanie poszczególnych słów — kolejność ma znaczenie.

Gdy Alicja zapisała frazę mnemoniczną, dotknęła na ekranie linku *OK GOT IT*. Po chwili wyświetlił się quiz, którego zadaniem jest sprawdzenie, czy fraza została poprawnie zapisana. W quizie wyświetliły się prośby o podanie trzech lub czterech losowych słów. Alicja nie spodziewała się quizu, ale ponieważ poprawnie zapisała frazę mnemoniczną, bez żadnych trudności przeszła test.

Po zapisaniu frazy mnemonicznej i zdaniu testu zaprezentowanego za pomocą quizu Alicja powinna schować każdą z kopii w osobnym, bezpiecznym miejscu, takim jak zamknięta szuflada biurka lub ognioodporny sejf.

Nigdy nie próbuj stosować schematu bezpieczeństwa typu „zrób to sam”, który w jakikolwiek sposób odbiega od metody zalecanej w punkcie „Bezpieczne przechowywanie frazy mnemonicznej”. Nie przecinaj frazy na pół, nie twórz zrzutów ekranu, nie przechowuj jej na dyskach USB lub dyskach w chmurze, nie szyfruj jej ani nie stosuj żadnej innej niestandardowej metody. W ten sposób przechylisz szalę i podejmiesz niepotrzebne ryzyko trwałej utraty środków. Wiele osób straciło swoje fundusze nie z powodu kradzieży, ale dlatego, że próbowały skorzystać z niestandardowych rozwiązań bez specjalistycznej wiedzy potrzebnej do zredukowania związanych z tym zagrożeń. Zalecona najlepsza metoda została dobrze przemyślana przez ekspertów i jest odpowiednia dla zdecydowanej większości użytkowników.

Po zainicjowaniu portfela Eclair Mobile Alicja wyświetliła krótki samouczek, w którym wyjaśniono różne elementy interfejsu użytkownika. Nie będziemy powtarzać tu opisu samouczka, ale przeanalizujemy wszystkie te elementy, gdy będziemy śledzić, jak Alicja próbuje kupić filiżankę kawy!

Ładowanie bitcoinów do portfela

Alicja ma teraz portfel Lightning. Ale jest on pusty! Teraz stoi przed jednym z trudniejszych aspektów tego eksperymentu: musi znaleźć sposób na zdobycie bitcoinów i załadowanie ich do portfela Eclair.

Jeżeli Alicja ma już bitcoiny w innym portfelu, to zamiast kupować nowe, może je wysłać do swojego portfela Eclair i w ten sposób załadować portfel.

Zdobywanie bitcoinów

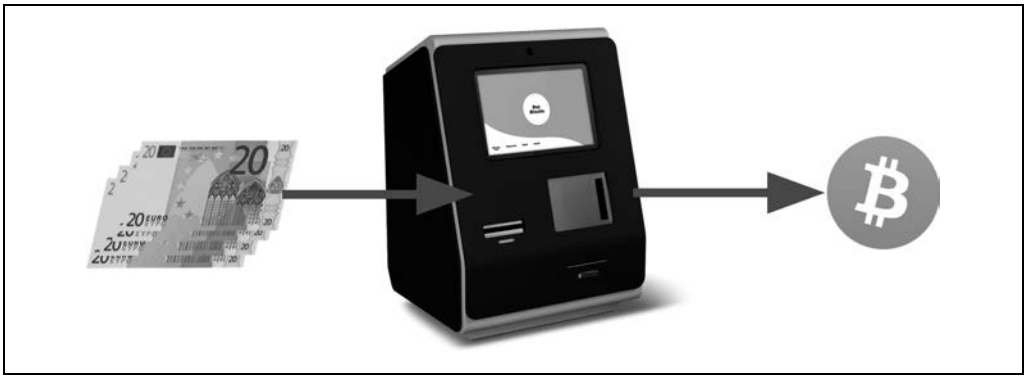
Istnieje kilka sposobów, w jakie Alicja może nabyć bitcoiny:

- Może wymienić na giełdzie kryptowalut na bitcoiny część swojej waluty krajowej (na przykład PLN).
- Może w zamian za gotówkę kupić trochę bitcoinów od przyjaciela lub znajomego.
- Może znaleźć w swojej okolicy *bankomat Bitcoin*, który działa jak automat sprzedający bitcoiny za gotówkę.
- Może akceptować płatności w bitcoinach, oferując swoje usługi lub sprzedaż produktów.
- Może poprosić swojego pracodawcę lub klientów, aby dokonywali płatności w bitcoinach.

