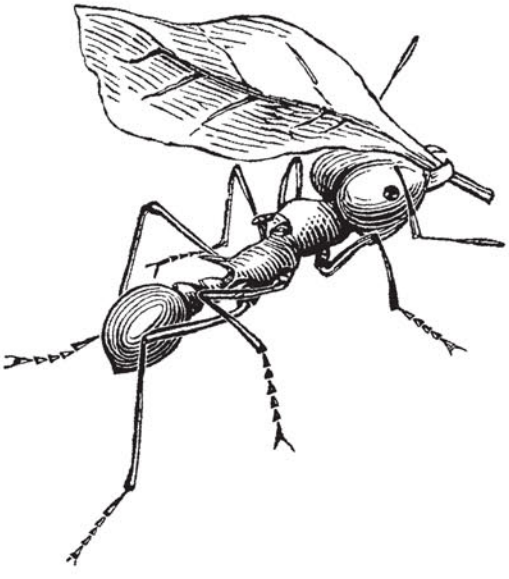
O'REILLY®

Wydanie II

Bitcoin
dla zaawansowanych

PROGRAMOWANIE Z UŻYCIEM
OTWARTEGO ŁAŃCUCHA BLOKÓW



Helion

Andreas M. Antonopoulos

Tytuł oryginału: Mastering Bitcoin: Programming the Open Blockchain

Tłumaczenie: Tomasz Walczak

ISBN: 978-83-283-4035-0

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

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

Pliki z przykładami omawianymi w książce można znaleźć pod adresem:
ftp://ftp.helion.pl/przyklady/bitzaa.zip

Printed in Poland.

Spis treści

Przedmowa **13**

Krótki słowniczek **21**

1. Wprowadzenie **31**
Czym jest bitcoin? 31
Historia bitcoina 33
Zastosowania bitcoina, jego użytkownicy i ich historie 34
Pierwsze kroki 35
Wybór portfela bitcoina 36
Szybkie wprowadzenie 38
Pozyskiwanie pierwszego bitcoina 39
Określanie aktualnej ceny bitcoinów 40
Przesyłanie i otrzymywanie bitcoinów 41

2. Jak działają bitcoiny? **43**
Transakcje, bloki, kopanie i łańcuch bloków 43
Omówienie bitcoinów 43
Zakup kubka kawy 44
Transakcje w bitcoinach 46
Wejścia i wyjścia w transakcjach 46
Łańcuchy transakcji 46
Wydawanie reszty 48
Typowe formy transakcji 48
Tworzenie transakcji 49
Wybór odpowiednich wejść 50
Generowanie wyjść 51
Dodawanie transakcji do księgi 52
Kopanie bitcoinów 53
Kopanie bloków transakcji 54
Wydawanie środków z transakcji 56

3. Bitcoin Core — implementacja wzorcowa 59
Środowisko programistyczne związane z bitcoinami 60
Budowanie implementacji Bitcoin Core z użyciem kodu źródłowego 60
Wybór wersji implementacji Bitcoin Core 61
Konfigurowanie budowania implementacji Bitcoin Core 62
Budowanie plików wykonywalnych implementacji Bitcoin Core 64
Uruchamianie węzła z implementacją Bitcoin Core 65
Pierwsze uruchamianie implementacji Bitcoin Core 66
Konfigurowanie węzła z implementacją Bitcoin Core 66
Interfejs API oprogramowania Bitcoin Core 70
Pobieranie informacji na temat stanu klienta Bitcoin Core 71
Sprawdzanie i dekodowanie transakcji 72
Badanie bloków 73
Używanie programowego interfejsu oprogramowania Bitcoin Core 74
Inne klienty, biblioteki i pakiety narzędzi 77
C i C++ 77
JavaScript 78
Java 78
Python 78
Ruby 78
Go 79
Rust 79
C# 79
Objective-C 79

4. Klucze i adresy 81
Wprowadzenie 81
Kryptografia z użyciem klucza publicznego a kryptowaluty 82
Klucze prywatny i publiczny 83
Klucze prywatne 83
Klucze publiczne 85
Objaśnienie kryptografii z użyciem krzywej eliptycznej 86
Generowanie klucza publicznego 88
Adresy bitcoin 90
Kodowanie Base58 i Base58Check 91
Formaty kluczy 95
Obsługa kluczy i adresów w Pythonie 101
Zaawansowane postacie kluczy i adresów 104
Szyfrowane klucze prywatne (BIP-38) 104
Adresy P2SH i adresy wielopodpisowe 105
Adresy vanity 106
Portfele papierowe 111

5. Portfele 115
Przegląd technologii obsługi portfeli 115
Portfele niedeterministyczne (losowe) 116
Portfele deterministyczne (z ziarnem) 117
Portfele HD (oparte na dokumentach BIP-32 i BIP-44) 117
Ziarna i kody mnemoniczne (BIP-39) 118
Dobre praktyki związane z portfelami 119
Używanie portfela bitcoinów 119
Szczegółowe omówienie technologii używanych w portfelach 121
Mnemoniczne słowa kodowe (BIP-39) 121
Tworzenie portfela HD na podstawie ziarna 126
Używanie rozszerzonego klucza publicznego w sklepie internetowym 132

6. Transakcje 137
Wprowadzenie 137
Szczegółowe omówienie transakcji 137
Transakcje — operacje wykonywane na zapleczu 137
Wyjścia i wejścia transakcji 139
Wyjścia transakcji 140
Wejścia transakcji 142
Opłaty transakcyjne 145
Dodawanie opłat do transakcji 148
Skrypty transakcji i język Script 149
Niekompletność w sensie Turinga 150
Weryfikacja bezstanowa 150
Tworzenie skryptów (blokowanie i odblokowywanie) 150
Skrypt P2PKH 154
Podpisy cyfrowe (ECDSA) 155
Jak działają podpisy cyfrowe? 157
Sprawdzanie poprawności podpisu 158
Typy skrótów podpisów (SIGHASH) 158
Obliczenia w algorytmie ECDSA 160
Znaczenie losowości w podpisach 162
Adresy bitcoin, stan konta i inne abstrakcyjne pojęcia 162

7. Zaawansowane transakcje i skrypty 165
Wprowadzenie 165
Skrypty wielopodpisowe 165
Transakcje P2SH 167
Adresy P2SH 169
Zalety stosowania P2SH 170
Skrypt wypłaty i sprawdzanie poprawności 170

Wyjścia rejestrujące dane (z operatorem RETURN) 171
Blokady oparte na czasie 172
Blokady oparte na czasie na poziomie transakcji (nLocktime) 173
Blokady CLTV 174
Względne blokady oparte na czasie 175
Względne blokady oparte na czasie z użyciem pola nSequence 176
Względne blokady oparte na czasie z operacją CSV 177
Mechanizm Median-Time-Past 178
Zabezpieczanie się przed „celowaniem w opłaty" za pomocą blokad opartych na czasie 179
Skrypty z przepływem sterowania (klauzule warunkowe) 179
Klauzule warunkowe z kodami operacji VERIFY 180
Przepływ sterowania w skryptach 181
Przykładowy złożony skrypt 182

8. Sieć bitcoina ... 185
Architektura sieci P2P 185
Typy i role węzłów 186
Rozszerzona sieć bitcoina 187
Sieć Bitcoin Relay Network 190
Wykrywanie sieci 190
Kompletne węzły 194
Przesyłanie „zawartości magazynu" 194
Węzły SPV 195
Filtry Blooma 198
Jak działają filtry Blooma? 199
W jaki sposób węzły SPV używają filtrów Blooma? 202
Węzły SPV a prywatność 203
Połączenia szyfrowane i uwierzytelniane 204
Transfer za pomocą sieci Tor 204
Uwierzytelnianie i szyfrowanie w sieci P2P 204
Pule transakcji 205

9. Łańcuch bloków ... 207
Wprowadzenie 207
Struktura bloku 208
Nagłówek bloku 209
Identyfikatory bloku — skrót nagłówka bloku i wysokość bloku 209
Blok początkowy 210
Łączenie bloków w ich łańcuchu 211
Drzewa skrótów 212
Drzewa skrótów i węzły SPV 218

