

Lightning Network dla praktyków : protokół drugiej warstwy i jego wykorzystanie do obsługi płatności bitcoinami / Andreas M. Antonopoulos, Osuntokun Olaoluwa, Pickhardt René. – Gliwice, © 2023

Spis treści

Przedmowa	15
------------------	-----------

Część I. Podstawy Lightning Network

1. Wprowadzenie	25
------------------------	-----------

Lightning Network — podstawowe pojęcia	25
Zaufanie w sieciach zdecentralizowanych	27
Uczciwość bez organu centralnego	28
Protokoły zaufania bez pośredników	28
Protokół uczciwości w działaniu	29
Prymitywy zabezpieczeń jako bloki konstrukcyjne	30
Przykład protokołu uczciwości	31
Sens istnienia sieci Lightning Network	32
Skalowanie łańcuchów bloków	33
Cechy charakterystyczne Lightning Network	35
Przypadki użycia Lightning Network, użytkownicy i ich historie	35
Podsumowanie	36

2. Pierwsze kroki	37
--------------------------	-----------

Pierwszy portfel Lightning Alicji	37
Węzły Lightning	38
Eksploratory Lightning	38
Portfele Lightning	39
Bitcoin Testnet	42
Równoważenie złożoności i kontroli	42
Pobieranie i instalowanie portfela Lightning	43
Tworzenie nowego portfela	44
Odpowiedzialność związana z przechowywanymi kluczami	44
Słowa mnemoniczne	45
Bezpieczne przechowywanie frazy mnemonicznej	46
Ładowanie bitcoinów do portfela	46
Zdobywanie bitcoinów	47
Odbieranie bitcoinów	47
Od sieci Bitcoin do Lightning Network	50
Kanały sieci Lightning Network	50
Otwieranie kanału Lightning	53
Kupowanie filiżanki kawy za pomocą Lightning Network	54
Kawiarnia u Bogdana	55

Rachunek Lightning	55
Podsumowanie	57
3. Jak działa sieć Lightning Network?	58
Czym jest kanał płatności?	59
Podstawowe informacje o kanale płatności	59
Routowanie płatności między kanałami	60
Kanały płatności	61
Adres wielopodpisowy	62
Transakcja finansowania	62
Transakcja zobowiązania	63
Oszukiwanie z wykorzystaniem poprzedniego stanu	65
Ogłaszanie kanału	67
Zamykanie kanału	68
Faktury	72
Skrót płatności i preobraz	73
Dodatkowe metadane	73
Dostarczanie płatności	74
Protokół plotkarski peer-to-peer	74
Znajdowanie ścieżek i wyznaczanie tras	76
Znajdowanie ścieżek oparte na źródle	76
Routing cebulowy	77
Algorytm przekazywania płatności	79
Szyfrowanie komunikacji peer-to-peer	80
Garść uwag o zaufaniu	81
Porównanie z Bitcoinem	81
Adresy kontra faktury, transakcje kontra płatności	81
Wybieranie wyjść a znajdowanie ścieżki	82
Zmiana wyjść w sieci Bitcoin kontra brak zmian w sieci Lightning	82
Opłaty za wydobycie a opłaty za routing	83
Różne opłaty w zależności od ruchu w porównaniu z opłatami ogłaszanymi	83
Publiczne transakcje Bitcoin kontra prywatne płatności Lightning	84
Oczekiwanie na potwierdzenie kontra natychmiastowe rozliczenie	84
Wysyłanie dowolnych kwot kontra ograniczenia pojemności	85
Zachęta do płatności o dużej wartości kontra zachęta do płatności o małej wartości	85
Korzystanie z blockchaina jako księgi kontra „system sądowy”	85
Offline kontra online, operacje asynchroniczne kontra synchroniczne	86
Satoshi kontra milisatoshi	86
Cechy wspólne sieci Bitcoin i Lightning Network	87
Jednostka monetarna	87
Nieodwracalność i ostateczność płatności	87
Zaufanie i ryzyko kontrahenta	87
Operacje w trybie „bez uprawnień”	87
Open Source i Open System	88

