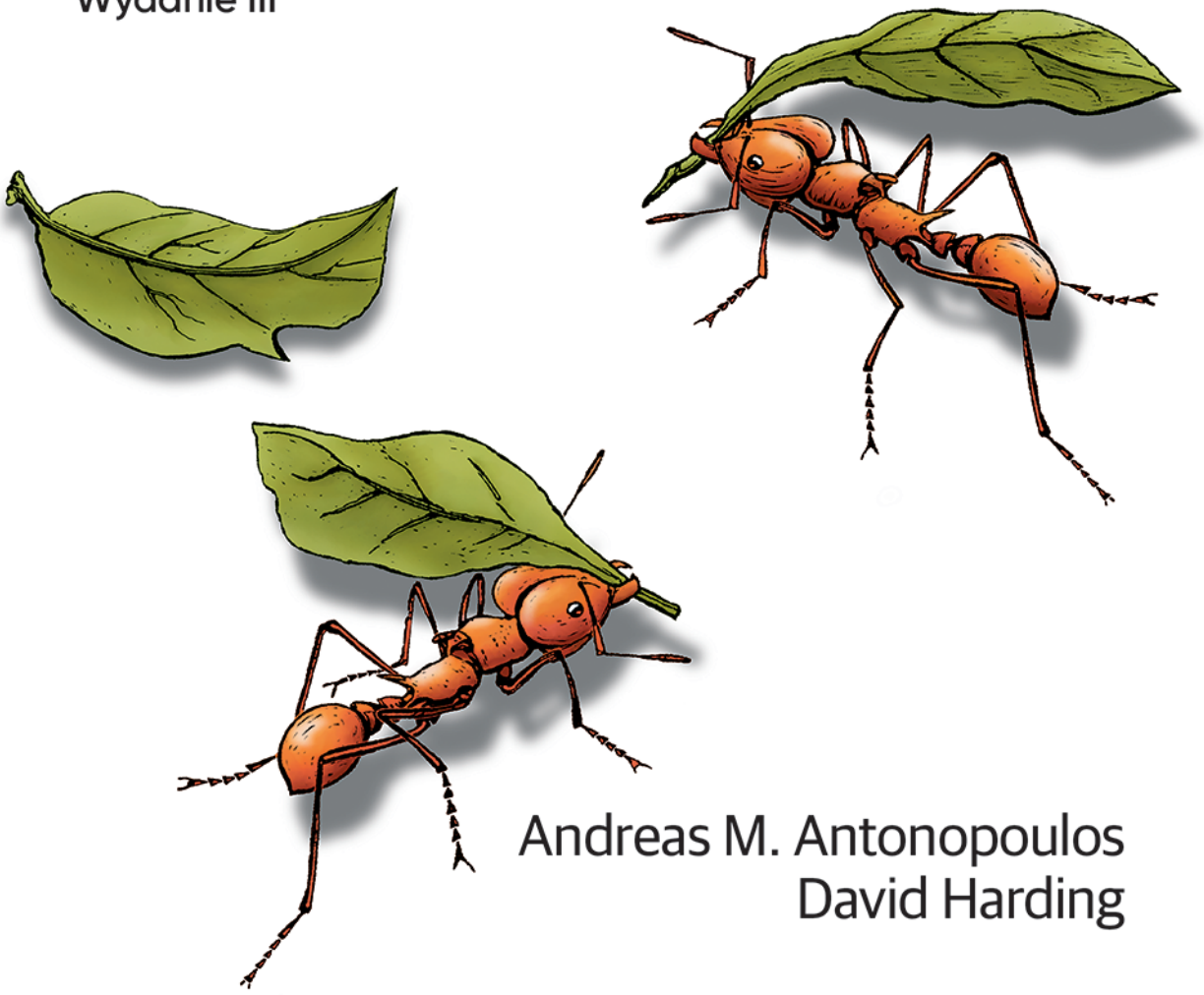
O'REILLY®

Helion

Bitcoin

Wszystko, co musisz wiedzieć o programowaniu z użyciem otwartego łańcucha bloków

Wydanie III



Andreas M. Antonopoulos
David Harding

Tytuł oryginału: Mastering Bitcoin: Programming the Open Blockchain, 3rd Edition

Tłumaczenie: Grzegorz Werner, z wykorzystaniem fragmentów książki „*Bitcoin dla zaawansowanych. Programowanie z użyciem otwartego łańcucha bloków. Wydanie II*” w przekładzie Tomasza Walczaka

ISBN: 978-83-289-1564-0

Authorized Polish translation of the English edition of *Mastering Bitcoin, 3E*
ISBN 9781098150099 © 2024 David Harding.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/bitws3
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

ROZDZIAŁ 2.