Testowe łańcuchy bloków bitcoina 218
Testnet — poligon doświadczalny bitcoina 219
Segnet — testnet z obsługą technologii Segregated Witness 220
Regtest — lokalny łańcuch bloków 221
Używanie testowych łańcuchów bloków w trakcie prac programistycznych 222

10. Kopanie i konsensus 223
Wprowadzenie 223
Ekonomia i podaż pieniądza w systemie bitcoina 224
Zdecentralizowane osiąganie konsensusu 226
Niezależne sprawdzanie poprawności transakcji 227
Węzły służące do kopania 228
Łączenie transakcji w bloki 229
Transakcja coinbase 230
Nagrody i opłaty w transakcji coinbase 231
Struktura transakcji coinbase 232
Dane coinbase 233
Tworzenie nagłówka bloku 235
Wykopywanie bloku 236
Algorytm Proof-of-Work 236
Reprezentacja celu 242
Zmiana celu, aby dostosować trudność 242
Udane wykopanie bloku 244
Sprawdzanie poprawności nowego bloku 245
Łączenie bloków i wybieranie łańcuchów 246
Rozgałęzienia łańcucha bloków 247
Kopanie i wyścig w obliczaniu skrótów 254
Rozwiązanie z użyciem dodatkowej wartości nonce 256
Kopalnie 256
Ataki związane z konsensusem 260
Zmienianie reguł osiągania konsensusu 263
Twarde rozgałęzienia 263
Twarde rozgałęzienia: oprogramowanie, sieć, kopanie i łańcuch 264
Podział górników na grupy a poziom trudności 265
Kontrowersyjne twarde rozgałęzienia 266
Miękkie rozgałęzienia 267
Krytyka miękkich rozgałęzień 268
Sygnalizowanie miękkich rozgałęzień za pomocą wersji bloku 269
Sygnalizowanie i aktywowanie zmian w specyfikacji BIP-34 269
Sygnalizowanie i aktywowanie zmian w specyfikacji BIP-9 270
Rozwój oprogramowania zgodnie z konsensusem 272

11. Bezpieczeństwo bitcoina 273
Reguły bezpieczeństwa 273
Bezpieczny rozwój systemów bitcoina 274
Źródło zaufania 275
Dobre praktyki z obszaru zabezpieczeń dla użytkowników 276
Fizyczne przechowywanie bitcoinów 276
Portfele sprzętowe 277
Równoważenie ryzyka 277
Dywersyfikacja ryzyka 277
Wielopodpis i zarządzanie 278
Zachowanie dostępu 278
Wnioski 278

12. Rozwiązania związane z łańcuchem bloków 279
Wprowadzenie 279
Cegiełki (podstawowe mechanizmy) 279
Rozwiązania oparte na cegiełkach 282
Colored coins 282
Używanie colored coins 283
Emisja colored coins 283
Transakcje z użyciem colored coins 284
Counterparty 287
Kanały płatności i kanały stanowe 287
Kanały stanowe — podstawowe zagadnienia i terminologia 288
Prosty przykładowy kanał płatności 290
Tworzenie kanałów niewymagających zaufania 292
Asymetryczne odwoływalne zobowiązania 295
Kontrakty HTLC 298
Kanały płatności z trasowaniem (Lightning Network) 299
Prosty przykład działania sieci Lightning Network 300
Przesył i trasowanie w sieci Lightning Network 303
Korzyści ze stosowania sieci Lightning Network 304
Wnioski 305

A Artykuł Satoshiego Nakamoty na temat bitcoina 307

B Operatory, stałe i symbole języka skryptowego transakcji 319

C Dokumenty BIP 325

D Mechanizm Segregated Witness 331

E Bitcore 343

F Biblioteki pycoin oraz narzędzia ku i tx 347

G Polecenia z narzędzia Bitcoin Explorer (bx) 355

Skorowidz 359

ROZDZIAŁ 1.

Wprowadzenie

Czym jest bitcoin?

Bitcoin to zbiór koncepcji i technologii stanowiących podstawę ekosystemu pieniądza cyfrowego. Jednostki tej waluty, nazywane bitcoinami, służą do przechowywania i przesyłania środków o określonej wartości między uczestnikami sieci bitcoina. Użytkownicy tej sieci komunikują się między sobą (za pomocą protokołu bitcoina) przede wszystkim przez internet, choć używane mogą być także inne sieci. Zestaw protokołów bitcoina, rozpowszechniony jako oprogramowanie o otwartym dostępie do kodu źródłowego, może działać w różnorodnych urządzeniach obliczeniowych, w tym w laptopach i smartfonach, dzięki czemu technologia ta jest łatwo osiągalna.

Użytkownicy mogą przesyłać bitcoiny w sieci, aby wykonywać niemal dowolne operacje, jakie są możliwe z wykorzystaniem tradycyjnych walut. Mogą m.in. kupować i sprzedawać produkty, przesyłać pieniądze ludziom i organizacjom lub udzielać kredytów. Bitcoiny można kupować, sprzedawać i wymieniać na inne waluty w specjalnych kantorach. Bitcoin jest w pewnym sensie doskonałą walutą dla internetu, ponieważ korzystanie z niego odbywa się szybko, bezpiecznie i bez uwzględniania granic.

W odróżnieniu od tradycyjnych walut bitcoiny są w pełni wirtualne. Nie występują fizyczne ani nawet cyfrowe monety w tej walucie. Istnienie monet wynika z transakcji, w których wartość jest przekazywana od nadawcy do odbiorcy. Użytkownicy bitcoinów uzyskują klucze, które pozwalają udowodnić posiadanie bitcoinów w ich sieci. Za pomocą tych kluczy można podpisywać transakcje, aby odblokować wartość i wydać ją, przekazując środki nowemu właścicielowi. Klucze są często przechowywane w cyfrowym portfelu na komputerze lub smartfonie użytkownika. Posiadanie klucza, którym można podpisać transakcję, to jedyny warunek do wydawania bitcoinów, dzięki czemu całkowita kontrola nad środkami pozostaje w rękach każdego użytkownika.

Bitcoiny działają w rozproszonym systemie typu P2P. Dlatego nie istnieje centralny serwer ani punkt kontroli. Bitcoiny są generowane w procesie kopania (ang. *mining*), co polega na konkurowaniu w wyszukiwaniu rozwiązania problemu matematycznego związanego z przetwarzaniem transakcji z użyciem bitcoinów. Każdy uczestnik sieci bitcoinów (czyli każdy użytkownik urządzenia, na którym działa pełny zestaw protokołów bitcoina) może zostać górnikiem, wykorzystując moc obliczeniową komputera do sprawdzania i rejestrowania transakcji. Średnio co 10 minut komuś udaje się potwierdzić transakcje z ostatnich 10 minut, za co dana osoba jest wynagradzana

nowymi bitcoinami. Kopanie bitcoinów prowadzi do decentralizacji działań związanych z emisją waluty i rozliczeniami oraz eliminuje konieczność istnienia banku centralnego.

Protokół bitcoina obejmuje wbudowane algorytmy regulujące przebieg kopania w sieci. Trudność zadań obliczeniowych, jakie górnicy muszą wykonywać, jest dostosowywana dynamicznie. Dlatego jakiś górnik odnosi sukces średnio co 10 minut, niezależnie od tego, ile osób konkuruje ze sobą w danym momencie i ile mocy obliczeniowej jest w to zaangażowane. Protokół zmniejsza też szybkość emisji nowych bitcoinów co cztery lata oraz ogranicza łączną liczbę bitcoinów, jakie zostaną wyemitowane, do stałej wartości wynoszącej niecałe 21 milionów. Dlatego liczba bitcoinów w obiegu ściśle odpowiada przewidywalnej krzywej i do roku 2140 wyniesie blisko 21 milionów. Ponieważ szybkość emisji bitcoinów stale spada, w długim terminie bitcoin jest walutą deflacyjną. Ponadto nie jest możliwa inflacja spowodowana „dodrukiem" nowych pieniędzy ponad poziom oczekiwanej szybkości emisji.