Wszystkie te metody charakteryzują się różnym stopniem trudności, a wiele z nich wymaga uiszczenia opłaty. Niektóre także, aby zachowana była zgodność z lokalnymi przepisami bankowymi, będą wymagały od Alicji dostarczenia dokumentów tożsamości. Jednak wszystkie te metody pozwolą Alicji odbierać bitcoiny.

Odbieranie bitcoinów

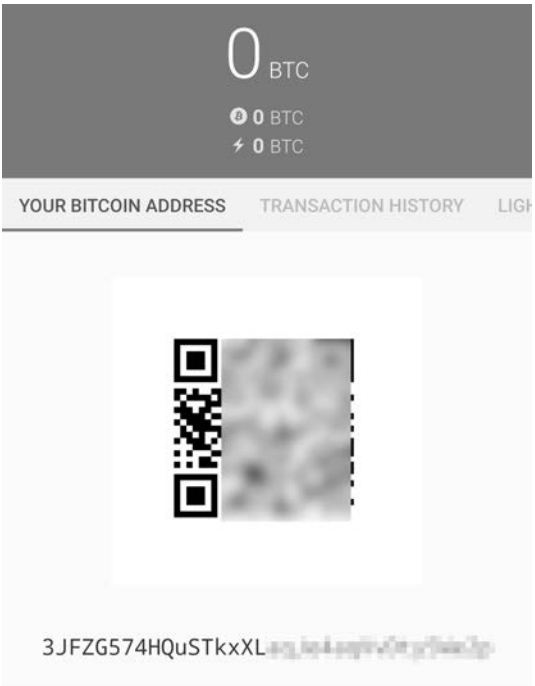
Załóżmy, że Alicja znalazła lokalny bankomat Bitcoin i postanowiła kupić trochę bitcoinów za gotówkę. Przykład bankomatu Bitcoin, zbudowanego przez firmę Lamassu, jest pokazany na rysunku 2.3. Takie bankomaty Bitcoin przyjmują walutę krajową (gotówkę) za pośrednictwem automatu gotówkowego i wysyłają bitcoiny na adres zeskanowany z portfela użytkownika za pomocą wbudowanej kamery.



Rysunek 2.3. Bankomat Bitcoin firmy Lamassu

Aby otrzymać bitcoiny do swojego portfela Eclair Lightning, Alicja musi okazać w bankomacie adres Bitcoin z portfela Eclair Lightning. Następnie bankomat wyśle Alicji nabyte bitcoiny na podany adres.

Aby zobaczyć adres Bitcoin portfela Eclair, Alicja musi przesunąć palcem do lewej kolumny o nazwie *YOUR BITCOIN ADDRESS* (rysunek 2.4). Zobaczy kwadrat z kodem QR, a poniżej niego ciąg liter i cyfr.



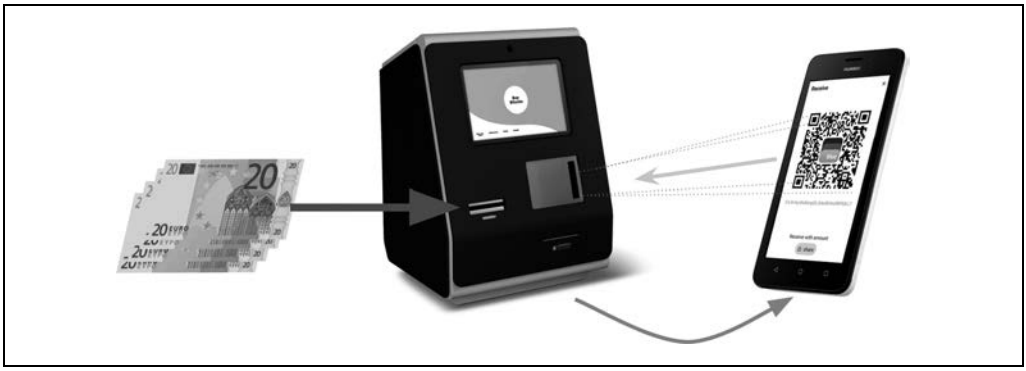
Rysunek 2.4. Adres bitcoin Alicji w aplikacji Eclair

Kod QR zawiera ten sam ciąg liter i cyfr, który znajduje się pod kodem, ale w formacie łatwym do zeskanowania. Dzięki temu Alicja nie musi wpisywać adresu Bitcoin. Na powyższym zrzucie ekranu (rysunek 2.4) celowo zamazaliśmy oba elementy, aby zapobiec przypadkowemu przesyłaniu przez czytelników bitcoinów na podany adres.