Jak działają bitcoiny?

System bitcoina, w odróżnieniu od tradycyjnych płatności i systemów bankowych, nie wymaga ufania stronom trzecim. W systemie bitcoina nie ma centralnej zaufanej jednostki; zamiast tego każdy może używać oprogramowania działającego we własnym komputerze, aby weryfikować poprawne działanie każdego aspektu systemu. W tym rozdziale analizuję bitcoiny na ogólnym poziomie, śledząc jedną transakcję w systemie bitcoina i patrząc, jak staje się ona „godna zaufania" — zostaje zaakceptowana przez mechanizm osiągania konsensusu w środowisku rozproszonym i ostatecznie zarejestrowana w łańcuchu bloków (rozproszonej księdze wszystkich transakcji). W dalszych rozdziałach opisane są technologie związane z transakcjami, siecią i kopaniem.

Omówienie bitcoinów

System bitcoina obejmuje użytkowników z portfelami zawierającymi klucze, transakcje rozsyłane w sieci i górników, którzy generują (konkurując w obliczeniach) oparte na konsensusie łańcuchy bloków, będące autorytatywną księgą wszystkich transakcji.

Każdy przykład z tego rozdziału jest oparty na rzeczywistej transakcji wykonanej w sieci bitcoina, symulującej interakcje między użytkownikami przesyłającymi środki z jednego portfela do drugiego. Do śledzenia transakcji w sieci bitcoina (aż do poziomu łańcucha bloków) posłuży witryna *eksploratora łańcucha bloków*, gdzie wizualizowane są wszystkie kroki. Eksplorator łańcucha bloków to aplikacja internetowa działająca jak wyszukiwarka w systemie bitcoina. Pozwala ona znaleźć adresy, transakcje i bloki, a także podejrzeć relacje między nimi i przepływ środków.

Oto popularne eksploratory łańcucha bloków:

- Blockstream Explorer (*https://blockstream.info*),
- Mempool.Space (*https://mempool.space*),
- BlockCypher Explorer (*https://live.blockcypher.com*).

Każdy z tych serwisów udostępnia wyszukiwarkę, w której można wpisać adres bitcoin, skrót transakcji, numer bloku lub skrót bloku i pobrać powiązane z danym elementem informacje z sieci bitcoina. Dla każdej transakcji lub bloku podany jest adres URL, dzięki czemu będziesz mógł sam przyjrzeć się danym i starannie je przeanalizować.

Ostrzeżenie dotyczące prywatności w eksploratorze łańcucha bloków

Wyszukiwanie informacji w eksploratorze łańcucha bloków ujawnia jego operatorowi, że jesteś zainteresowany tymi informacjami, i pozwala powiązać je z Twoim adresem IP, szczegółami przeglądarki, poprzednimi wyszukiwaniami oraz innymi identyfikowalnymi danymi. Jeśli sprawdzisz informacje opublikowane w tej książce, operator eksploratora może domyślić się, że uczysz się o bitcoinie, co nie powinno być problemem. Jeśli jednak wyszukasz własne transakcje, operator prawdopodobnie będzie w stanie ustalić, ile bitcoinów otrzymałeś, wydałeś i obecnie posiadasz.

Zakup w sklepie internetowym

Przedstawiona w poprzednim rozdziale Alice to nowa użytkowniczka, która właśnie pozyskała pierwsze bitcoiny. W punkcie „Pozyskiwanie pierwszych bitcoinów" przeczytałeś, że Alice spotkała się z przyjacielem (Joem), by wymienić gotówkę na bitcoiny. Transakcja utworzona przez Joego zasiliła portfel Alice kwotą 0,001 BTC. Teraz Alice dokona pierwszej transakcji kupna, nabywając dostęp do płatnego podcastu w internetowym sklepie Boba.

Sklep internetowy Boba niedawno zaczął akceptować płatności w bitcoinach, dodając taką opcję do witryny. Ceny w sklepie Boba są podawane w lokalnej walucie (dolarach), jednak klienci mogą płacić zarówno dolarami, jak i bitcoinami.

Alice znajduje odcinek podcastu, który chce kupić, i przechodzi do strony płatności. Oprócz typowych sposobów płatności znajduje się tu również opcja zapłaty bitcoinami. Koszyk wyświetla cenę w dolarach, a także w bitcoinach (BTC) w przeliczeniu według bieżącego kursu.

