Zrozumieć Bitcoin : programowanie kryptowalut od podstaw / Jimmy Song. – Gliwice, © 2020

Spis treści

Przedmowa **11**

Wprowadzenie **13**

Rozdział 1. Ciała skończone **23**
Trochę matematyki wyższej 23
Definicja ciała skończonego 24
Definiowanie zbiorów skończonych 25
Tworzenie ciała skończonego w Pythonie 25
Ćwiczenie 1. 26
Arytmetyka modulo 26
Arytmetyka modulo w Pythonie 28
Dodawanie i odejmowanie w ciele skończonym 29
Ćwiczenie 2. 30
Programowanie dodawania i odejmowania w Pythonie 30
Ćwiczenie 3. 31
Mnożenie i potęgowanie w ciele skończonym 31
Ćwiczenie 4. 32
Ćwiczenie 5. 32
Programowanie mnożenia w Pythonie 32
Ćwiczenie 6. 33
Programowanie potęgowania w Pythonie 33
Ćwiczenie 7. 33
Dzielenie w ciele skończonym 33
Ćwiczenie 8. 35
Ćwiczenie 9. 35
Redefiniowanie potęgowania 36
Podsumowanie 37

Rozdział 2. Krzywe eliptyczne **39**
Definicja 39
Kodowanie krzywych eliptycznych w Pythonie 44
Ćwiczenie 1. 45
Ćwiczenie 2. 45
Dodawanie punktów 45
Matematyka dodawania punktów 49
Programowanie dodawania punktów 51
Ćwiczenie 3. 52
Dodawanie punktów, gdy $x_1 \neq x_2$ 52

Ćwiczenie 4. 54
Dodawanie punktów, gdy $x_1 \neq x_2$ 54
Ćwiczenie 5. 54
Dodawanie punktów, gdy $P_1 = P_2$ 54
Ćwiczenie 6. 55
Programowanie dodawania punktów, gdy $P_1 = P_2$ 56
Ćwiczenie 7. 56
Programowanie jeszcze jednego przypadku 56
Podsumowanie 57

Rozdział 3. Kryptografia krzywych eliptycznych 59
Krzywe eliptyczne nad ciałem liczb rzeczywistych 59
Krzywe eliptyczne nad ciałami skończonymi 60
Ćwiczenie 1. 61
Programowanie krzywych eliptycznych nad ciałami skończonymi 62
Dodawanie punktów nad ciałami skończonymi 63
Programowanie dodawania punktów na krzywej nad ciałami skończonymi 64
Ćwiczenie 2. 64
Ćwiczenie 3. 65
Mnożenie skalarne dla krzywych eliptycznych 65
Ćwiczenie 4. 67
Mnożenie skalarne — druga odsłona 67
Grupy w matematyce 68
Element neutralny 68
Zamkniętość 69
Element odwrotny 70
Przemienność 70
Łączność 70
Ćwiczenie 5. 70
Programowanie mnożenia skalarnego 72
Definiowanie krzywej dla Bitcoina 74
Korzystanie z krzywej secp256k1 75
Kryptografia klucza publicznego 76
Podpisywanie i weryfikacja 77
Wpisywanie celu 78
Szczegóły weryfikacji 79
Weryfikacja podpisu 81
Ćwiczenie 6. 81
Programowanie weryfikacji podpisów 82
Szczegóły podpisywania 82
Tworzenie podpisu 83
Ćwiczenie 7. 84
Programowanie podpisywania komunikatów 84
Podsumowanie 86

Rozdział 4. Serializacja **87**
Nieskompresowany format SEC 87
Ćwiczenie 1. 89
Skompresowany format SEC 89
Ćwiczenie 2. 92
Podpisy DER 92
Ćwiczenie 3. 94
Base58 94
Przesyłanie klucza publicznego 94
Ćwiczenie 4. 96
Format adresu 96
Ćwiczenie 5. 97
Format WIF 97
Ćwiczenie 6. 98
Porządek bajtowy (big- i little-endian) — dodatkowe informacje 98
Ćwiczenie 7. 98
Ćwiczenie 8. 98
Ćwiczenie 9. 99
Podsumowanie 99

Rozdział 5. Transakcje **101**
Składniki transakcji 101
Wersja 103
Ćwiczenie 1. 104
Wejścia 104
Przetwarzanie pola ze skryptem 108
Ćwiczenie 2. 108
Wyjścia 108
Ćwiczenie 3. 110
Czas blokady 110
Ćwiczenie 4. 110
Ćwiczenie 5. 111
Kodowanie transakcji 111
Opłata transakcyjna 112
Obliczanie opłaty transakcyjnej 113
Ćwiczenie 6. 113
Podsumowanie 114

Rozdział 6. Język Script **115**
Zasada działania języka Script 115
Jak działa Script? 116
Przykładowe operacje 117
Programowanie obsługi kodów operacji 118
Ćwiczenie 1. 118
Przetwarzanie pól ze skryptami 119
Programowanie analizatora składniowego i serializatora pól skryptów 120

Scalanie pól ze skryptami 121
Programowanie scalania skryptów 122
Skrypty standardowe 122
p2pk 123
Programowanie interpretera skryptów 125
Elementy stosu pod lupą 127
Ćwiczenie 2. 128
Problemy z p2pk 128
Rozwiązywanie problemów za pomocą p2pkh 130
p2pkh 130
Skrypty mogą być konstruowane dowolnie 134
Ćwiczenie 3. 136
Użyteczność skryptów 137
Ćwiczenie 4. 137
Wyzwanie: znalezienie kolizji SHA-1 137
Podsumowanie 137