Zarówno adresy Bitcoin, jak i kody QR zawierają informacje o wykrywaniu błędów. Zapobiega to błędom podczas wpisywania lub skanowania, w których wyniku mogłyby być wygenerowane „niepoprawne" adresy Bitcoin. Jeśli w adresie wystąpi błąd, każdy portfel Bitcoin go zauważy i odmówi zaakceptowania ważności adresu.

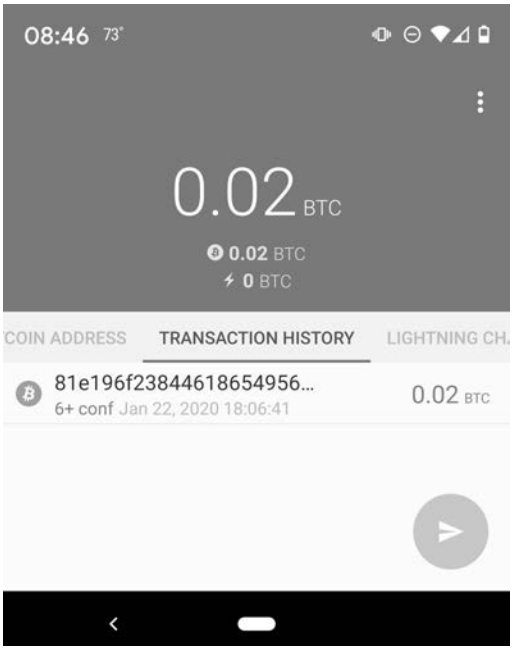
Alicja może wziąć swoje urządzenie mobilne do bankomatu i pokazać je do wbudowanej kamery, tak jak pokazano na rysunku 2.5. Po umieszczeniu gotówki w bankomacie otrzyma bitcoiny do portfela Eclair!

Alicja zobaczy transakcję z bankomatu w zakładce *TRANSACTION HISTORY* portfela Eclair. Chociaż Eclair wykryje transakcję Bitcoin w ciągu zaledwie kilku sekund, to „potwierdzenie" transakcji Bitcoin w blockchainie może zająć około godziny. Jak widać na rysunku 2.6, portfel Eclair Alicji wyświetla pod transakcją „6+ conf". Oznacza to, że transakcja otrzymała wymagane minimum sześć potwierdzeń, a środki są teraz gotowe do użycia.



Rysunek 2.5. Bankomat Bitcoin skanujący kod QR

Liczba potwierdzeń transakcji to liczba bloków wydobytych od czasu wydobycia bloku, który zawierał tę transakcję (włącznie z nim). Uzyskanie sześciu potwierdzeń jest najlepszą praktyką, ale inne portfele Lightning mogą uznawać kanał za otwarty po dowolnej liczbie potwierdzeń. Niektóre portfele nawet skalują w górę liczbę wymaganych potwierdzeń o wartość pieniężną kanału.



Rysunek 2.6. Alicja otrzymuje bitcoiny

Chociaż w tym przykładzie Alicja skorzystała z bankomatu do nabycia swojego pierwszego bitcoina, te same pojęcia miałyby zastosowanie także w przypadkach, gdyby użyła jednej z innych metod wymienionych w punkcie „Zdobywanie bitcoinów". Na przykład, gdyby Alicja chciała

sprzedać produkt lub zapewnić profesjonalną usługę w zamian za bitcoiny, jej klienci mogliby skanować adres Bitcoin za pomocą swoich portfeli i płacić jej w bitcoinach.

Na podobnej zasadzie, gdyby Alicja wystawiła klientowi rachunek za usługę oferowaną przez internet, mogłaby wysłać do niego wiadomość e-mail lub SMS-a z adresem Bitcoin lub kodem QR. Klient mógłby wówczas zapłacić jej przez wklejenie informacji do portfela Bitcoin lub ich zeskanowanie.

Alicja mogłaby nawet wydrukować kod QR, umieścić go w widocznym miejscu i prezentować publicznie, aby otrzymywać napiwki. Na przykład może przymocować kod QR do gitary i otrzymywać napiwki podczas ulicznych występów![3]

Na koniec, jeśli Alicja kupiłaby bitcoiny na giełdzie kryptowalut, mogłaby (i powinna) „wypłacić" je przez wklejenie na stronie internetowej giełdy swojego adresu Bitcoin. W odpowiedzi giełda wysłałaby bitcoiny bezpośrednio na jej adres.