Podsumowanie	88
4. Oprogramowanie węzłów Lightning	89
Środowisko programistyczne Lightning	90
Korzystanie z wiersza polecenia	90
Pobieranie repozytorium książki	91
Kontenery Docker	91
Bitcoin Core i Regtest	93
Budowanie kontenera Bitcoin Core	93
Projekt c-lightning	96
Budowanie c-lightning jako kontenera Docker	96
Konfiguracja sieci Docker	97
Uruchamianie kontenerów bitcoind i c-lightning	97
Instalowanie c-lightning z kodu źródłowego	99
Instalowanie wymaganych bibliotek i pakietów	99
Kopiowanie kodu źródłowego c-lightning	100
Kompilowanie kodu źródłowego c-lightning	100
Projekt węzła Lightning Network Daemon	102
Kontener Docker węzła LND	102
Uruchamianie kontenerów bitcoind i LND	103
Instalowanie kontenera LND z kodu źródłowego	104
Kopiowanie kodu źródłowego LND	105
Kompilowanie kodu źródłowego LND	106
Projekt węzła Eclair Lightning	106
Kontener Docker serwera Eclair	106
Uruchamianie kontenerów bitcoind i Eclair	107
Instalowanie serwera Eclair z kodu źródłowego	109
Kopiowanie kodu źródłowego Eclair	109
Kompilowanie kodu źródłowego Eclair	109
Budowanie kompletnej sieci z różnych węzłów Lightning	110
Korzystanie z funkcji docker-compose do orkiestracji kontenerów	
Docker	111
Konfigurowanie polecenia docker-compose	111
Uruchamianie przykładu Lightning Network	112
Otwieranie kanałów i routowanie płatności	113
Podsumowanie	115
5. Obsługa węzła sieci Lightning Network	116
Wybór platformy	117
Dlaczego ważna jest niezawodność działania węzła Lightning?	117
Rodzaje sprzętu dla węzłów Lightning	117
Utrzymywanie węzła w chmurze	118
Uruchamianie węzła w warunkach domowych	118
Jaki sprzęt jest wymagany do uruchomienia węzła Lightning?	119
Przełączanie konfiguracji serwerowej w chmurze	120
Korzystanie z instalatora lub pomocnika	121

RaspiBlitz	122
Mynode	123
Umbrel	123
BTCPay Server	124
Węzeł Bitcoin czy węzeł Lightning w trybie uproszczonym?	125
Wybór systemu operacyjnego	126
Wybór implementacji węzła Lightning	126
Instalowanie węzła Bitcoin lub Lightning	127
Usługi w tle	128
Izolacja procesu	128
Uruchamianie węzła	129
Konfiguracja węzła	130
Konfiguracja sieci	131
Bezpieczeństwo węzła	136
Bezpieczeństwo systemu operacyjnego	136
Dostęp do węzłów	137
Kopie zapasowe węzłów i kanałów	138
Zagrożenia dla gorących portfeli	140
„Wymiatanie” funduszy	140
Czas pracy i dostępność węzła Lightning	142
Tolerowanie błędów i automatyzacja	143
Monitorowanie dostępności węzłów	144
Monitorowanie dostępności węzłów	144
Wieże strażnicze	144
Zarządzanie kanałami	146
Otwieranie kanałów wychodzących	146
Osiąganie płynności przychodzącej	149
Zamykanie kanałów	150
Rebalancing kanałów	150
Opłaty za routing	152
Zarządzanie węzłami	153
Ride The Lightning	153
Indmon	154
ThunderHub	154
Podsumowanie	154

Część II. Lightning Network w szczegółach

6. Architektura Lightning Network	157
Zestaw protokołów Lightning Network Protocol Suite	157
Lightning w szczegółach	158
7. Kanały płatności	160
Inny sposób korzystania z systemu Bitcoin	161
Własność sieci Bitcoin i zarządzanie nią	162
Różnorodność (niezależnej) własności i wielopodpisowość	162