Nazwa „bitcoin" oznacza też protokół, sieć P2P i innowacyjną technologię przetwarzania rozproszonego. Waluta bitcoin to tylko pierwsze zastosowanie tej innowacji. Bitcoin to punkt kulminacyjny dziesięcioleci badań z dziedziny kryptografii i systemów rozproszonych, łączący cztery ważne innowacje w unikatowy i wartościowy sposób. Oto elementy tworzące bitcoina:

- zdecentralizowana sieć P2P (oparta na protokole bitcoina),
- publiczna księga transakcji (łańcuch bloków),
- zestaw reguł służący do niezależnej walidacji transakcji i emisji waluty (są to reguły oparte na konsensusie),
- mechanizm osiągania w środowisku zdecentralizowanym globalnego konsensusu dotyczącego poprawnego łańcucha bloków (algorytm Proof-of-Work).

Ponieważ jestem programistą, traktuję bitcoin jako walutę internetową i jako sieć przekazywania wartości oraz zabezpieczania własności środków cyfrowych za pomocą obliczeń rozproszonych. Jednak bitcoin to coś znacznie więcej, niż może się początkowo wydawać.

Ten rozdział rozpoczynam od objaśnienia wybranych podstawowych koncepcji i pojęć, ponadto omawiam pobieranie niezbędnego oprogramowania oraz opisuję używanie bitcoinów w prostych transakcjach. W dalszych rozdziałach wyjaśniam warstwy technologii, dzięki którym bitcoiny mogły powstać, i analizuję wewnętrzne mechanizmy sieci i protokołu bitcoina.

Waluty cyfrowe przed pojawieniem się bitcoinów

Powstanie wiarygodnych pieniędzy cyfrowych jest ściśle powiązane z osiągnięciami z obszaru kryptografii. Nie jest to zaskoczeniem, jeśli uwzględnić wyzwania związane z używaniem bitów do reprezentowania wartości, którą można wymieniać na towary i usługi. Oto trzy podstawowe pytania każdej osoby akceptującej pieniądze cyfrowe:

1. Czy mogę zaufać, że pieniądze są autentyczne (a nie podrobione)?
2. Czy mogę mieć pewność, że pieniądze cyfrowe mogą zostać wydane tylko raz (jest to problem podwójnego wydatkowania; ang. *double-spending*)?
3. Czy mogę mieć pewność, że nikt inny nie stwierdzi, iż pieniądze należą do niego, a nie do mnie?

Emitenci pieniędzy papierowych nieustannie walczą z fałszerzami, używając coraz bardziej zaawansowanych materiałów i technologii druku. Pieniądze fizyczne łatwo rozwiązują problem podwójnego wydatkowania, ponieważ ten sam banknot nie może znajdować się jednocześnie w dwóch miejscach. Oczywiście — tradycyjne pieniądze często są przechowywane i przekazywane cyfrowo. Wtedy problemy fałszerstw i podwójnego wydatkowania są rozwiązywane dzięki rozliczaniu wszystkich transakcji elektronicznych przez jednostki centralne, mające globalny wgląd w pieniądze będące w obiegu. W przypadku pieniędzy cyfrowych, gdzie nie można wykorzystać wyrafinowanych tuszów lub pasków holograficznych, to kryptografia pozwala zaufać w zasadność roszczeń użytkownika do środków. Konkretnie chodzi o to, że podpisy cyfrowe umożliwiają użytkownikowi podpisywanie środków lub transakcji cyfrowych i udowodnienie posiadania danych środków. Dzięki odpowiedniej architekturze podpisy cyfrowe pozwalają też rozwiązać problem podwójnego wydatkowania.

Gdy pod koniec lat 80. kryptografia stała się bardziej dostępna i zrozumiała, wielu naukowców zaczęło próbować wykorzystać ją do utworzenia walut cyfrowych. W tych wczesnych projektach emitowane były pieniądze cyfrowe oparte zwykle na walutach krajowych lub metalach wartościowych (np. na złocie).

Choć te dawne waluty cyfrowe funkcjonowały poprawnie, były scentralizowane i z tego powodu podatne na ataki ze strony rządów i hakerów. Dla wczesnych walut cyfrowych działała centralna jednostka rozrachunkowa zatwierdzająca w regularnych odstępach czasu wszystkie transakcje (podobnie jak w tradycyjnym systemie bankowym). Niestety w większości sytuacji te nowe waluty cyfrowe stawały się obiektem ataków zaniepokojonych rządów i ostatecznie wychodziły z użycia. Niektóre próby kończyły się spektakularnymi katastrofami, np. gdy spółka nadrzędna była nagle likwidowana. Aby zapewnić odporność na interwencje ze strony przeciwników (czy to rządów, czy to organizacji przestępczych), potrzebna była *zdecentralizowana* waluta cyfrowa, pozwalająca uniknąć powstania jednego punktu podatnego na ataki. Takim systemem jest bitcoin, z natury zdecentralizowany i wolny od centralnej jednostki nadrzędnej, którą można by zaatakować lub złamać.

Historia bitcoina

Bitcoin został wymyślony w 2008 roku w wyniku publikacji artykułu *Bitcoin: A Peer-to-Peer Electronic Cash System*[1] napisanego pod pseudonimem Satoshi Nakamoto (zob. dodatek A). Nakamoto połączył kilka wcześniejszych wynalazków (takich jak protokół b-money i algorytm HashCash), aby zbudować w pełni zdecentralizowany system pieniędzy elektronicznych, który nie jest zależny od jednostki centralnej w zakresie emisji pieniędzy lub zatwierdzania i walidacji transakcji. Najważniejszą innowacją było wykorzystanie rozproszonego systemu obliczeniowego (nazwanego algorytmem Proof-of-Work) do przeprowadzania co 10 minut globalnych „wyborów", co umożliwiało zdecentralizowanej sieci osiągnięcie *konsensusu* w kwestii stanu transakcji. Ten model w elegancki sposób rozwiązuje problem podwójnego wydatkowania (polegający na tym, że jednostkę waluty można wydać dwukrotnie). Wcześniej było to słabością waluty cyfrowej, obchodzoną przez rozliczanie wszystkich transakcji za pośrednictwem centralnej jednostki rozliczeniowej.

Sieć bitcoin powstała w 2009 roku na podstawie opublikowanej przez Nakamoto wzorcowej implementacji, poprawianej później przez wielu innych programistów. Moc obliczeniowa dostępna dla algorytmu Proof-of-Work (związanego z kopaniem), który zapewnia bezpieczeństwo i odporność

[1] *Bitcoin: A Peer-to-Peer Electronic Cash System*, Satoshi Nakamoto (*https://bitcoin.org/bitcoin.pdf*).

bitcoina na ataki, wzrosła wykładniczo i obecnie przekracza łączną moc obliczeniową najszybszych superkomputerów świata. Wartość rynkowa bitcoinów okresowo przekraczała 20 mld dolarów (zależy to od kursu wymiany bitcoinów na dolary). Największa z dotychczas przetwarzanych w sieci transakcji była warta 150 mln dolarów, które zostały przesłane natychmiastowo i rozliczone bez żadnych opłat.

Satoshi Nakamoto wycofał się z życia publicznego w kwietniu 2011 roku, przekazując aktywnej grupie wolontariuszy odpowiedzialność za rozwijanie kodu i sieci. Tożsamość osoby lub osób stojących za bitcoinem jest do tej pory nieznana. Jednak ani Satoshi Nakamoto, ani nikt inny nie sprawuje jednostkowej kontroli nad systemem bitcoina. System ten działa na podstawie w pełni jawnych reguł matematycznych, oprogramowania o otwartym dostępie do kodu źródłowego i konsensusu między użytkownikami sieci. Samo powstanie bitcoina jest przełomowym osiągnięciem, które doprowadziło do powstania nowego obszaru nauki w dziedzinach obliczeń rozproszonych, ekonomii i ekonometrii.

Rozwiązanie problemu obliczeń rozproszonych

Pomysł Sathoshiego Nakamoty jest praktycznym i nowatorskim rozwiązaniem problemu obliczeń rozproszonych, znanego jako problem bizantyjskich generałów. Dotyczy on próby uzgodnienia działań lub stanu systemu przez wymianę informacji w zawodnej i podatnej na ataki sieci. Rozwiązanie Nakamoty, który wykorzystał dowód pracy (ang. *Proof-of-Work*) do uzgadniania konsensusu *bez centralnej zaufanej jednostki*, stanowi przełom w obliczeniach rozproszonych i ma wiele zastosowań niezwiązanych z walutami. Można się nim posługiwać do osiągania konsensusu w zdecentralizowanych sieciach, aby zapewniać wiarygodność wyborów, loterii, rejestrów środków, poświadczeń cyfrowych itd.