Rozdział 7. Tworzenie i walidacja transakcji 139
Walidacja transakcji 139
Sprawdzanie wydania wejść 139
Sprawdzanie sumy wejść i sumy wyjść 140
Sprawdzanie podpisu 141
Ćwiczenie 1. 144
Ćwiczenie 2. 144
Weryfikacja całej transakcji 144
Tworzenie transakcji 145
Konstruowanie transakcji 145
Tworzenie transakcji 148
Podpisywanie transakcji 149
Ćwiczenie 3. 150
Tworzenie własnych transakcji w testnecie 150
Ćwiczenie 4. 150
Ćwiczenie 5. 150
Podsumowanie 151

Rozdział 8. Pay-to-script-hash 153
Czysty multisig 153
Programowanie obsługi OP_CHECKMULTISIG 157
Ćwiczenie 1. 158
Problemy z czystym multisig 158
Pay-to-script-hash (p2sh) 158
Programowanie p2sh 164
Bardziej skomplikowane skrypty 165
Adresy 165
Ćwiczenie 2. 166
Ćwiczenie 3. 166

Weryfikacja podpisów p2sh 166
Ćwiczenie 4. 169
Ćwiczenie 5. 169
Podsumowanie 169

Rozdział 9. Bloki 171
Transakcje coinbase 171
Ćwiczenie 1. 172
ScriptSig 172
BIP0034 173
Ćwiczenie 2. 173
Nagłówki bloków 174
Ćwiczenie 3. 175
Ćwiczenie 4. 175
Ćwiczenie 5. 175
Wersja 175
Ćwiczenie 6. 176
Ćwiczenie 7. 176
Ćwiczenie 8. 176
Poprzedni blok 177
Korzeń drzewa skrótów 177
Znacznik czasu 177
Sekwencja bitowa 177
Wartość nonce 178
Dowód pracy 178
W jaki sposób górnik generuje nowe skróty? 179
Cel 179
Ćwiczenie 9. 180
Trudność 180
Ćwiczenie 10. 181
Sprawdzanie dowodu pracy 181
Ćwiczenie 11. 181
Zmiana trudności 181
Ćwiczenie 12. 183
Ćwiczenie 13. 183
Podsumowanie 183

Rozdział 10. Techniki sieciowe 185
Komunikaty sieciowe 185
Ćwiczenie 1. 186
Ćwiczenie 2. 186
Ćwiczenie 3. 187
Interpretowanie treści komunikatu 187
Ćwiczenie 4. 188
Uzgadnianie komunikacji w sieci 188
Łączenie się z siecią 188

Ćwiczenie 5. 191
Odbieranie nagłówków bloków 191
Ćwiczenie 6. 192
Odpowiedź z nagłówkami 192
Podsumowanie 194

Rozdział 11. Uproszczona weryfikacja płatności 195
Motywacja 195
Drzewo skrótów 196
Element nadrzędny 197
Ćwiczenie 1. 198
Poziom nadrzędny drzewa skrótów 198
Ćwiczenie 2. 199
Korzeń drzewa skrótów 199
Ćwiczenie 3. 200
Korzeń drzewa skrótów w blokach 200
Ćwiczenie 4. 201
Korzystanie z drzewa skrótów 201
Blok drzewa skrótów 202
Struktura drzewa skrótów 204
Ćwiczenie 5. 205
Programowanie obsługi drzewa skrótów 205
Komunikat sieciowy merkleblock 209
Ćwiczenie 6. 210
Wykorzystanie flag bitowych i skrótów 211
Ćwiczenie 7. 214
Podsumowanie 214

Rozdział 12. Filtry Blooma 215
Czym jest filtr Blooma? 215
Ćwiczenie 1. 217
Krok dalej 217
Filtry Blooma według BIP0037 218
Ćwiczenie 2. 220
Ćwiczenie 3. 220
Ładowanie filtra Blooma 220
Ćwiczenie 4. 220
Pobieranie bloków drzewa skrótów 221
Ćwiczenie 5. 221
Pobieranie interesujących nas transakcji 221
Ćwiczenie 6. 223
Podsumowanie 223

Rozdział 13. Segwit 225
Pay-to-witness-pubkey-hash (p2wpkh) 225
Kowalność transakcji 225

Eliminowanie kowalności 226
Transakcje p2wpkh 227
p2sh-p2wpkh 230
Programowanie p2wpkh i p2sh-p2wpkh 234
Pay-to-witness-script-hash (p2wsh) 237
p2sh-p2wsh 241
Programowanie p2wsh i p2sh-p2wsh 246
Inne usprawnienia 247
Podsumowanie 248

Rozdział 14. Tematy zaawansowane i dalsze kroki 249
Proponowane tematy do dalszej nauki 249
Portfele 249
Kanały płatnicze i sieć Lightning 250
Społeczność 250
Proponowane dalsze projekty 251
Portfel test netowy 251
Eksplorator bloków 251
Sklep internetowy 251
Biblioteka narzędzi 252
Poszukiwanie pracy 252
Podsumowanie 252

Dodatek A. Rozwiązania ćwiczeń 253

Skorowidz 287

oprac. BPK