System e-commerce Boba automatycznie tworzy kod QR zawierający *fakturę* (rysunek 2.1).

Rysunek 2.1. Kod QR faktury

W odróżnieniu od kodu QR zawierającego docelowy adres bitcoin faktura jest kodem QR z adresem URI obejmującym adres docelowy, kwotę i ogólny opis. Dzięki temu portfel może wstępnie uzupełnić informacje potrzebne do przesłania płatności, a jednocześnie wyświetlić użytkownikowi czytelny opis. Możesz zeskanować ten kod QR za pomocą aplikacji portfela, aby zobaczyć to, co ujrzałaby Alice.

```
bitcoin: bc1qk2g6u8p4qm2s2lh3gts5cpt2mrv5skcuu7u3e4?amount=0.01577764&
label=Bob%27s%20Store&
message=Purchase%20at%20Bob%27s%20Store
```

```
Składowe adresu URI

Adres bitcoin: "bc1qk2g6u8p4qm2s2lh3gts5cpt2mrv5skcuu7u3e4"
Kwota płatności: "0.01577764"
Etykieta dla adresu odbiorcy: "Bob's Store"
Opis płatności: "Zakup w Bob's Store"
```

Spróbuj zeskanować ten kod za pomocą swojego portfela, aby zobaczyć adres i kwotę, jednak NIE WYSYŁAJ PIENIĘDZY.

Alice używa smartfona do zeskanowania kodu kreskowego z wyświetlacza. Smartfon informuje o płatności w odpowiedniej kwocie na rzecz `Bob's Store`, po czym Alice wybiera opcję *Send*, aby zatwierdzić płatność. W przeciągu kilku sekund (mniej więcej tyle samo czasu trwa autoryzowanie transakcji kartą kredytową) Bob widzi na kasie, że transakcja została zrealizowana.

W sieci bitcoina transakcje mogą dotyczyć wartości ułamkowych od milibitcoinów (1/1000 bitcoina) aż do 1/100 000 000 bitcoina (ta jednostka to satoshi). W tej książce używane są te same reguły odmiany co w przypadku dolarów i innych tradycyjnych walut oraz ich wartości ułamkowych w notacji dziesiętnej, na przykład „10 bitcoinów" albo „0,001 bitcoina". Te same reguły dotyczą innych jednostek księgowych bitcoina, takich jak milibitcoiny i satoshi.

Możesz użyć eksploratora bloków, aby zbadać dane zapisane w łańcuchu bloków, takie jak płatność na rzecz Boba w transakcji Alice (*https://oreil.ly/hAeyh*).

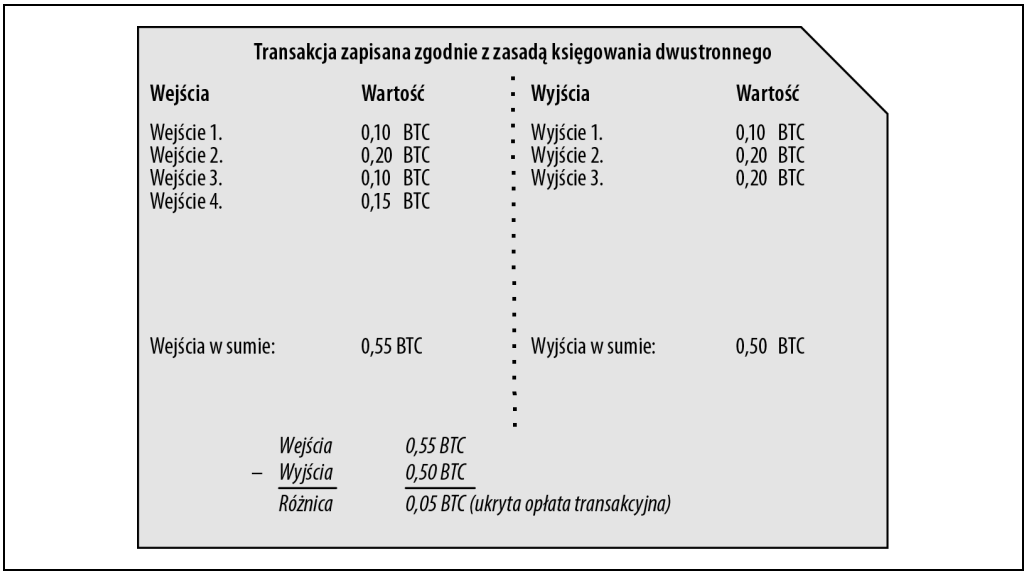
W dalszych punktach ta transakcja jest opisana bardziej szczegółowo. Zobaczysz, jak portfel Alice ją wygenerował, jak została ona rozesłana w sieci, jak przebiegała weryfikacja i jak Bob może wydać środki w dalszych transakcjach.