Zastosowania bitcoina, jego użytkownicy i ich historie

Bitcoin to prawdziwa innowacja, jeśli chodzi o technologię pieniądza. W swej istocie pieniądze ułatwiają wymianę wartości między ludźmi. Dlatego aby w pełni zrozumieć bitcoina i jego zastosowania, przeanalizuję go z perspektywy użytkowników tej waluty. Wszystkie wymienione tu osoby i ich historie ilustrują konkretny przypadek użycia (lub kilka takich przypadków). Te historie będą się w książce powtarzać.

Handel produktami o małej wartości w Ameryce Północnej

Alice mieszka w regionie Bay Area w północnej Kalifornii. Usłyszała o bitcoinie od zainteresowanego technologiami znajomego i chce zacząć korzystać z tej waluty. Zobaczysz, jak Alice poznaje bitcoiny, kupuje je, a następnie wydaje w celu zakupu kubka kawy w kawiarni Bob's Cafe w Palo Alto. W ramach tej historii poznasz oprogramowanie, kantory i podstawowe transakcje z perspektywy klienta sklepu.

Handel produktami o dużej wartości w Ameryce Północnej

Carol jest właścicielką galerii w San Francisco. Sprzedaje drogie obrazy za bitcoiny. W tej historii poznasz zagrożenie atakiem przez konsensus na poziomie 51%, wymierzonym w sprzedawców drogich towarów.

Kontrakty zagraniczne

Robert, właściciel kawiarni w Palo Alto, tworzy nową witrynę. Zatrudnił indyjskiego programistę stron internetowych Gopesha, który mieszka w Bangalore w Indiach. Gopesh zgodził się na zapłatę w bitcoinach. W tej historii zapoznasz się z używaniem bitcoinów w kontekście outsourcingu, usług kontraktowych i przelewów międzynarodowych.

Sklep internetowy

Gabriel jest przedsiębiorczym nastolatkiem z Rio de Janeiro prowadzącym mały sklep internetowy, w którym sprzedaje koszulki, kubki i naklejki z rysunkami bitcoinów. Gabriel jest zbyt młody, by posiadać konto w banku, ale jego rodzice zachęcają go do przedsiębiorczości.

Datki na organizacje charytatywne

Eugenia jest dyrektorem filipińskiej instytucji charytatywnej działającej na rzecz dzieci. Niedawno odkryła bitcoiny i chce używać ich, aby dotrzeć do nowej grupy zagranicznych i lokalnych sponsorów. Interesuje się też możliwością wykorzystania bitcoinów do szybkiego przesyłania środków w miejsca, gdzie są one potrzebne. W tej historii zobaczysz, jak wykorzystać bitcoiny do globalnych zbiórek niezależnych od walut i granic oraz jak dzięki ogólnie dostępnej księdze zapewnić przejrzystość działań organizacji charytatywnych.

Import i eksport

Mohammed jest importerem elektroniki z Dubaju. Chce wykorzystać bitcoiny do zakupu elektroniki ze Stanów Zjednoczonych i Chin oraz importowania towarów do Zjednoczonych Emiratów Arabskich, aby przyspieszyć proces płatności za importowane dobra. W tej historii zobaczysz, w jaki sposób bitcoiny mogą być używane do dokonywania dużych międzynarodowych płatności za fizyczne towary w handlu B2B.

Kopanie bitcoinów

Jing studiuje inżynierię komputerową w Szanghaju. Jing, wykorzystując umiejętności inżynieryjne, zbudował platformę do kopania bitcoinów, aby zapewniała mu dodatkowy dochód. W tej historii poznasz „przemysłowe" podstawy bitcoina — wyspecjalizowany sprzęt służący do zabezpieczania sieci bitcoina i generowania nowych pieniędzy.

Każda z tych historii jest oparta na rzeczywistych ludziach i branżach, które obecnie używają bitcoinów do tworzenia nowych rynków, nowych przemysłów i innowacyjnych rozwiązań globalnych problemów ekonomicznych.

Pierwsze kroki

Bitcoin to protokół, który może być używany poprzez obsługującą go aplikację kliencką. Portfel bitcoina to najczęściej używany interfejs systemu bitcoina (podobnie jak przeglądarka to najczęściej stosowany interfejs dla protokołu HTTP). Istnieje wiele implementacji i rodzajów takich portfeli, podobnie jak jest wiele rodzajów przeglądarek (np. Chrome, Safari, Firefox i Internet Explorer). I podobnie jak każdy ma ulubione (Mozilla Firefox, super!) i nielubiane przeglądarki (Internet Explorer, fe!), tak portfele bitcoina różnią się ze względu na jakość, wydajność, bezpieczeństwo, prywatność i niezawodność. Istnieje też wzorcowa implementacja protokołu bitcoina obejmująca portfel. Jej nazwa to Satoshi Client lub Bitcoin Core, a implementacja ta jest oparta na pierwotnym rozwiązaniu napisanym przez Satoshiego Nakamotę.

Wybór portfela bitcoina

Portfele to jedne z najaktywniej rozwijanych aplikacji w ekosystemie bitcoina. W tym obszarze panuje duża konkurencja i choć prawdopodobnie właśnie tworzony jest nowy portfel, niektóre tego typu narzędzia z zeszłego roku nie są już rozwijane. Wiele portfeli jest przeznaczonych dla konkretnych platform lub zastosowań. Niektóre są lepiej dostosowane do początkujących, natomiast inne udostępniają wiele funkcji dla zaawansowanych użytkowników. Wybór portfela to wysoce subiektywna kwestia, zależna od planowanego zastosowania i doświadczenia. Dlatego nie da się polecić konkretnej marki lub projektu portfela. Można jednak skategoryzować portfele według platform i funkcji oraz w przejrzysty sposób przedstawić ich różne typy. Co lepsze, przenoszenie pieniędzy między portfelami jest łatwe, tanie i szybkie, dlatego warto wypróbować kilka takich narzędzi w celu znalezienia tego, które spełnia Twoje potrzeby.

Portfele według platform można skategoryzować w następujący sposób:

Portfele desktopowe

Portfel desktopowy był pierwszym typem portfela opracowanym jako implementacja wzorcowa. Wielu użytkowników korzysta z takich portfeli z powodu funkcji, jakie oferuje, autonomii i kontroli. Używanie systemów operacyjnych ogólnego użytku, takich jak Windows i Mac OS, ma jednak wady związane z bezpieczeństwem, ponieważ systemy te są często niezabezpieczone i źle skonfigurowane.

Portfele mobilne

Portfele mobilne są najpopularniejszym typem tego rodzaju narzędzi. Działają w systemach operacyjnych smartfonów (np. Apple iOS lub Android) i często stanowią doskonały wybór dla nowych użytkowników. Wiele takich portfeli jest projektowanych pod kątem prostoty i łatwości użycia, jednak istnieją też bogate w funkcje portfele mobilne dla zaawansowanych użytkowników.

Portfele internetowe

Portfele internetowe są dostępne z poziomu przeglądarki i przechowują portfel użytkownika na niezależnym serwerze, co upodabnia je do systemów poczty elektronicznej. W niektórych usługach tego typu stosowany jest kod kliencki działający w przeglądarce użytkownika. Ten kod kontroluje klucze bitcoina należące do użytkownika. Jednak w większości takich portfeli działa kompromisowe rozwiązanie — narzędzie przejmuje kontrolę nad należącymi do użytkownika kluczami bitcoina w zamian za łatwość użytkowania portfela. Przechowywanie bitcoinów o dużej wartości w systemach niezależnych firm nie jest zalecane.

Portfele sprzętowe

Portfele sprzętowe to urządzenia obsługujące bezpieczny, niezależny portfel za pomocą wyspecjalizowanego sprzętu. Takie portfele działają z użyciem portu USB i przeglądarki desktopowej lub komunikacji NFC i urządzeń mobilnych. Dzięki obsłudze wszystkich operacji związanych z bitcoinami za pomocą wyspecjalizowanego sprzętu te portfele są uznawane za bardzo bezpieczne i nadają się do przechowywania bitcoinów o dużej wartości.

