

Spis treści

- Przedmowa
- Wprowadzenie
 - Dla kogo jest przeznaczona ta książka?
 - Co muszę umieć?
 - Jak uporządkowany jest materiał w tej książce?
 - Przygotowanie środowiska
 - Rozwiązania
 - Konwencje zastosowane w tej książce
 - Korzystanie z kodu zawartego w tej książce
 - Podziękowania
- Rozdział 1. Ciała skończone
 - Trochę matematyki wyższej
 - Definicja ciała skończonego
 - Definiowanie zbiorów skończonych
 - Tworzenie ciała skończonego w Pythonie
 - Ćwiczenie 1.
 - Arytmetyka modulo
 - Arytmetyka modulo w Pythonie
 - Dodawanie i odejmowanie w ciele skończonym
 - Ćwiczenie 2.
 - Programowanie dodawania i odejmowania w Pythonie
 - Ćwiczenie 3.
 - Mnożenie i potęgowanie w ciele skończonym
 - Ćwiczenie 4.
 - Ćwiczenie 5.
 - Programowanie mnożenia w Pythonie
 - Ćwiczenie 6.
 - Programowanie potęgowania w Pythonie
 - Ćwiczenie 7.
 - Dzielenie w ciele skończonym

- Ćwiczenie 8.
 - Ćwiczenie 9.
 - Redefiniowanie potęgowania
 - Podsumowanie
- Rozdział 2. Krzywe eliptyczne
 - Definicja
 - Kodowanie krzywych eliptycznych w Pythonie
 - Ćwiczenie 1.
 - Ćwiczenie 2.
 - Dodawanie punktów
 - Matematyka dodawania punktów
 - Programowanie dodawania punktów
 - Ćwiczenie 3.
 - Dodawanie punktów, gdy $x_1 \neq x_2$
 - Ćwiczenie 4.
 - Dodawanie punktów, gdy $x_1 = x_2$
 - Ćwiczenie 5.
 - Dodawanie punktów, gdy $P_1 = P_2$
 - Ćwiczenie 6.
 - Programowanie dodawania punktów, gdy $P_1 \neq P_2$
 - Ćwiczenie 7.
 - Programowanie jeszcze jednego przypadku
 - Podsumowanie
- Rozdział 3. Kryptografia krzywych eliptycznych
 - Krzywe eliptyczne nad ciałem liczb rzeczywistych
 - Krzywe eliptyczne nad ciałami skończonymi
 - Ćwiczenie 1.
 - Programowanie krzywych eliptycznych nad ciałami skończonymi
 - Dodawanie punktów nad ciałami skończonymi
 - Programowanie dodawania punktów na krzywej nad ciałami skończonymi
 - Ćwiczenie 2.

- Ćwiczenie 3.
- Mnożenie skalarne dla krzywych eliptycznych
 - Ćwiczenie 4.
- Mnożenie skalarne druga odłona
- Grupy w matematyce
 - Element neutralny
 - Zamkniętość
 - Element odwrotny
 - Przemienność
 - Łączność
 - Ćwiczenie 5.
- Programowanie mnożenia skalarnego
- Definiowanie krzywej dla Bitcoina
 - Korzystanie z krzywej secp256k1
- Kryptografia klucza publicznego
- Podpisywanie i weryfikacja
 - Wpisywanie celu
 - Szczegóły weryfikacji
 - Weryfikacja podpisu
 - Ćwiczenie 6.
 - Programowanie weryfikacji podpisów
 - Szczegóły podpisywania
 - Tworzenie podpisu
 - Ćwiczenie 7.
 - Programowanie podpisywania komunikatów
- Podsumowanie
- Rozdział 4. Serializacja
 - Nieskompresowany format SEC
 - Ćwiczenie 1.
 - Skompresowany format SEC
 - Ćwiczenie 2.

- Podpisy DER
 - Ćwiczenie 3.
- Base58
 - Przesyłanie klucza publicznego
 - Ćwiczenie 4.
 - Format adresu
 - Ćwiczenie 5.
 - Format WIF
 - Ćwiczenie 6.
- Porządek bajtowy (big- i little-endian) dodatkowe informacje
 - Ćwiczenie 7.
 - Ćwiczenie 8.
 - Ćwiczenie 9.
- Podsumowanie
- Rozdział 5. Transakcje
 - Składniki transakcji
 - Wersja
 - Ćwiczenie 1.
 - Wejścia
 - Przetwarzanie pola ze skryptem
 - Ćwiczenie 2.
 - Wyjścia
 - Ćwiczenie 3.
 - Czas blokady
 - Ćwiczenie 4.
 - Ćwiczenie 5.
 - Kodowanie transakcji
 - Opłata transakcyjna
 - Obliczanie opłaty transakcyjnej
 - Ćwiczenie 6.
 - Podsumowanie