Współwłasność bez niezależnej kontroli	162
Niedopuszczenie do zablokowania bitcoinów i przekształcenia ich w niemożliwe do wydania	163
Konstruowanie kanału płatności	163
Prywatne i publiczne klucze węzłów	163
Sieciowy adres węzła	164
Identyfikatory węzłów	164
Łączenie węzłów jako bezpośrednich partnerów	165
Budowanie kanału	165
Protokół partnerski do zarządzania kanałem	165
Przepływ komunikatów podczas ustanawiania kanału	165
Transakcja finansowania	169
Generowanie adresu wielopodpisowego	169
Konstruowanie transakcji finansowania	169
Utrzymywanie podpisanych transakcji bez ich publikowania	170
Refundacja przed finansowaniem	170
Konstruowanie wstępnie podpisanej transakcji zwrotu	171
Łączenie transakcji w łańcuch bez publikowania	171
Rozwiązywanie problemu plastyczności (Segregated Witness)	172
Publikowanie transakcji finansowania	174
Wysyłanie płatności przez kanał	175
Podział salda	175
Konkurencyjne zobowiązania	176
Oszustwa z wykorzystaniem przedawnionych transakcji zobowiązania	177
Odwoływanie nieaktualnych transakcji zobowiązania	177
Asymetryczne transakcje zobowiązania	178
Opóźnione (zablokowane w czasie) wydatki to_self	179
Klucze odwołania	180
Transakcja zobowiązania	180
Zmiany stanu kanału	182
Komunikat commitment_signed	183
Komunikat revoke_and_ack	184
Odwoływanie i ponowne zobowiązanie	184
Oszukiwanie i karanie w praktyce	185
Rezerwacja kanału: zapewnienie ryzyka w grze	188
Zamykanie kanału (zamknięcie wzajemne)	188
Komunikat shutdown	189
Komunikat closing_signed	189
Transakcja wzajemnego zamknięcia	190
Podsumowanie	191
8. Routing w sieci kanałów płatności	192
Routowanie płatności	192
Routing a znajdowanie ścieżek	194
Tworzenie sieci kanałów płatności	194
Fizyczny przykład „routingu”	195

Protokół uczciwości	200
Implementacja atomowych, wieloprzeskokowych płatności w trybie „bez zaufania”	201
Wracamy do przykładu napiwków	201
Rozliczanie kontraktów HTLC w trybie on-chain a rozliczanie ich w trybie off-chain	203
Kontrakty HTLC	203
Kontrakty HTLC w Bitcoin Script	204
Preobraz płatności i weryfikacja skrótu	205
Rozszerzanie kontraktu HTLC od Alicji do Darii	206
Wsteczne propagowanie sekretu	207
Wiązanie podpisów: zabezpieczenia kontraktów HTLC przed kradzieżą	209
Optymalizacja skrótów	210
Kooperatywne kontrakty HTLC i błędy limitu czasu	212
Zmniejszanie blokad czasowych	213
Podsumowanie	213
9. Obsługa kanału i przekazywanie płatności	215
Lokalne (jednokanałowe) a routowane (wielokanałowe)	216
Przekazywanie płatności i aktualizacja zobowiązań za pomocą kontraktów HTLC	216
Przepływ komunikatów związanych z HTLC i transakcjami zobowiązań	216
Przekazywanie płatności z wykorzystaniem kontraktów HTLC	217
Dodawanie kontraktu HTLC	217
Komunikat update_add_HTLC	218
Kontrakty HTLC w transakcjach zobowiązania	219
Nowe zobowiązanie z wyjściem HTLC	220
Zobowiązania Alicji	221
Bogdan uznaje nowe zobowiązanie i odwołuje stare	222
Zobowiązania Bogdana	224
Wielokrotne kontrakty HTLC	225
Realizacja kontraktu HTLC	226
Propagacja HTLC	226
Daria wypełnia kontrakt HTLC z Chanem	226
Bogdan rozlicza HTLC z Alicją	227
Usuwanie kontraktu HTLC z powodu błędu lub wygaśnięcia ważności	230
Wykonywanie płatności lokalnej	231
Podsumowanie	232
10. Routing cebulowy	233
Fizyczny przykład ilustrujący routing cebulowy	234
Wybieranie ścieżki	234
Budowanie warstw	235
Obieranie warstw	237
Wprowadzenie do routingu cebulowego opartego na kontraktach HTLC	238
Alicja wybiera ścieżkę	238