Od sieci Bitcoin do Lightning Network

Bitcoin Alicji jest teraz obsługiwany przez portfel Eclair i został zarejestrowany w blockchainie Bitcoin. W tym momencie bitcoiny Alicji są w trybie *on-chain*, co oznacza, że transakcja została rozesłana do całej sieci Bitcoin. Została zweryfikowana przez wszystkie węzły i wydobyta (zarejestrowana) w blockchainie Bitcoin.

Do tej pory portfel Eclair Mobile działał tylko jako portfel Bitcoin, a Alicja jeszcze nie korzystała z funkcji Lightning Network Eclair. Podobnie jak w przypadku wielu innych portfeli Lightning Eclair łączy w sobie węzeł Bitcoin i Lightning Network. Działa zarówno jako portfel Bitcoin, jak i portfel Lightning.

Alicja jest teraz gotowa, by używać Lightning Network. W tym celu powinna przenieść swoje bitcoiny do trybu *off-chain*. Dzięki temu będzie mogła skorzystać z szybkich, tanich i prywatnych płatności oferowanych przez Lightning Network.

Kanały sieci Lightning Network

Alicja przesunęła palcem w prawo i uzyskała dostęp do sekcji *LIGHTNING CHANNELS* aplikacji Eclair. Może tutaj zarządzać kanałami, które połączą jej portfel z siecią Lightning Network.

Aby nieco rozjaśnić pojęcie kanału LN, spróbujmy przyjrzeć się jego definicji. Po pierwsze, słowo „kanał" jest metaforą *relacji finansowej* pomiędzy portfelem Lightning Alicji a innym portfelem Lightning. Nazywamy tę relację kanałem, ponieważ jest to mechanizm umożliwiający portfelowi Alicji i temu drugiemu portfelowi wymianę wielu płatności w sieci Lightning Network (*off-chain*) bez dokonywania transakcji w blockchainie Bitcoin (*on-chain*).

[3] Ogólnie rzecz biorąc, nie zaleca się używania tego samego adresu Bitcoin do wielu płatności, ponieważ wszystkie transakcje Bitcoin są publiczne. Wścibska osoba przechodząca obok może zeskanować kod QR Alicji i zobaczyć, ile napiwków Alicja już otrzymała na ten adres na blockchainie Bitcoin. Na szczęście Lightning Network oferuje bardziej prywatne rozwiązania tego problemu, omówione w dalszej części książki!

Portfel lub *węzeł*, dla którego Alicja otwiera kanał, nazywa się *kanałem partnerskim* (ang. *channel peer*). Po „otwarciu" kanał może być używany do wysyłania wielu płatności w obu kierunkach między portfelem Alicji a partnerem kanału.

Co więcej, kanał partnerski może *przekazywać* płatności dalej za pośrednictwem innych kanałów do sieci Lightning Network. Dzięki temu Alicja może *przekazać* płatność do dowolnego portfela (na przykład portfela Lightning Bogdana), pod warunkiem że portfel Alicji znajdzie realną *ścieżkę* utworzoną za pomocą przeskoków pomiędzy kanałami, aż do portfela Bogdana.

Nie wszystkie kanały partnerskie są odpowiednie do przekazywania płatności. Tzw. kanały *well-connected* (dosłownie: dobrze połączone) mogą kierować płatności krótszymi ścieżkami do miejsca docelowego, co zwiększa szansę powodzenia operacji. Kanały partnerskie ze sporymi funduszami mogą obsługiwać większe płatności.

Innymi słowy, Alicja potrzebuje jednego lub większej liczby kanałów, które połączą ją z jednym lub kilkoma innymi węzłami w Lightning Network. Nie potrzebuje kanału, aby połączyć swój portfel bezpośrednio z „Kawiarnią u Bogdana" i wysłać Bogdanowi płatność, choć może również otworzyć kanał bezpośredni. Rolę pierwszego kanału Alicji może odgrywać dowolny węzeł w sieci Lightning Network. Im węzeł ma lepsze połączenia, tym większa jest liczba osób, do których Alicja może dotrzeć. W tym przykładzie chcemy również zademonstrować przekierowywanie płatności, dlatego Alicja nie otworzy kanału bezpośrednio do portfela Bogdana. Zamiast tego otworzy kanał do węzła *well-connected*. Użyje go potem do przekazania swojej płatności, a jeśli to będzie konieczne, przekieruje ją przez inne węzły, tak by płatność dotarła do Bogdana.