- Rozdział 6. Język Script
 - Zasada działania języka Script
 - Jak działa Script?
 - Przykładowe operacje
 - Programowanie obsługi kodów operacji
 - Ćwiczenie 1.
 - Przetwarzanie pól ze skryptami
 - Programowanie analizatora składniowego i serializatora pól skryptów
 - Scalanie pól ze skryptami
 - Programowanie scalania skryptów
 - Skrypty standardowe
 - p2pk
 - Programowanie interpretera skryptów
 - Elementy stosu pod lupą
 - Ćwiczenie 2.
 - Problemy z p2pk
 - Rozwiązywanie problemów za pomocą p2pkh
 - p2pkh
 - Skrypty mogą być konstruowane dowolnie
 - Ćwiczenie 3.
 - Użyteczność skryptów
 - Ćwiczenie 4.
 - Wyzwanie: znalezienie kolizji SHA-1
 - Podsumowanie
- Rozdział 7. Tworzenie i walidacja transakcji
 - Walidacja transakcji
 - Sprawdzanie wydania wejść
 - Sprawdzanie sumy wejść i sumy wyjść
 - Sprawdzanie podpisu
 - Krok 1.: zerujemy wszystkie skrypty ScriptSig

- Krok 2.: zastępujemy ScriptSig podpisywanego wejścia poprzednim ScriptPubKey
 - Krok 3.: dołączamy typ skrótu
 - Ćwiczenie 1.
 - Ćwiczenie 2.
 - Weryfikacja całej transakcji
 - Tworzenie transakcji
 - Konstruowanie transakcji
 - Tworzenie transakcji
 - Podpisywanie transakcji
 - Ćwiczenie 3.
 - Tworzenie własnych transakcji w testniecie
 - Ćwiczenie 4.
 - Ćwiczenie 5.
 - Podsumowanie
- Rozdział 8. Pay-to-script-hash
 - Czysty multisig
 - Programowanie obsługi OP_CHECKMULTISIG
 - Ćwiczenie 1.
 - Problemy z czystym multisig
 - Pay-to-script-hash (p2sh)
 - Programowanie p2sh
 - Bardziej skomplikowane skrypty
 - Adresy
 - Ćwiczenie 2.
 - Ćwiczenie 3.
 - Weryfikacja podpisów p2sh
 - Krok 1.: zerujemy wszystkie skrypty ScriptSig
 - Krok 2.: zastępujemy ScriptSig podpisywanego wejścia p2sh skryptem RedeemScript
 - Krok 3.: dołączamy typ skrótu
 - Ćwiczenie 4.

- Ćwiczenie 5.
 - Podsumowanie
- Rozdział 9. Bloki
 - Transakcje coinbase
 - Ćwiczenie 1.
 - ScriptSig
 - BIP0034
 - Ćwiczenie 2.
 - Nagłówki bloków
 - Ćwiczenie 3.
 - Ćwiczenie 4.
 - Ćwiczenie 5.
 - Wersja
 - Ćwiczenie 6.
 - Ćwiczenie 7.
 - Ćwiczenie 8.
 - Poprzedni blok
 - Korzeń drzewa skrótów
 - Znacznik czasu
 - Sekwencja bitowa
 - Wartość nonce
 - Dowód pracy
 - W jaki sposób górnik generuje nowe skróty?
 - Cel
 - Ćwiczenie 9.
 - Trudność
 - Ćwiczenie 10.
 - Sprawdzanie dowodu pracy
 - Ćwiczenie 11.
 - Zmiana trudności
 - Ćwiczenie 12.

- Ćwiczenie 13.
 - Podsumowanie
- Rozdział 10. Techniki sieciowe
 - Komunikaty sieciowe
 - Ćwiczenie 1.
 - Ćwiczenie 2.
 - Ćwiczenie 3.
 - Interpretowanie treści komunikatu
 - Ćwiczenie 4.
 - Uzgadnianie komunikacji w sieci
 - Łączenie się z siecią
 - Ćwiczenie 5.
 - Odbieranie nagłówków bloków
 - Ćwiczenie 6.
 - Odpowiedź z nagłówkami
 - Podsumowanie
- Rozdział 11. Uproszczona weryfikacja płatności
 - Motywacja
 - Drzewo skrótów
 - Element nadrzędny
 - Ćwiczenie 1.
 - Poziom nadrzędny drzewa skrótów
 - Ćwiczenie 2.
 - Korzeń drzewa skrótów
 - Ćwiczenie 3.
 - Korzeń drzewa skrótów w blokach
 - Ćwiczenie 4.
 - Korzystanie z drzewa skrótów
 - Blok drzewa skrótów
 - Struktura drzewa skrótów
 - Ćwiczenie 5.