Portfele papierowe

Klucze kontrolujące bitcoiny można też wydrukować na potrzeby ich długoterminowego przechowywania. Są to tak zwane portfele papierowe, choć czasem używane są inne materiały (drewno, metal itd.). Portfele papierowe to prosty technologicznie, ale bardzo bezpieczny sposób długoterminowego przechowywania bitcoinów. Przechowywanie bitcoinów w trybie offline jest też czasem nazywane składowaniem „w chłodni".

Inny sposób kategoryzowania portfeli bitcoina opiera się na poziomie autonomii i sposobie interakcji z siecią bitcoina:

Kompletny klient

Kompletny klient charakteryzuje się przechowywaniem całej historii transakcji (wszystkich transakcji przeprowadzonych kiedykolwiek przez dowolnego użytkownika), zarządzaniem portfelami i możliwością bezpośredniego inicjowania transakcji w sieci bitcoina. Kompletny klient obsługuje wszystkie aspekty protokołu oraz może niezależnie przeprowadzać walidację całego łańcucha bloków i dowolnych transakcji. Taki klient zużywa dużo zasobów komputera (np. ponad 125 GB miejsca na dysku i 2 GB pamięci RAM), ale zapewnia całkowitą autonomię i niezależne weryfikowanie transakcji.

Prosty klient

Prosty klient, nazywany też klientem **SPV** (ang. *Simple Payment Verification*), łączy się z opisanymi wcześniej kompletnymi klientami, aby uzyskać informacje o transakcjach, jednak przechowuje portfel użytkownika lokalnie i niezależnie tworzy transakcje, sprawdza ich poprawność i przesyła je. Proste klienty bezpośrednio komunikują się z siecią bitcoina (nie korzystają z pośredników).

Klient z niezależnym interfejsem API

Taki klient komunikuje się z siecią bitcoina za pomocą systemu niezależnych interfejsów API, a nie bezpośrednio. Portfel może być wtedy przechowywany u użytkownika lub na niezależnych serwerach, przy czym wszystkie transakcje odbywają się z udziałem niezależnego pośrednika.

Uwzględniając oba sposoby kategoryzowania, wiele portfeli można przypisać do kilku grup. Najczęściej spotykane kategorie to pełny klient desktopowy, prosty portfel mobilny i portfel internetowy z niezależnym interfejsem. Granice między kategoriami często się zacierają, ponieważ wiele portfeli działa na różnych platformach i może komunikować się z siecią w rozmaity sposób.

Na potrzeby tej książki przedstawiam używanie różnych dostępnych do pobrania klientów bitcoina — od implementacji wzorcowej (Bitcoin Core) po portfele mobilne i internetowe. Niektóre przykłady wymagają użycia narzędzia Bitcoin Core, który oprócz tego, że jest kompletnym klientem, udostępnia interfejsy API do usług związanych z portfelem, siecią i transakcjami. Jeśli planujesz zapoznać się z interfejsami programowymi systemu bitcoina, będziesz potrzebował narzędzia Bitcoin Core lub jednego z innych klientów (zob. punkt „Inne klienty, biblioteki i pakiety narzędzi").

Szybkie wprowadzenie

Alice, którą poznałeś w punkcie „Zastosowania bitcoina, jego użytkownicy i ich historie", nie ma wiedzy technicznej i dopiero niedawno dowiedziała się o bitcoinach od swojego przyjaciela Joego. Na przyjęciu Joe entuzjastycznie objaśnia działanie bitcoinów wszystkim osobom i demonstruje, jak posługiwać się tą walutą. Alice zaintrygowana pyta, jak może zacząć korzystać z bitcoinów. Joe wyjaśnia, że dla początkujących najlepszy jest portfel mobilny i poleca kilka swoich ulubionych narzędzi tego typu. Alice pobiera narzędzie Mycelium na Androida i instaluje je w telefonie.

Gdy Alice pierwszy raz uruchamia Mycelium, narzędzie to (podobnie jak wiele portfeli bitcoinów) automatycznie tworzy nowy portfel. Alice widzi ten portfel na ekranie, co przedstawia rysunek 1.1 (uwaga: *nie* przesyłaj bitcoinów pod ten przykładowy adres, ponieważ zostaną one na zawsze utracone).

Rysunek 1.1. Portfel mobilny Mycelium

Najważniejszą informacją na tym ekranie jest *adres bitcoin* należący do Alice. Na ekranie ma on postać długiego łańcucha liter i cyfr: `1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK`. Obok tego adresu znajduje się kod QR. Jest to odmiana kodu kreskowego zawierającego te same informacje w formacie możliwym do zeskanowania za pomocą aparatu smartfona. Kod QR to kwadrat ze wzorem z czarnych i białych kropek. Alice może skopiować adres bitcoin lub kod QR do schowka, dotykając kod QR lub przycisk *Receive*. W większości portfeli dotknięcie kodu QR powoduje też powiększenie go, dzięki czemu można go łatwiej zeskanować za pomocą aparatu smartfona.

Adresy bitcoin rozpoczynają się od cyfry 1 lub 3. Podobnie jak adresy e-mail mogą być one udostępniane innym użytkownikom, którzy mogą za pomocą tych adresów przesyłać bitcoiny bezpośrednio do portfela odbiorcy. W kontekście bezpieczeństwa w adresach bitcoin nie ma żadnych poufnych danych. Adres ten możesz zamieścić w dowolnym miejscu, nie narażając konta na niebezpieczeństwo. W odróżnieniu od adresów e-mail możesz tworzyć nowe adresy bitcoin tak często, jak masz na to ochotę, a wszystkie te adresy spowodują przesyłanie środków do Twojego portfela. Wiele niedawno powstałych portfeli automatycznie tworzy nowy adres dla każdej transakcji, aby zmaksymalizować prywatność. Portfel to zbiór adresów i kluczy odblokowujących dostępne środki.

Alice może teraz zacząć otrzymywać środki. Jej portfel losowo generuje klucz prywatny (opisany szczegółowo w punkcie „Klucze prywatne") wraz z powiązanym adresem bitcoin. Na tym etapie adres bitcoin nie jest znany w sieci bitcoina ani zarejestrowany w systemie bitcoina. Ten adres to liczba powiązana z kluczem, za pomocą którego Alice kontroluje dostęp do środków. Adres jest generowany niezależnie przez portfel bez powiadamiania o tym innych usług ani rejestrowania się w nich. W większości portfeli nie istnieje związek między adresem bitcoin a zewnętrznie identyfikowalnymi informacjami na temat tożsamości użytkownika. Do momentu, w którym adres jest wskazywany jako odbiorca wartości w transakcji w księdze, jest on tylko jednym z wielu możliwych poprawnych adresów w świecie bitcoina. Dopiero po powiązaniu adresu z transakcją staje się on jednym ze znanych adresów w sieci.

Alice może teraz zacząć korzystać z nowego portfela.

Pozyskiwanie pierwszego bitcoina

Pierwszym i często najtrudniejszym zadaniem dla nowych użytkowników jest pozyskanie bitcoinów. W odróżnieniu od innych walut obcych nie da się na razie kupić bitcoinów w banku lub kantorze.

Transakcje z użyciem bitcoinów są nieodwracalne. Większość transakcji w sieciach obsługujących płatności elektroniczne, np. przy użyciu kart kredytowych, kart debetowych, systemu PayPal i kont bankowych, jest odwracalna. To stanowi dla sprzedawcy bitcoinów wysokie ryzyko: kupujący może wycofać płatność elektroniczną po otrzymaniu bitcoinów, w ten sposób oszukując sprzedawcę. Aby ograniczyć to ryzyko, firmy pozwalające kupować bitcoiny przy użyciu tradycyjnych płatności elektronicznych zwykle sprawdzają tożsamość kupującego i jego wiarygodność kredytową, co może zająć kilka dni lub tygodni. Dla nowego użytkownika oznacza to, że nie może on od razu zakupić bitcoinów za pomocą karty kredytowej. Jednak odrobina cierpliwości i twórczego myślenia pozwalają rozwiązać ten problem.

Oto kilka metod na pozyskanie bitcoinów przez nowych użytkowników:

- Znajdź znajomego, który posiada bitcoiny, i zakup je bezpośrednio od niego. Wielu użytkowników bitcoinów zaczyna w ten sposób. Jest to najmniej skomplikowany sposób. Jednym ze sposobów na spotkanie właścicieli bitcoinów jest udział w lokalnych spotkaniach meetupowych ogłaszanych w serwisie Meetup.com[2].