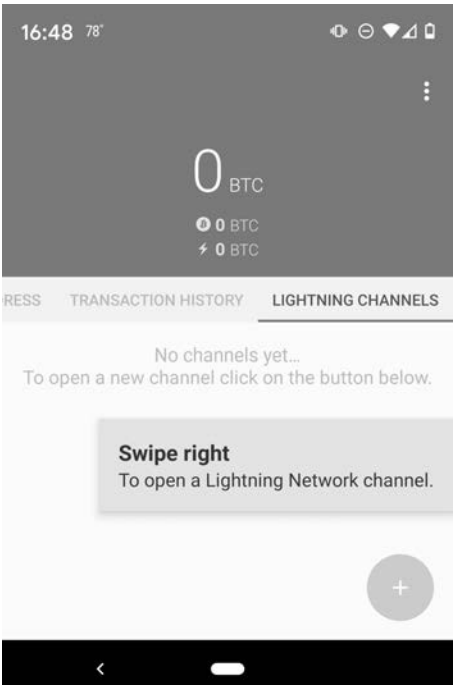
Na początku Alicja nie ma otwartych kanałów, więc jak widać na rysunku 2.7, zakładka *LIGHTNING CHANNELS* wyświetla pustą listę. W prawym dolnym rogu można zauważyć symbol plus (+). Jest to przycisk pozwalający otworzyć nowy kanał.

Alicja nacisnęła symbol plusa. W odpowiedzi wyświetliły się cztery możliwe sposoby otwarcia kanału:

- wklejenie identyfikatora URI węzła (*Paste a node URI*),
- skanowanie identyfikatora URI węzła (*Scan a node URI*),
- wybranie losowego węzła (*Random node*),
- wybranie węzła ACINQ (*ACINQ node*).

„Identyfikator URI węzła" to uniwersalny identyfikator zasobu (ang. *universal resource identifier*), który identyfikuje określony węzeł Lightning. Alicja może wkleić taki identyfikator URI ze schowka lub zeskanować kod QR zawierający te same informacje. Przykład identyfikatora URI węzła w postaci kodu QR jest pokazany na rysunku 2.8. Poniżej rysunku widnieje ten sam identyfikator w formacie tekstowym.

Alicja mogłaby wybrać określony węzeł Lightning lub użyć opcji *Random node*, aby portfel Eclair wybrał go losowo. Alicja wybrała jednak opcję *ACINQ Node*, co pozwoli jej połączyć się z jednym z węzłów *well-connected* ACINQ w sieci Lightning.



Rysunek 2.7. Zakładka LIGHTNING CHANNELS

Rysunek 2.8. Kod QR identyfikatora URI węzła

```
0237fefbe8626bf888de0cad8c73630e32746a22a2c4faa91c1d9877a3826e1174@1.ln.aantonop. com:9735
```

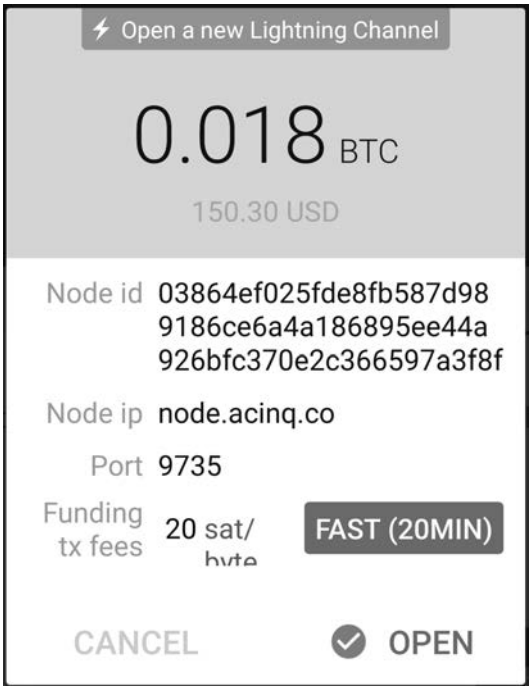
Wybór węzła ACINQ nieznacznie ograniczy prywatność Alicji, ponieważ sieć ACINQ daje możliwość podglądu wszystkich transakcji użytkownika. Taki wybór spowoduje również powstanie pojedynczego punktu awarii. Alicja będzie dysponować tylko jednym kanałem, a jeśli węzeł ACINQ nie będzie dostępny, nie będzie mogła dokonywać płatności. Aby wszystko było na początku proste, zaakceptujemy te kompromisy. W dalszych rozdziałach będziesz się stopniowo uczyć, w jaki sposób uzyskać większą niezależność oraz jak przyjmować mniej kompromisów!

