

Przedmowa	15
1. Wprowadzenie	27
Historia bitcoina	29
Pierwsze kroki	30
Wybór portfela bitcoina	30
Szybkie wprowadzenie	33
Kody odzyskiwania	33
Adresy bitcoin	34
Otrzymywanie bitcoinów	35
Pozyskiwanie pierwszego bitcoina	35
Określanie aktualnej ceny bitcoinów	36
Przesyłanie i otrzymywanie bitcoinów	37
2. Jak działają bitcoiny?	39
Omówienie bitcoinów	39
Zakup w sklepie internetowym	40
Transakcje w bitcoinach	41
Wejścia i wyjścia w transakcjach	41
Łańcuchy transakcji	42
Wydawanie reszty	43
Wybór monet	44
Typowe formy transakcji	44
Tworzenie transakcji	45
Wybór odpowiednich wejść	45
Generowanie wyjść	46
Dodawanie transakcji do łańcucha bloków	46
Kopanie bitcoinów	47
Wydawanie środków z transakcji	50

3. Bitcoin Core — implementacja wzorcowa	52
Od bitcoina do Bitcoin Core	52
Środowisko programistyczne związane z bitcoinami	54
Budowanie implementacji Bitcoin Core z użyciem kodu źródłowego	54
Wybór wersji implementacji Bitcoin Core	55
Konfigurowanie budowania implementacji Bitcoin Core	55
Budowanie plików wykonywalnych implementacji Bitcoin Core	57
Uruchamianie węzła z implementacją Bitcoin Core	58
Konfigurowanie węzła z implementacją Bitcoin Core	59
Interfejs API oprogramowania Bitcoin Core	63
Pobieranie informacji na temat stanu Bitcoin Core	64
Sprawdzanie i dekodowanie transakcji	65
Badanie bloków	67
Używanie programowego interfejsu oprogramowania Bitcoin Core	68
Inne klienty, biblioteki i pakiety narzędzi	71
C i C++	71
JavaScript	71
Java	71
Python	72
Go	72
Rust	72
Scala	72
C#	72
4. Klucze i adresy	73
Kryptografia z użyciem klucza publicznego	74
Klucze prywatne	75
Objaśnienie kryptografii z użyciem krzywej eliptycznej	76
Klucze publiczne	78
Skrypty wyjściowe i wejściowe	80
Adresy IP: pierwotne adresy bitcoin (P2PK)	81
Tradycyjne adresy na użytek P2PKH	82
Kodowanie Base58Check	84
Skompresowane klucze publiczne	86
Tradycyjne adresy P2SH	89
Adresy Bech32	91
Problemy z adresami bech32	94
Bech32m	94
Formaty kluczy prywatnych	98
Skompresowane klucze prywatne	99
Zaawansowane postacie kluczy i adresów	100
Adresy vanity	100
Portfele papierowe	102

5. Odzyskiwanie portfela	104
Niezależne generowanie kluczy	104
Deterministyczne generowanie kluczy	105
Generowanie publicznego klucza podrzędnego	107
Hierarchiczne deterministyczne (HD) generowanie kluczy (BIP32)	108
Ziarna i kody odzyskiwania	109
Kopie zapasowe danych innych niż klucze	112
Kopie zapasowe ścieżek generowania kluczy	113
Technologie obsługi portfeli	115
Kody odzyskiwania BIP39	116
Tworzenie portfela HD na podstawie ziarna	122
Używanie rozszerzonego klucza publicznego w sklepie internetowym	127
6. Transakcje	132
Zserializowana transakcja bitcoina	132
Wersja	133
Rozszerzony znacznik i flaga	135
Wejścia	135
Długość listy wejść transakcji	135
Punkt wyjścia	137
Skrypt wejściowy	139
Sekwencja	139
Wyjścia	142
Liczba wyjść	142
Kwota	143
Skrypty wyjściowe	144
Struktura poświadczeń	145
Okrężne zależności	146
Plastyczność transakcji powodowana przez strony trzecie	146
Plastyczność transakcji powodowana przez stronę drugą	147
Segregated Witness	148
Serializacja struktury poświadczenia	149
Czas blokady	150
Transakcje coinbase	151
Waga i jednostka vbyte	152
Serializacja tradycyjna	153
7. Autoryzacja i uwierzytelnianie	154
Skrypty transakcji i język Script	154
Niekompletność w sensie Turinga	155
Weryfikacja bezstanowa	155
Tworzenie skryptów	155
Skrypt P2PKH	159

Wielopodpisy skryptowe	159
Transakcje P2SH	163
Adresy P2SH	165
Zalety stosowania P2SH	165
Skrypt wypłaty i sprawdzanie poprawności	166
Wyjścia rejestrujące dane (z operatorem OP_RETURN)	166
Ograniczenia czasu blokady transakcji	167
Weryfikacja blokady czasowej (OP_CLTV)	168
Względne blokady czasowe	170
Względne blokady czasowe z operatorem OP_CLV	170
Skrypty z przepływem sterowania (klauzule warunkowe)	171
Klauzule warunkowe z kodami operacji VERIFY	172
Przepływ sterowania w skryptach	173
Przykładowy złożony skrypt	174
Przykładowe wyjścia i transakcje Segregated Witness	176
Przejście na Segregated Witness	179
MAST (Merkalized Alternative Script Tree)	181
Transakcje P2C (pay to contract)	185
Wielopodpisy bezskryptowe i podpisy progowe	185
Taproot	187
Tapscrip	189
8. Podpisy cyfrowe	190
Jak działają podpisy cyfrowe?	190
Tworzenie podpisu cyfrowego	191
Sprawdzanie poprawności podpisu	191
Typy skrótów podpisów (SIGHASH)	191
Podpisy Schnorra	194
Serializowanie podpisów Schnorra	199
Wielopodpisy bezskryptowe oparte na algorytmie Schnorra	199
Bezskryptowe podpisy progowe oparte na algorytmie Schnorra	201
Podpisy ECDSA	203
Algorytm ECDSA	204
Serializowanie podpisów ECDSA (do formatu DER)	205
Znaczenie losowości w podpisach	205
Nowy algorytm podpisywania w Segregated Witness	206
9. Opłaty transakcyjne	207
Kto uiszcza opłaty transakcyjne?	208
Opłaty i stawki opłat	208
Szacowanie odpowiednich stawek opłat	209
Podwyższanie opłat metodą RBF (Replace By Fee)	210