Transakcje w bitcoinach

W prostych słowach można opisać, że transakcja informuje sieć, iż właściciel bitcoinów o pewnej wartości autoryzował transfer tej wartości do innego właściciela. Nowy właściciel może następnie wydać te środki, tworząc inną transakcję i autoryzując transfer wartości do innej osoby, przez co powstaje łańcuch własności.

Wejścia i wyjścia w transakcjach

Transakcje są jak wiersze w księdze rachunkowej, w której używana jest zasada księgowania dwustronnego. Każda transakcja obejmuje *wejścia*, które są jak wydatki na rachunku w bitcoinach. Po drugiej stronie znajdują się *wyjścia*, które są jak środki dodawane do rachunku (wpływy). Wejścia i wyjścia nie muszą sumować się do tej samej wartości. Wyjścia są zwykle nieco niższe niż wejścia, a różnica reprezentuje ukrytą *opłatę transakcyjną*, czyli niewielką kwotę pobieraną przez górnika, który dodał transakcję do łańcucha bloków. Transakcja w bitcoinach jako wpis z księgi rachunkowej jest przedstawiona na rysunku 2.2.

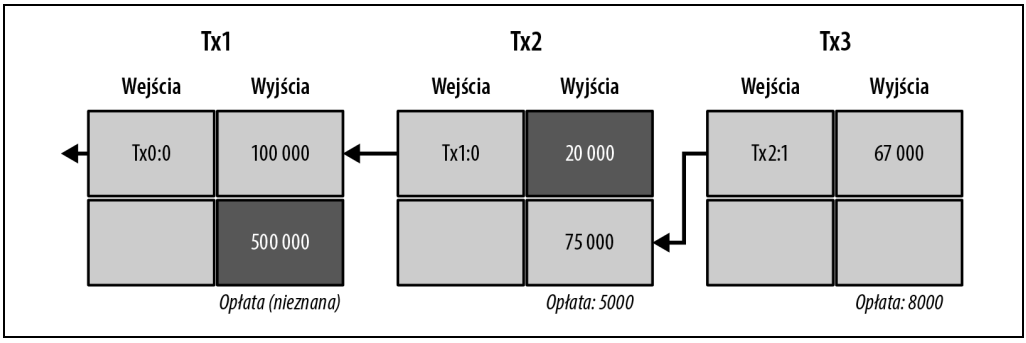


Rysunek 2.2. Transakcja zapisana zgodnie z zasadą księgowania dwustronnego

Transakcja obejmuje też dowód na posiadanie wydawanych kwot bitcoinów (wejść). Ma on postać cyfrowego podpisu właściciela i może zostać niezależnie sprawdzony przez dowolną osobę. W systemie bitcoina „wydawanie" polega na podpisaniu transakcji przekazującej wartość od wcześniejszego właściciela do nowego, identyfikowanego za pomocą adresu bitcoin.

Łańcuchy transakcji

W płatności Alice na rzecz Bob's Store jako wejście posłużyło wyjście z wcześniejszej transakcji. W poprzednim rozdziale Alice w zamian za gotówkę otrzymała od Joego bitcoiny. Na rysunku 2.3 oznaczyliśmy to jako *Transakcję 1* (Tx1).



Rysunek 2.3. Łańcuch transakcji, w którym wyjście z jednej transakcji stanowi wejście następnej

Transakcja Tx1 wysłała 0,001 bitcoina (100 000 satoshi) do wyjścia blokowanego przez klucz Alice. Jej nowa transakcja na rzecz Bob's Store (Tx2) odwołuje się do poprzedniego wyjścia jako do wejścia. Na rysunku pokazujemy tę referencję za pomocą strzałki oraz oznaczenia wejścia jako „Tx1:0".

W rzeczywistej transakcji referencją jest 32-bajtowy identyfikator transakcji (txid), w której Alice otrzymała pieniądze od Joego. Zapis „:0” wskazuje pozycję wejścia, w którym Alice otrzymała pieniądze, w tym przypadku pierwszą pozycję (pozycję 0).