Alicja wybrała pozycję *ACINQ Node* i jest gotowa do otwarcia swojego pierwszego kanału w sieci Lightning Network.

Otwieranie kanału Lightning

Gdy Alicja wybrała węzeł, aby otworzyć nowy kanał, wyświetliło się pytanie o kwotę w bitcoinach, jaką chce zaalokować w tym kanale. W kolejnych rozdziałach omówimy implikacje tych wyborów. Na razie jednak Alicja zaalokowała w tym kanale prawie wszystkie swoje fundusze. Ponieważ Alicja jest zobowiązana do uiszczenia opłat transakcyjnych za otwarcie kanału, wybrała kwotę nieco mniejszą, niż wynosiło jej całkowite saldo[4].

Alicja zaalokowała 0,018 BTC ze swoich 0,020 BTC do swojego kanału i zaakceptowała domyślną stawkę opłaty, co widać na rysunku 2.9.

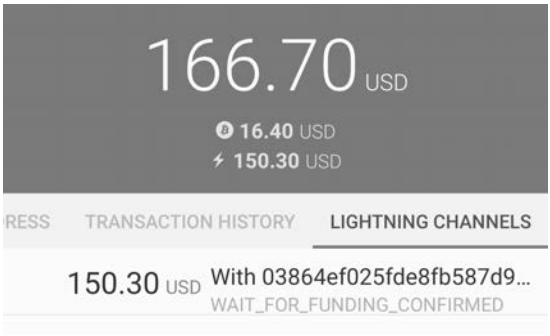


Rysunek 2.9. Otwieranie kanału Lightning

Po kliknięciu *OPEN* jej portfel utworzył specjalną transakcję Bitcoin, zwaną *transakcją finansowania* (ang. *funding transaction*), która otwiera kanał Lightning. Transakcja finansowania jest typu *on-chain* i jest wysyłana do sieci Bitcoin w celu jej potwierdzenia.

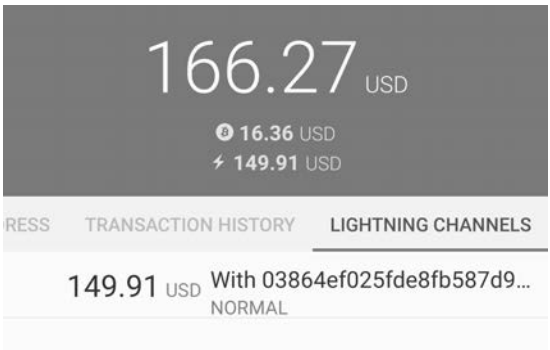
Alicja musi teraz ponownie poczekać (patrz rysunek 2.10), aż transakcja zostanie zarejestrowana w blockchainie Bitcoin. Podobnie jak w przypadku początkowej transakcji Bitcoin, użytej do nabycia bitcoina, Alicja musi poczekać na sześć lub więcej potwierdzeń (około godziny).

[4] Portfel Eclair nie oferuje opcji automatycznego obliczania niezbędnych opłat i przydzielania maksymalnej kwoty środków do kanału, więc Alicja musi sama je obliczyć.



Rysunek 2.10. Oczekiwanie na otwarcie kanału przez transakcję finansowania

Po potwierdzeniu transakcji finansowania kanał Alicji do węzła ACINQ zostaje otwarty, jest sfinansowany i gotowy, co widać na rysunku 2.11.



Rysunek 2.11. Kanał jest otwarty

Być może Ci się wydaje, że kwota kanału się zmieniła. Otóż nie. Kanał zawiera 0,018 BTC, ale w czasie między zrzutami ekranu zmienił się kurs BTC, zatem wartość w USD jest inna. W portfelu możesz wybrać pomiędzy wyświetlaniem salda w BTC lub w USD. Należy jednak pamiętać, że wartości w USD są obliczane w czasie rzeczywistym i się zmieniają!.

Kupowanie filiżanki kawy za pomocą Lightning Network

Alicja ma teraz przygotowane to, co jest jej potrzebne do rozpoczęcia korzystania z Lightning Network. Jak widać, wymagało to trochę pracy i czasu oczekiwania na potwierdzenia. Teraz jednak wszystko może przebiegać szybko i łatwo. Sieć Lightning Network umożliwia dokonywanie płatności bez konieczności czekania na potwierdzenia, ponieważ środki są rozliczane w ciągu kilku sekund. Alicja wzięła swój telefon i poszła do „Kawiarni u Bogdana" w swojej okolicy. Jest podekscytowana perspektywą wypróbowania nowego portfela Lightning. Chce coś kupić!