Podwyższanie opłat metodą CFPF (Child Pays for Parent)	213
Sztafeta pakietów	214
Przygniatanie transakcji	214
Wykrawanie CFPF i wyjścia kotwiczne	216
Dodawanie opłat do transakcji	217
Blokada czasowa jako obrona przed celowaniem w opłaty	217
10. Sieć bitcoina	219
Typy i role węzłów	219
Sieć	220
Przekazywanie bloków kompaktowych	220
Prywatne sieci przekazywania bloków	223
Wykrywanie sieci	224
Kompletne węzły	227
Przesyłanie „zawartości magazynu”	228
Klienci lekkie	229
Filtry Blooma	231
Jak działają filtry Blooma?	232
W jaki sposób klienci lekkie używają filtrów Blooma?	235
Kompaktowe filtry bloków	237
Kodowane zbiory Golomba-Rice'a (GCS)	237
Jakie dane dołącza się do filtra bloków?	239
Pobieranie filtrów bloków od wielu węzłów	240
Ograniczanie zużycia pasma przez kodowanie stratne	240
Używanie kompaktowych filtrów bloków	241
Klienci lekkie a prywatność	242
Połączenia szyfrowane i uwierzytelniane	242
Pule pamięciowe i pule transakcji osieroconych	243
11. Łańcuch bloków	244
Struktura bloku	245
Nagłówek bloku	246
Identyfikatory bloku — skrót nagłówka bloku i wysokość bloku	246
Blok początkowy	247
Łączenie bloków w łańcuchu	248
Drzewa skrótów	249
Drzewa skrótów i klienci lekkie	254
Testowe łańcuchy bloków bitcoina	255
Testnet — poligon doświadczalny bitcoina	255
Signet — testnet z dowodem autorytetu	257
Regtest — lokalny łańcuch bloków	258
Używanie testowych łańcuchów bloków w trakcie prac programistycznych	259

12. Kopanie i konsensus	260
Ekonomia i podaż pieniądza w systemie bitcoina	261
Zdecentralizowane osiągnięcie konsensusu	263
Niezależne sprawdzanie poprawności transakcji	264
Węzły służące do kopania	265
Transakcja coinbase	266
Nagrody i opłaty w transakcji coinbase	266
Struktura transakcji coinbase	267
Dane coinbase	268
Tworzenie nagłówka bloku	269
Wykopywanie bloku	270
Algorytm Proof-of-Work	270
Reprezentacja celu	272
Dostosowywanie trudności przez zmianę celu	273
Mediana przeszłego czasu (MTP)	275
Udane wykopanie bloku	276
Sprawdzanie poprawności nowego bloku	276
Łączenie bloków i wybieranie łańcuchów	277
Kopanie i loteria haszowania	278
Rozwiązanie z użyciem dodatkowej wartości nonce	279
Kopalnie	279
Ataki związane z tempem haszowania	282
Zmienianie reguł osiągnięcia konsensusu	285
Twarde rozgałęzienia	285
Miękkie rozgałęzienia	289
Krytyka miękkich rozgałęzień	289
Rozwój oprogramowania zgodnie z konsensem	295
13. Bezpieczeństwo bitcoina	296
Zasady bezpieczeństwa	296
Bezpieczny rozwój systemów bitcoina	297
Źródło zaufania	298
Dobre praktyki z obszaru zabezpieczeń dla użytkowników	298
Fizyczne przechowywanie bitcoinów	299
Urządzenia podpisujące	300
Gwarantowanie dostępu	300
Dywersyfikacja ryzyka	300
Wielopodpis i zarządzanie	301
Zachowanie dostępu	301

14. Rozwiązania warstwy drugiej	302
Cegielki (podstawowe mechanizmy)	302
Rozwiązania oparte na cegielkach	304
Colored coins	305
Pieczęcie jednokrotnego użytku	305
Płatności na kontrakt (P2C)	306
Sprawdzanie poprawności po stronie klienta	306
RGB	307
Taproot Assets	308
Kanały płatności i kanały stanowe	309
Kanały stanowe — podstawowe zagadnienia i terminologia	309
Prosty przykładowy kanał płatności	310
Tworzenie kanałów niewymagających zaufania	314
Asymetryczne odwoływalne zobowiązania	316
Kontrakty HTLC	320
Kanały płatności z trasowaniem (Lightning Network)	321
Prosty przykład działania sieci Lightning Network	321
Przesył i trasowanie w sieci Lightning Network	324
Korzyści ze stosowania sieci Lightning Network	326
A Artykuł Satoshi'ego Nakamoto na temat bitcoina	329
B Errata do artykułu na temat bitcoina	341
C Dokumenty BIP	347