[2] *https://www.meetup.com/*.

- Posłuż się katalogiem takim jak localbitcoins.com[3], aby znaleźć sprzedawcę w swojej okolicy w celu osobistego zakupu bitcoinów za gotówkę.
- Zarób bitcoiny, sprzedając za nie produkty lub usługi. Jeśli jesteś programistą, możesz sprzedać swoje umiejętności programistyczne. Jeżeli jesteś fryzjerem, możesz kogoś uczesać za bitcoiny.
- Użyj bankomatu z bitcoinami w swoim mieście. Takie bankomaty to maszyny, które przyjmują gotówkę i przesyłają bitcoiny do portfela bitcoinów na smartfonie. Poszukaj takiej maszyny za pomocą mapy internetowej ze strony Coin ATM Radar[4].
- Posłuż się wymieniającym bitcoiny kantorem powiązanym z Twoim rachunkiem bankowym. Obecnie w wielu państwach dostępne są kantory, które umożliwiają sprzedającym i kupującym wymianę bitcoinów na lokalną walutę. W serwisach wyświetlających kursy wymiany (np. w serwisie BitcoinAverage[5]) często dostępne są listy kantorów dla poszczególnych walut.

Jedną z zalet bitcoinów, w porównaniu z innymi systemami płatności, jest to, że odpowiednio używane zapewniają użytkownikom znacznie więcej prywatności. Pozyskiwanie, przechowywanie i wydawanie bitcoinów nie wymaga ujawniania poufnych informacji i danych osobowych osobom trzecim. Jednak tam, gdzie bitcoiny stykają się z tradycyjnymi systemami (np. w kantorach), często obowiązują regulacje krajowe i międzynarodowe. Aby wymienić bitcoiny na walutę krajową, często trzeba przedstawić dowód tożsamości i informacje z banku. Użytkownicy powinni wiedzieć, że po powiązaniu adresu bitcoin z danymi osobowymi wszystkie transakcje z użyciem tego adresu łatwo można zidentyfikować i prześledzić. Jest to jeden z powodów, dla których wielu użytkowników decyduje się utrzymywać specjalne konta do wymiany walut niepowiązane ze swoimi portfelami.

Alice zapoznała się z bitcoinami dzięki przyjacielowi, dlatego może w łatwy sposób pozyskać swoje pierwsze bitcoiny. Zobacz teraz, w jaki sposób Alice może kupić bitcoiny od swojego przyjaciela Joego i jak Joe może przesłać środki do portfela przyjaciółki.

Określanie aktualnej ceny bitcoinów

Zanim Alice kupi bitcoiny od Joego, osoby te muszą uzgodnić *kurs wymiany* bitcoinów na dolary amerykańskie. Pojawia się wtedy pytanie często zadawane przez osoby dopiero zapoznające się z bitcoinami: „Kto ustala cenę bitcoinów?". Krótka odpowiedź jest taka, że robi to rynek.

Bitcoiny, podobnie jak większość innych walut, mają *płynny kurs wymiany*. To oznacza, że wartość bitcoina w stosunku do innych walut zmienia się zgodnie z popytem i podażą na różnych rynkach, na których handluje się tymi walutami. Na przykład „cena" bitcoinów w dolarach amerykańskich jest obliczana na każdym rynku na podstawie ostatniej transakcji. Dlatego cena błyskawicznie zmienia się kilka razy na minutę. Serwisy zajmujące się wyceną agregują ceny z kilku rynków i obliczają ważoną wolumenem średnią, reprezentującą na szerokim rynku kurs wymiany dla pary walutowej (np. BTC/USD).

[3] *https://localbitcoins.com/*.

[4] *https://coinatmradar.com/*.

[5] *https://bitcoinaverage.com/*.

Istnieją setki aplikacji i witryn, które udostępniają aktualny kurs wymiany. Oto kilka najpopularniejszych serwisów tego typu:

Bitcoin Average[6]

W tej witrynie znajdziesz prostą ważoną wolumenem średnią dla poszczególnych walut.

CoinCap[7]

W tym serwisie podana jest kapitalizacja rynku i kursy wymiany dla setek kryptowalut, w tym dla bitcoinów.

Chicago Mercantile Exchange Bitcoin Reference Rate[8]

Tu znajdziesz kurs referencyjny, który może być stosowany przez instytucje i w kontraktach. Jest on podawany przez CME w ramach danych dla inwestorów.

Oprócz tego, że dostępne są różne witryny i aplikacje podające kurs, większość portfeli automatycznie przelicza bitcoiny na inne waluty. Joe używa swojego portfela, aby automatycznie ustalić cenę przed przesłaniem bitcoinów do Alice.

Przesyłanie i otrzymywanie bitcoinów

Alice zdecydowała się kupić bitcoiny za 10 dolarów, aby nie ryzykować zbyt dużo pieniędzy na poznanie nowej technologii. Płaci Joemu 10 dolarów w gotówce, otwiera portfel Mycelium i wybiera opcję *Receive*. W efekcie wyświetla się kod QR z pierwszym należącym do Alice adresem bitcoin.

Joe w swoim smartfonie wybiera opcję *Send*, po czym pojawił się ekran z dwoma polami:

- miejscem na docelowy adres bitcoin,
- miejscem na kwotę w bitcoinach (BTC) lub lokalnej walucie (USD).

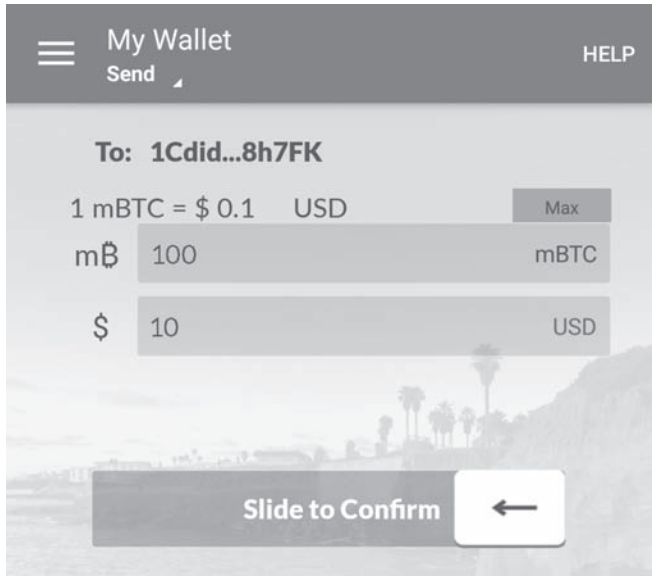
W polu przeznaczonym na adres bitcoin znajduje się mała ikona wyglądająca jak kod QR. Umożliwia to Joemu zeskanowanie kodu kreskowego za pomocą aparatu smartfona, dzięki czemu nie trzeba wpisywać adresu bitcoin Alice (który jest dość długi i skomplikowany). Joe klika ikonę kodu QR i włącza aparat, po czym skanuje kod QR ze smartfona Alice.

W smartfonie Joego w polu odbiorcy pojawia się adres bitcoin Alice. Joe wprowadza kwotę 10 dolarów, a portfel przelicza ją, pobierając najnowszy kurs wymiany z serwisu internetowego. W tym czasie kurs wymiany wynosi 100 dolarów za bitcoin, tak więc 10 dolarów jest warte 0,10 bitcoina (BTC) lub 100 milibitcoinów (mBTC), co widać na zrzucie ilustrującym portfel Joego (zob. rysunek 1.2).

[6] *https://bitcoinaverage.com/*.

[7] *http://coincap.io/*.

[8] *http://www.cmegroup.com/trading/cf-bitcoin-reference-rate.html*.