Alicja konstruuje ładunki kanału	240
Generowanie kluczy	243
„Owijanie” warstw cebuli	247
Cebule o stałej długości	247
Owijanie cebuli (zarys)	247
Owijanie ładunku przeskoku Darii	249
Opakowywanie ładunku przeskoku Chana	253
Opakowywanie ładunku przeskoku Bogdana	254
Końcowa postać pakietu cebuli	255
Wysyłanie cebuli	256
Komunikat update_add_htlc	256
Alicja wysyła cebulę do Bogdana	256
Bogdan sprawdza cebulę	257
Bogdan generuje wypełniacz	257
Bogdan usuwa zaciemnienie swojego ładunku przeskoku	257
Bogdan wydobywa zewnętrzny skrót HMAC dla następnego przeskoku	258
Bogdan usuwa swój ładunek i przesuwą zawartość cebuli w lewo	259
Bogdan konstruuje nowy pakiet cebuli	260
Bogdan weryfikuje szczegóły kontraktu HTLC	260
Bogdan wysyła komunikat update_add_htlc do Chana	260
Chan przekazuje cebulę	261
Daria otrzymuje ostateczny ładunek	261
Zwracanie błędów	262
Komunikaty o błędach	263
Spontaniczne płatności Keysend	265
Niestandardowe rekordy TLV cebuli	265
Wysyłanie i odbieranie płatności Keysend	266
Płatności Keysend i niestandardowe rekordy w aplikacjach Lightning	266
Podsumowanie	266
11. Plotki i graf kanałów	267
Odkrywanie węzłów partnerskich	269
Bootstrapping w sieci P2P	270
Bootstrapping DNS	270
Opcje zapytań SRV	274
Graf kanałów	275
Graf skierowany	275
Komunikaty protokołu plotkarskiego	276
Komunikat node_announcement	276
Komunikat channel_announcement	278
Komunikat channel_update	282
Bieżące utrzymywanie grafu kanałów	283
Podsumowanie	283
12. Znajdowanie ścieżek i dostarczanie płatności	284
Znajdowanie ścieżek w pakiecie protokołów Lightning Protocol Suite	284

Gdzie jest BOLT?	285
Znajdowanie ścieżek. Jaki problem rozwiązujemy?	285
Wybieranie najlepszej ścieżki	286
Znajdowanie ścieżek w matematyce i informatyce	286
Pojemność, saldo, płynność	287
Niepewność sald	287
Złożoność znajdowania ścieżek	288
Zachowaj prostotę	289
Znajdowanie ścieżek i dostarczanie płatności	289
Konstrukcja grafu kanałów	290
Niepewność płynności i prawdopodobieństwo	293
Opłaty i inne metryki kanałów	294
Znajdowanie ścieżek kandydatów	295
Dostarczanie płatności (pętla prób i błędów)	296
Pierwsza próba (ścieżka nr 1)	296
Druga próba (ścieżka nr 4)	297
Płatności wieloczęściowe	298
Korzystanie z płatności MPP	299
Próby i błędy w wielu „rundach”	300
Podsumowanie	302