Kawiarnia u Bogdana

Bogdan posiada prostą aplikację punktu sprzedaży (ang. *point-of-sale* — PoS) dostępną dla każdego klienta, który chciałby płacić bitcoinami w sieci Lightning Network. Jak się dowiesz w następnym rozdziale, Bogdan korzysta z popularnej platformy open source *BTCPay Server*. Zawiera ona niezbędne komponenty rozwiązania e-commerce lub punktu sprzedaży detalicznej, takie jak:

- węzeł Bitcoin korzystający z oprogramowania Bitcoin Core,
- węzeł Lightning korzystający z oprogramowania c-lightning,
- prosta aplikacja PoS na tablet.

BTCPay Server upraszcza instalację potrzebnego oprogramowania, przesyłanie zdjęć i cen produktów oraz pozwala szybko uruchomić sklep.

Na ladzie w „Kawiarni u Bogdana" znajduje się tablet. Jego ekran jest pokazany na rysunku 2.12.

Rysunek 2.12. Aplikacja punktu sprzedaży w Kawiarni u Bogdana

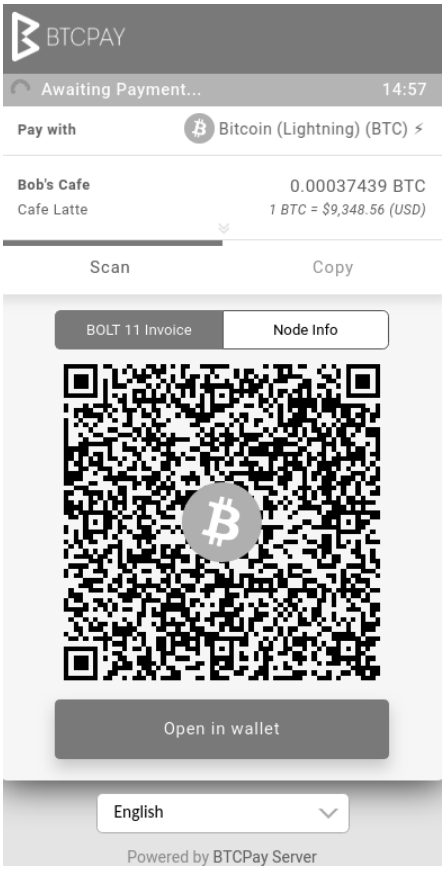
Rachunek Lightning

Alicja wybrała na ekranie opcję *Cafe Latte* i otrzymała rachunek Lightning (nazywany również „żądaniem płatności"), co pokazano na rysunku 2.13.

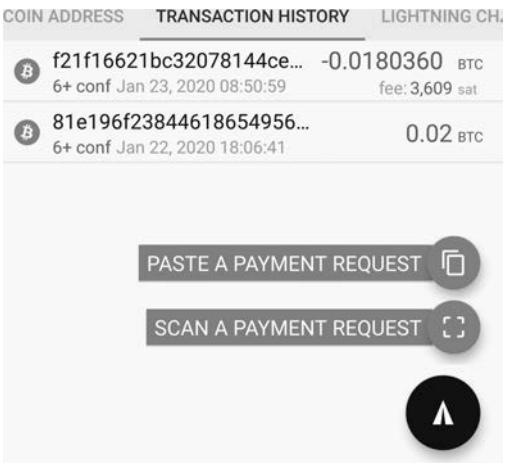
Aby zapłacić rachunek, Alicja otworzyła portfel Eclair i wybrała na karcie *TRANSACTION HISTORY* przycisk przesyłania płatności (oznaczony strzałką w górę), co pokazano na rysunku 2.14.

Termin „żądanie płatności" może się odnosić do żądania płatności Bitcoin lub rachunku Lightning. Terminy „faktura" i „żądanie płatności" są często używane zamiennie. Poprawny termin techniczny to „rachunek Lightning", niezależnie od tego, jak nazywa się w portfelu.

Alicja wybrała opcję *SCAN A PAYMENT REQUEST* (dosłownie: zeskanuj żądanie płatności) i zeskanowała kod QR wyświetlany na ekranie tabletu (patrz rysunek 2.13). Wyświetliła się prośba o potwierdzenie płatności, co pokazano na rysunku 2.15.