Jak pokazano, rzeczywiste transakcje bitcoina nie obejmują jawnie wartości wejścia. Aby określić wartość wejścia, oprogramowanie musi użyć referencji do wejścia i znaleźć wydatkowane wyjście poprzedniej transakcji.

Transakcja Tx2 obejmuje dwa nowe wyjścia. Jedno wypłaca 75 000 satoshi za podcast, a drugie wypłaca Alice z powrotem 20 000 satoshi jako resztę.

Serializowane transakcje bitcoina — format danych, którego oprogramowanie używa do wysyłania transakcji — kodują przekazywaną wartość jako całkowitą wielokrotność najmniejszej zdefiniowanej jednostki wartości. Zaraz po utworzeniu systemu bitcoina jednostka ta nie miała nazwy i niektórzy deweloperzy nazywali ją po prostu *jednostką podstawową*. Później wielu użytkowników zaczęło nazywać ją *satoshi* (sat) na cześć twórcy bitcoina. Na rysunku 2.3 i niektórych innych ilustracjach w książce używamy wartości satoshi, ponieważ właśnie ich używa sam protokół.

Wydawanie reszty

Oprócz jednego lub wielu wyjść, które opłacają odbiorcę bitcoinów, wiele transakcji obejmuje wyjścia, które opłacają wydającego bitcoiny, nazywane *wyjściami reszty*. Jest to potrzebne, ponieważ wejścia transakcji, podobnie jak banknoty, nie mogą być dzielone. Jeśli kupisz w sklepie produkt za 5 dolarów, ale masz tylko banknot 20-dolarowy, oczekujesz, że otrzymasz 15 dolarów reszty. To samo dotyczy wejść w transakcjach w bitcoinach. Jeśli zakupisz produkt wart 5 bitcoinów, ale masz do wykorzystania tylko wejście o wartości 20 bitcoinów, prześlesz jedno wyjście (o wartości 5 bitcoinów) do sprzedawcy i drugie (o wartości 15 bitcoinów minus koszty transakcji) do samego siebie.

Na poziomie protokołu bitcoina nie ma różnicy między wyjściem reszty (i opłacanym przez nie adresem, nazywanym *adresem reszty*) a wyjściem płatności.

Ważne jest to, że adres reszty nie musi być taki sam jak adres, z którego pochodzi wejście. Ze względu na prywatność adres reszty jest często nowym adresem właściciela portfela. W idealnych okolicznościach dwa różne zastosowania wyjść używają niewidzianych wcześniej adresów i pod innymi względami wyglądają identycznie, co uniemożliwia stronom trzecim ustalenie, które wyjścia są resztami, a które płatnościami. Jednakże dla celów ilustracyjnych zacieniowaliśmy wyjścia reszty na rysunku 2.3.

Nie każda transakcja ma wyjście reszty. Te, które go nie mają, są nazywane *transakcjami bezresztowymi* i mogą mieć tylko jedno wyjście. Transakcje bezresztowe są praktyczną opcją tylko pod warunkiem, że wydawana kwota jest mniej więcej taka sama jak kwota dostępna w wejściach transakcji pomniejszona o przewidywaną opłatę transakcyjną. Na rysunku 2.3 pokazano, jak Bob tworzy transakcję bezresztową, w której wydaje wyjście otrzymane w transakcji Tx2.

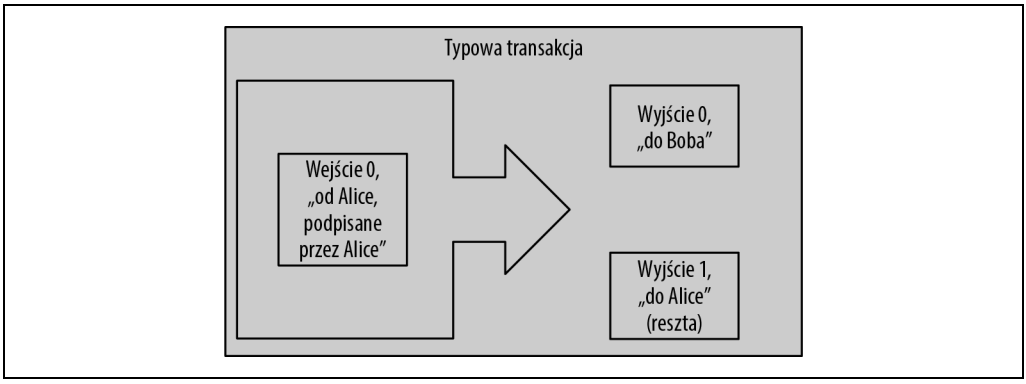
Wybór monet

W różnych portfelach mogą być stosowane odmienne strategie łączenia wejść w celu dokonywania płatności żądanych przez użytkownika. Określa się to mianem *wyboru monet*.