Rysunek 1.2. Ekran wysyłania środków w portfelu mobilnym Airbitz

Joe dokładnie upewnia się, że wprowadził poprawną kwotę, ponieważ za chwilę prześle środki, a pomyłki są nieodwracalne. Po dokładnym sprawdzeniu adresu i kwoty wciska przycisk *Send*, aby zrealizować transakcję. Portfel mobilny Joego generuje transakcję, w której 0,10 BTC jest przesyłane na adres podany przez Alice. Środki te pochodzą z portfela Joego, a transakcja jest podpisana kluczami prywatnymi tej osoby. W ten sposób do sieci bitcoina trafiają informacje, że Joe autoryzował transfer wartości na nowy adres Alice. Gdy transakcja jest przesyłana protokołem P2P, szybko rozprzestrzenia się po sieci bitcoina. W mniej niż sekundę większość mających wiele połączeń węzłów sieci otrzymuje informacje o transakcji i po raz pierwszy otrzymuje adres Alice.

W tym czasie portfel Alice cały czas śledzi transakcje publikowane w sieci bitcoina, oczekując na te, które pasują do adresów z jej portfeli. Kilka sekund po tym, jak transakcja została wysłana z portfela Joego, portfel Alice informuje o otrzymaniu 0,10 BTC.

Potwierdzenia

Początkowo portfel Alice wyświetla transakcję od Joego jako niezatwierdzoną. To oznacza, że transakcja została rozesłana po sieci, ale nie została jeszcze zarejestrowana w księdze transakcji (nazywanej łańcuchem bloków). Aby transakcja została zatwierdzona, musi zostać umieszczona w bloku i dodana do łańcucha bloków, co odbywa się średnio co 10 minut. W terminologii z tradycyjnego świata finansów jest to proces *rozliczania*. Więcej informacji na temat rozsyłania, walidacji i rozliczania (zatwierdzania) transakcji w bitcoinach znajdziesz w rozdziale 10.

Alice jest teraz dumną posiadaczką 0,10 BTC, które może wydać. W następnym rozdziale przyjrzysz się jej pierwszemu zakupowi z użyciem bitcoinów oraz znajdziesz szczegółowe omówienie technologii związanych z transakcjami i ich rozsyłaniem.

Skorowidz

A

adres, 21
  bitcoin, 90, 162
  P2SH, 21, 105, 169
  vanity, 106
adresy wielopodpisowe, 105
algorytm
  ECD, 160
  podpisywania, 340
  Proof-of-Work, 236
API, 70
architektura sieci P2P, 185
asymetryczne odwoływalne zobowiązania, 295
ataki związane z konsensusem, 260

B

badanie bloków, 73
Base58, 91
Base58Check, 91
bezpieczeństwo, 273
  adresów vanity, 110
  dobre praktyki, 276
  reguły, 273
  rozwoju systemów, 274
biblioteka, 77
  Bitcore, 343
  pycoin, 347
BIND, 192
BIP, Bitcoin Improvement Proposal, 21, 325
BIP-32, 117
BIP-34, 269
BIP-39, 118, 121, 125
BIP-44, 117
BIP-9, 270
bitcoin, 21, 31
Bitcoin Core
  API, 70
  dekodowanie transakcji, 72
  implementacja, 60
  konfiguracja, 62
  konfigurowanie węzła, 66
  pliki wykonywalne, 64
  sprawdzanie transakcji, 72
  stan klienta, 71
  uruchamianie węzła, 65
  wybór wersji, 61
Bitcoin Explorer, 355
Bitcore, 343
blok, 21, 207
  identyfikatory, 209
  łańcuch, 279
  łączenie, 211, 246
  nagłówek, 209
  początkowy, 21, 210
  rozgałęzienia łańcucha, 247
  sprawdzanie poprawności, 245
  struktura, 208
  testowe łańcuchy, 218
  tworzenie nagłówka, 235
  udane wykopanie, 244
  wykopywanie, 236
blokady
  CLTV, 174
  oparte na czasie, 22, 172, 175, 177
  z użyciem skrótu, 22
błąd w wykonywaniu operacji, 166

C

cegiełki, 279
cel, 22, 242
  określający poziom trudności, 22
celowanie w opłaty, 179
cena, 40
coinbase, 22
colored coins, 22, 282
counterparty, 287

D

dane coinbase, 233
dekodowanie transakcji, 72
dobre praktyki
  zabezpieczenia dla użytkowników, 276
  związane z portfelami, 119
dodatkowa wartość nonce, 22
dokumenty BIP, 325
dowód pracy, 22
drzewo skrótów, 23, 212, 218
dywersyfikacja ryzyka, 277
dzielenie wartości, 313

E

ECDSA, 23, 155, 160
ekonomia, 224
EVM, Ethereum Virtual Machine, 287

F

filtry Blooma, 198
fizyczne przechowywanie bitcoinów, 276
format
  Base58Check, 96, 97
  WIF, 23
formaty
  kluczy prywatnych, 95
  kluczy publicznych, 97
formy transakcji, 48
FPGA, 254
funkcje pakietu Bitcore, 343

G

generowanie
  adresów vanity, 107
  klucza publicznego, 88
  kodów mnemonicznych, 121
  prywatnych kluczy podrzędnych, 128
  publicznych kluczy podrzędnych, 130
  zabezpieczone kluczy podrzędnych, 132
górnik, 23, 265

H

hasło opcjonalne, 125
HD, Hierarchical Deterministic, 26
historia, 33
HTLC, Hash Time Lock Contract, 23, 298

I

identyfikatory
  bloku, 209
  transakcji, 339
implementacja
  Bitcoin Core, 60
  wzorcowa, 59
indeks bazy danych, 68
interfejs API, 70, 74

J

język Script, 149

K

kanały
  niewymagające zaufania, 292
  płatności, 23, 287, 290
  płatności z trasowaniem, 299
  stanowe, 287, 288
Key Utility, 347
klauzule warunkowe, 179
klienty, 77
klucz, 81
  formaty, 95
  generowanie, 88
  obsługa w Pythonie, 101
  podrzędny, 128
  prywatny, 23, 83
  publiczny, 82, 85
  rozszerzony, 129
  skompresowany, 97
kod
  operacji, 23
  QR, 45

kodowanie Base58, 91
kody mnemoniczne, 118
kompletność w sensie Turinga, 23
konfigurowanie
  Bitcoin Core, 62
  węzła, 66
konsensus, 24, 223, 260
  ataki, 260
  rozwój oprogramowania, 272
  zmienianie reguł, 263
kontrakty HTLC, 298
kopalnie, 256
  P2P, 259
  zarządzane, 258
kopanie, 223, 254
  bitcoinów, 53
  bloków transakcji, 54
  w ramach kopalni, 24
korzeń drzewa skrótów, 24
kryptografia, 82, 87
krytyka miękkich rozgałęzień, 268
krzywa eliptyczna, 86
KYC, Know Your Customer, 24

L

LevelDB, 24
LIFO, Last-In-First-Out, 151
Lightning Network, 24, 299
  przesył, 303
  trasowanie, 303

Ł

łańcuch
  bloków, 24, 207, 218, 279
  transakcji, 46
łączenie
  bloków, 211, 246
  transakcji w bloki, 229
  wartości, 313

M

mechanizm
  Median-Time-Past, 178
  Segregated Witness, 331
miękkie rozgałęzienie, 24, 333
mnemoniczne słowa kodowe, 121

N

nagłówek bloku, 209
nagroda, 24
  w transakcji, 231
narzędzie
  Bitcoin Explorer, 355
  Key Utility, 347
  Transaction Utility, 353
nieaktualny blok, 24
niekompletność w sensie Turinga, 150

O

obliczanie skrótów, 254
obliczenia, 314
  rozproszone, 34
obsługa
  adresów, 101
  kluczy, 101
  portfeli, 115
  technologii Segregated Witness, 220
odzyskiwanie pamięci, 311
określanie aktualnej ceny, 40
OP_RETURN, 25
opcja txindex, 68
operacja
  CHECKMULTISIG, 166
  CSV, 177
  VERIFY, 180
operatory, 319
opłaty, 25
  transakcyjne, 145, 231
osiąganie konsensusu, 226, 263
osierocone transakcje, 25
otrzymywanie bitcoinów, 41