- Programowanie obsługi drzewa skrótów
 - Komunikat sieciowy merkleblock
 - Ćwiczenie 6.
 - Wykorzystanie flag bitowych i skrótów
 - Ćwiczenie 7.
 - Podsumowanie
- Rozdział 12. Filtry Blooma
 - Czym jest filtr Blooma?
 - Ćwiczenie 1.
 - Krok dalej
 - Filtry Blooma według BIP0037
 - Ćwiczenie 2.
 - Ćwiczenie 3.
 - Ładowanie filtra Blooma
 - Ćwiczenie 4.
 - Pobieranie bloków drzewa skrótów
 - Ćwiczenie 5.
 - Pobieranie interesujących nas transakcji
 - Ćwiczenie 6.
 - Podsumowanie
- Rozdział 13. Segwit
 - Pay-to-witness-pubkey-hash (p2wpkh)
 - Kowalność transakcji
 - Eliminowanie kowalności
 - Transakcje p2wpkh
 - p2sh-p2wpkh
 - Programowanie p2wpkh i p2sh-p2wpkh
 - Pay-to-witness-script-hash (p2wsh)
 - p2sh-p2wsh
 - Programowanie p2wsh i p2sh-p2wsh
 - Inne usprawnienia

- Podsumowanie
- Rozdział 14. Tematy zaawansowane i dalsze kroki
 - Proponowane tematy do dalszej nauki
 - Portfele
 - Hierarchiczne portfele deterministyczne
 - Seedy mnemoniczne
 - Kanały płatnicze i sieć Lightning
 - Społeczność
 - Proponowane dalsze projekty
 - Portfel testnetowy
 - Eksplorator bloków
 - Sklep internetowy
 - Biblioteka narzędzi
 - Poszukiwanie pracy
 - Podsumowanie
- Dodatek A Rozwiązania ćwiczeń
 - Rozdział 1. Ciała skończone
 - Ćwiczenie 1.
 - Ćwiczenie 2.
 - Ćwiczenie 3.
 - Ćwiczenie 4.
 - Ćwiczenie 5.
 - Ćwiczenie 6.
 - Ćwiczenie 7.
 - Ćwiczenie 8.
 - Ćwiczenie 9.
 - Rozdział 2. Krzywe eliptyczne
 - Ćwiczenie 1.
 - Ćwiczenie 2.
 - Ćwiczenie 3.
 - Ćwiczenie 4.

- Ćwiczenie 5.
- Ćwiczenie 6.
- Ćwiczenie 7.
- Rozdział 3. Kryptografia krzywych eliptycznych
 - Ćwiczenie 1.
 - Ćwiczenie 2.
 - Ćwiczenie 3.
 - Ćwiczenie 4.
 - Ćwiczenie 5.
 - Ćwiczenie 6.
 - Ćwiczenie 7.
- Rozdział 4. Serializacja
 - Ćwiczenie 1.
 - Ćwiczenie 2.
 - Ćwiczenie 3.
 - Ćwiczenie 4.
 - Ćwiczenie 5.
 - Ćwiczenie 6.
 - Ćwiczenie 7.
 - Ćwiczenie 8.
 - Ćwiczenie 9.
- Rozdział 5. Transakcje
 - Ćwiczenie 1.
 - Ćwiczenie 2.
 - Ćwiczenie 3.
 - Ćwiczenie 4.
 - Ćwiczenie 5.
 - Ćwiczenie 6.
- Rozdział 6. Język Script
 - Ćwiczenie 1.
 - Ćwiczenie 2.

- Ćwiczenie 3.
- Ćwiczenie 4.
- Rozdział 7. Tworzenie i walidacja transakcji
 - Ćwiczenie 1.
 - Ćwiczenie 2.
 - Ćwiczenie 3.
 - Ćwiczenie 4.
 - Ćwiczenie 5.
- Rozdział 8. Pay-to-script-hash
 - Ćwiczenie 1.
 - Ćwiczenie 2.
 - Ćwiczenie 3.
 - Ćwiczenie 4.
 - Ćwiczenie 5.
- Rozdział 9. Bloki
 - Ćwiczenie 1.
 - Ćwiczenie 2.
 - Ćwiczenie 3.
 - Ćwiczenie 4.
 - Ćwiczenie 5.
 - Ćwiczenie 6.
 - Ćwiczenie 7.
 - Ćwiczenie 8.
 - Ćwiczenie 9.
 - Ćwiczenie 10.
 - Ćwiczenie 11.
 - Ćwiczenie 12.
 - Ćwiczenie 13.
- Rozdział 10. Techniki sieciowe
 - Ćwiczenie 1.
 - Ćwiczenie 2.

- Ćwiczenie 3.
- Ćwiczenie 4.
- Ćwiczenie 5.
- Ćwiczenie 6.
- Rozdział 11. Uproszczona weryfikacja płatności
 - Ćwiczenie 1.
 - Ćwiczenie 2.
 - Ćwiczenie 3.
 - Ćwiczenie 4.
 - Ćwiczenie 5.
 - Ćwiczenie 6.
 - Ćwiczenie 7.
- Rozdział 12. Filtry Blooma
 - Ćwiczenie 1.
 - Ćwiczenie 2.
 - Ćwiczenie 3.
 - Ćwiczenie 4.
 - Ćwiczenie 5.
 - Ćwiczenie 6.
 - O autorze
 - Kolofon