Rysunek 2.13. Rachunek Lightning za latte Alicji



Rysunek 2.14. Alicja powinna kliknąć przycisk Send

Rysunek 2.15. Potwierdzenie transakcji Alicji

Alicja nacisnęła *PAY*, a sekundę później na tablecie Bogdana wyświetliła się potwierdzona płatność. Alicja wykonała swoją pierwszą płatność LN! Płatność była szybka, niedroga i łatwa. Teraz może cieszyć się kawą latte kupioną za pomocą bitcoinów za pośrednictwem systemu płatności, który jest szybki, tani i zdecentralizowany. Od teraz Alicja może wybrać towar na ekranie tabletu Bogdana, zeskanować kod QR za pomocą telefonu komórkowego, kliknąć *PAY* i otrzymać kawę. Wszystko w ciągu kilku sekund i bez transakcji w trybie *on-chain*.

Płatności Lightning dla Bogdana również są lepsze. Jest przekonany, że otrzyma zapłatę za latte Alicji bez oczekiwania na potwierdzenie transakcji *on-chain*. Następnym razem, gdy Alicja będzie miała ochotę wypić kawę w „Kawiarni u Bogdana", będzie mogła zapłacić bitcoinami w sieci Bitcoin lub Lightning Network. Którą metodę wybierze Twoim zdaniem?

Podsumowanie

W tym rozdziale obserwowaliśmy Alicję podczas pobierania i instalowania pierwszego portfela Lightning. Alicja nabyła trochę bitcoinów, otworzyła swój pierwszy kanał Lightning i kupiła filiżankę kawy, za którą zapłaciła z wykorzystaniem Lightning Network. W dalszych rozdziałach zajrzymy „pod maskę" wszystkich komponentów w Lightning Network i się dowiesz, w jaki sposób płatność Alicji dotarła do „Kawiarni u Bogdana".

Skorowidz

A

B

C

D

E

F

G

H

I

J

K

L

Ł

M

N

O

P

R

S

Ś

T

U

V

W

Z

Ż

Poznaj potencjał LN i zostań mistrzem technologii przyszłości!

Potencjał blockchaina jest ogromny i zapewne wciąż nie znamy jego wszystkich możliwych zastosowań. Jest to dosyć nowa, dynamicznie rozwijająca się technologia, już teraz jednak dostrzegalne są pewne jej ograniczenia. Problemem jest na przykład skalowalność bitcoina. Rozwiązaniem wydaje się Lightning Network (LN), protokół drugiej warstwy, który zapewnia niemal natychmiastowe transakcje w systemie bitcoina. Umożliwia również zwiększenie szybkości i prywatności zawieranych transakcji, a przy tym pozwala na zmniejszenie opłat.

To książka przeznaczona dla osób, które chcą zrozumieć działanie Lightning Network i wykorzystać możliwości tej technologii we własnych aplikacjach. Z lektury skorzystają programiści, architekci systemowi i inżynierowie. Omówiono tu podstawy funkcjonowania sieci LN i sposoby jej użycia w praktyce. Przedstawiono również zasady oprogramowywania węzłów Lightning, ich implementacji i konfiguracji, a także zagadnienia budowania kanałów płatności w systemie bitcoina, obsługi kanałów i przekazywania płatności. Zaprezentowano też informacje dotyczące bezpieczeństwa i prywatności w sieci Lightning Network. Poszczególne zagadnienia zostały zilustrowane praktycznymi przykładami kodu w językach Go, C++, Python i przy użyciu wiersza poleceń uniksowych systemów operacyjnych.

W książce między innymi:

- technologia Lightning Network a skalowanie blockchaina
- standardy stosowane w Lightning Network
- warstwy zestawu protokołów Lightning Network
- portfele i węzły oraz ich obsługa
- kanały płatności Lightning, routing cebulowy i protokół plotkarski
- kanały płatności od nadawcy do odbiorcy w trybie off-chain

Andreas M. Antonopoulos jest autorem, nauczycielem i jednym z czołowych ekspertów w dziedzinie bitcoina i otwartego blockchaina.

Olaoluwa Osuntokun jest programistą bitcoina, naukowcem i dyrektorem technicznym firmy Lightning Labs.

René Pickhardt jest konsultantem w dziedzinie inżynierii danych i naukowcem. Dzięki swojej pracy nad routingiem płatności odkrył tanie i niezawodne przepływy płatności, określane jako „płatności Pickhardta".

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-283-9322-6
9 788328 393226
Cena: 119,00 zł