P

P2P, peer-to-peer, 185
  sieć rozszerzona, 187
  szyfrowanie, 204
  uwierzytelnianie, 204
  węzły, 186
P2PKH, Pay to PubKey Hash, 25, 154
P2SH, Pay to Script Hash, 25, 167, 337
P2WPKH, Pay to Witness Public Key Hash, 25, 334–337
P2WSH, Pay to Witness Script Hash, 25, 335–338

pakiet Bitcore, 343
pakiety narzędzi, 77
podaż pieniądza, 224
podpisy cyfrowe, 155
podwójne wydatkowanie, 25
podział górników na grupy, 265
pole z czasem blokady, 25
polecenia Bitcoin Explorer, 355
połączenia szyfrowane, 204
portfele, 26, 115
  deterministyczne, 117
  dobre praktyki, 119
  HD, 262, 117, 126
  niedeterministyczne, 116
  papierowe, 26, 111
  sprzętowe, 26, 277
  stosowane technologie, 121
  struktura drzewiasta, 135
  używanie, 119
potwierdzenia, 26, 42
POW, Proof-of-Work, 54
pozyskiwanie bitcoinów, 39
problem
  bizantyjskich generałów, 26
  obliczeń rozproszonych, 34
Proof-of-Stake, 26
protokół
  HD, 26
  Open Assets, 26
  Segregated Witness, 27
prywatność, 203, 313
przechowywanie w trybie offline, 27
przepływ sterowania, 181
przesyłanie bitcoinów, 41
pula transakcji, 27, 205
Python
  obsługa kluczy i adresów, 101

R

Regtest, 221
reguły
  bezpieczeństwa, 273
  utrzymywania konsensusu, 27
reprezentacja celu, 242
RIPEMD-160, 27
role węzłów, 186
rozgałęzienie, 27
  kontrowersyjne, 266
  łańcucha bloków, 247–253
  miękkie, 267
  twarde, 263
  sygnalizowanie, 269
rozwiązania oparte na cegiełkach, 282
równoważenie ryzyka, 277
RPC, Remote Procedure Call, 75
ryzyko
  dywersyfikacja, 277
  równoważenie, 277

S

Satoshi, 27
Satoshi Nakamoto, 27
Script, 149
segnet, 220
Segregated Witness, 220, 331
segwit, 336
serializowanie
  podpisów, 157
  transakcji, 144
serwer znaczników czasu, 309
SHA, Secure Hash Algorithm, 28, 90
sieć, 28, 310
  Bitcoin Relay Network, 190
  Lightning Network, 300
  P2P, 185, 307
  testnet, 219
  Tor, 204
SIGHASH, 158
skompresowane
  klucze prywatne, 99
  klucze publiczne, 97
skrót, 28, 254
skrypt, 28
  P2PKH, 154
  P2SH, 338
  P2WPKH, 25, 334–337
  P2WSH, 335–338
  scriptPubKey, 28
  scriptSig, 28
skrypty
  transakcji, 149
  wielopodpisowe, 165
  wypłaty, 170
  z przepływem sterowania, 179
sprawdzanie
  poprawności, 170
  poprawności nowego bloku, 245

poprawności podpisu, 158
poprawności transakcji, 227
transakcji, 72
SPV, Simplified Payment Verification, 28, 186, 195, 312
stałe, 319
stan konta, 162
stos wykonawczy skryptu, 151
stosowanie segwita, 340
struktura
bloku, 208
transakcji coinbase, 232
sygnalizowanie miękkich rozgałęzień, 269
symbole, 319
system bitcoina, 44
szyfrowane klucze prywatne, 104

Ś

ścieżki w portfelach HD, 134
środowisko programistyczne, 60

T

testnet, 219
testy regresyjne, 221
Tor, The Onion Routing, 204
Transaction Utility, 353
transakcja, 28, 46, 137, 308
coinbase, 28, 230–232
OP_RETURN, 28
transakcje
API, 74
dekodowanie, 72
dodawane do księgi, 52
dodawanie opłat, 148
generowanie wyjść, 51
identyfikatory, 339
łańcuchy, 46
łączenie w bloki, 229
nagrody, 231
niezależne sprawdzanie poprawności, 227
operacje wykonywane na zapleczu, 137
opłaty, 145, 231
P2SH, 167
serializowanie, 144
skrypty, 149
spoza łańcucha, 29
sprawdzanie, 72
tworzenie, 49
typowe formy, 48
wejścia, 46, 139
wybór wejść, 50
wydawanie reszty, 48
wydawanie środków, 56
wyjścia, 46, 139
z użyciem colored coins, 284
zaawansowane, 165
transfer, 204
trasowanie, 299
trudność, 29
twarde rozgałęzienie, 29
tworzenie
kanałów niewymagających zaufania, 292
nagłówka bloku, 235
podpisu cyfrowego, 157
portfela HD, 126
skryptów, 150
transakcji, 49
wyjść P2WPKH, 335
typy
skrótów podpisów, 158
węzłów, 186

U

uruchamianie węzła, 65
UTXO, Unspent Transaction Output, 29
uwierzytelniane, 204
używanie
portfela, 119
rozszerzonego klucza publicznego, 132

W

waluta
cyfrowa, 32
deflacyjna, 226
wartość nonce, 29, 256
wejścia transakcji, 139
weryfikacja bezstanowa, 150
węzły, 186
kompletne, 194
służące do kopania, 228
SPV, 195, 202, 203, 218
wielopodpis, 29, 278

wybór
łańcuchów, 246
portfela, 36
wersji implementacji, 61
wydawanie
reszty, 48
środków, 56
wyjścia, 29
P2WPKH, 335
rejestrujące dane, 171
transakcji, 139
wykopywanie bloku, 236
wykrywanie sieci, 190

Z

zachowanie dostępu, 278
zalety stosowania P2SH, 170
zastosowania, 34
zdecentralizowane osiąganie konsensusu, 226
ziarna, 118, 123
portfela HD, 29
zmiana celu, 242
określającego poziom trudności, 29
zobowiązania odwoływalne, 295

Ź

źródło zaufania, 275

Ż

żądanie płatności, 45

O'REILLY®

Bitcoin — rewolucja technologiczna wkracza w świat finansów!

Być może słowo „bitcoin" kojarzy Ci się z niezwykle skomplikowanym i niebezpiecznym półświatkiem cyberprzestępców. Możliwe, że widzisz w rozwoju tej kryptowaluty szansę ucieczki przed pazernością bankierów. A może po prostu chcesz dokładniej wiedzieć, czym jest ta technologia, jakie może mieć wkrótce znaczenie dla nowoczesnych firm i jak ją wykorzystać we własnych aplikacjach. Warto! Zdecentralizowana waluta bitcoin, choć wciąż jest na wczesnym etapie rozwoju, już zapoczątkowała wart wiele miliardów dolarów globalny rynek otwarty dla każdego, kto posiada wiedzę, pasję i jest gotów do działania.

Niniejsza książka jest przeznaczona dla każdego, kto chce zrozumieć zasady funkcjonowania bitcoina i kryptowalut. Skorzystają z niej zwłaszcza programiści, którzy będą mogli nauczyć się pisania oprogramowania związanego z bitcoinem. Znalazło się tu objaśnienie technicznych podstaw bitcoina i kryptowalut, podano informacje na temat zdecentralizowanej sieci bitcoina, architektury P2P, cyklu życia transakcji i zasad bezpieczeństwa, a także omówienie nowych technologii. Sporo miejsca poświęcono zastosowaniom łańcucha bloków. Dzięki ciekawie i zrozumiale przedstawionym informacjom zawartym w książce zyskasz aktualną wiedzę, która pozwoli Ci wkroczyć na ścieżkę bitcoina!

W tej książce między innymi:

- zasady funkcjonowania bitcoina i łańcucha bloków
- sposób działania kryptowalut z punktu widzenia architektury systemu
- implementacja wzorcowa Bitcoin Core
- technologie obsługi portfeli i sieci bitcoina

Andreas M. Antonopoulos — jest niekwestionowanym autorytetem w świecie bitcoina i kryptowalut. Równocześnie jest cenionym specjalistą w zakresie technologii sieci, bezpieczeństwa, centrów danych i przetwarzania w chmurze. Doradza kierownictwu wielu firm z listy Fortune 500. Został również uznany za osobę o dużych zdolnościach dydaktycznych: wygłasza prelekcje, jest cenionym nauczycielem akademickim, chętnie zabiera głos na konferencjach poświęconych nowoczesnym technologiom, przede wszystkim bezpieczeństwu.

ISBN 978-83-283-4035-0
9 788328 340350
Cena: 69,00 zł