13. Protokół łącza fizycznego: tworzenie ramek i rozszerzalność 303

Warstwa komunikatów w pakiecie protokołów Lightning Protocol Suite	303
Tworzenie ramek łącza fizycznego	304
Wysokopoziomowe tworzenie ramki łącza fizycznego	304
Kodowanie typów	305
Rozszerzenia komunikatów „Typ-Długość-Wartość”	306
Format komunikatów Protobuf	306
Zgodność wstecz i w przód	306
Format „Typ-Długość-Wartość”	307
Kodowanie z wykorzystaniem typu BigSize	307
Ograniczenia kodowania TLV	308
Kodowanie kanoniczne TLV	308
Bity funkcji i rozszerzalność protokołu	309
Bity funkcji jako mechanizm wykrywania uaktualnień	309
TLV dla zgodności wstecz i w przód	310
Taksonomia mechanizmów aktualizacji	311
Uaktualnienia „od końca do końca”	311
Aktualizacje na poziomie budowy kanału	312
Podsumowanie	312

14. Szyfrowany transport komunikatów w Lightning Network 313

Szyfrowany transport w pakiecie protokołów Lightning Protocol Suite	313
Wprowadzenie	314
Graf kanałów jako zdecentralizowana infrastruktura klucza publicznego	314
Dlaczego nie TLS?	315

Framework protokołów Noise	315
Szyfrowany transport Lightning w szczegółach	316
Noise_XK: uzgadnianie w Lightning Network	316
Notacja uzgadniania i przepływ protokołu	316
Ogólny przebieg protokołu	317
Uzgadnianie w trzech aktach	318
Podsumowanie	326
15. Żądania płatności w sieci Lightning	327
Faktury w pakiecie protokołów Lightning Protocol Suite	327
Wprowadzenie	327
Żądania płatności Lightning a adresy Bitcoin	328
BOLT nr 11: serializacja i interpretacja żądania płatności w Lightning	329
Kodowanie żądań płatności w praktyce	329
Prefiks czytelny dla człowieka	329
bech32 i segment danych	330
Podsumowanie	332
16. Bezpieczeństwo i prywatność w Lightning Network	333
Dlaczego prywatność jest ważna?	333
Definicje prywatności	333
Proces oceny prywatności	334
Zbiór anonimowości	335
Różnice między Lightning Network a Bitcoinem w kontekście prywatności	336
Ataki na sieć Lightning	338
Obserwowanie kwot płatności	338
Łączenie nadawców z odbiorcami	338
Ujawnianie sald kanałów (sondowanie)	339
Ataki DoS	341
Zagłuszanie zobowiązań	343
Blokada płynności kanału	343
Dezanonimizacja obejmująca wiele warstw	343
Klasteryzacja podmiotów on-chain Bitcoina	344
Klasteryzacja węzłów off-chain w sieci Lightning Network	345
Łączenie obejmujące wiele warstw: węzły Lightning i podmioty Bitcoin	345
Graf sieci Lightning	346
Jak naprawdę wygląda graf sieci Lightning?	346
Centralizacja w sieci Lightning Network	349
Zachęty ekonomiczne a struktura grafu	349
Praktyczne porady co do ochrony prywatności użytkowników	350
Kanały nieogłoszone	350
Zagadnienia dotyczące routingu	351
Akceptowanie kanałów	351
Podsumowanie	352
Bibliografia i dalsza lektura	353

17. Podsumowanie	354
Innowacje asynchroniczne i zdecentralizowane	354
Usprawnienia protokołu Bitcoin i języka Bitcoin Script	355
Innowacje w protokole Lightning	355
Rozszerzalność TLV	356
Konstrukcja kanału płatności	356
Funkcje opt-in	356
Aplikacje Lightning (LApps)	357
Gotowi, do startu, start!	357
 A. Podstawy Bitcoina — przegląd	 359
 B. Podstawowa instalacja i użytkowanie platformy Docker	 377
 C. Komunikaty protokołu komunikacyjnego	 380
 D. Źródła i informacje o licencjach	 395
 Glosariusz	 397
 Skorowidz	 414

oprac. BPK