Portfel może łączyć wiele drobnych wejść lub wykorzystać wejście równe lub większe względem oczekiwanej płatności. Jeśli portfel nie może połączyć wejść w taki sposób, by uzyskać wartość dokładnie równą oczekiwanej płatności (z uwzględnieniem opłat transakcyjnych), nieuniknione jest wygenerowanie reszty. Bardzo przypomina to korzystanie z gotówki. Jeśli zawsze będziesz wydawał banknot o najwyższym nominale, będziesz miał kieszenie pełne drobnych. Jeżeli zawsze będziesz wydawał drobne, zostaną Ci tylko banknoty o wysokim nominale. Ludzie nieświadomie dążą do zachowania równowagi między tymi dwoma skrajnościami, a twórcy portfeli starają się programować podobne rozwiązania.

Typowe formy transakcji

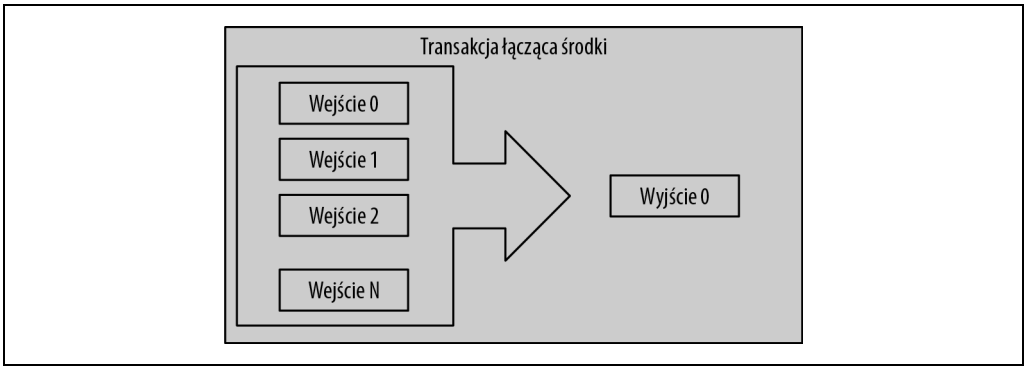
Najczęściej występującą formą transakcji jest płatność prosta. W transakcjach tego typu występuje jedno wejście i dwa wyjścia (rysunek 2.4).



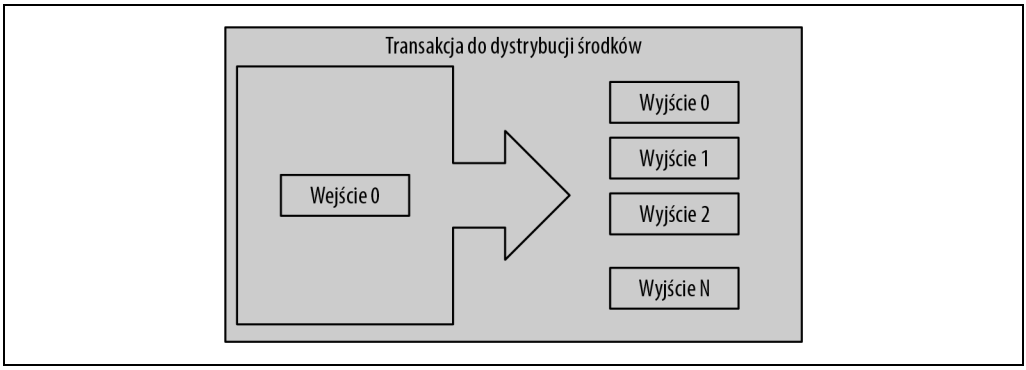
Rysunek 2.4. Najczęściej spotykany rodzaj transakcji

Innym często występującym rodzajem transakcji jest *transakcja konsolidacyjna*, która polega na łączeniu grupy wejść w jedno wyjście (rysunek 2.5). Jest to odpowiednik wymiany monet i banknotów o niższym nominale na jeden banknot o wysokim nominale. Tego rodzaju transakcje są czasem generowane przez portfele i firmy w celu scalenia wielu drobnych kwot.

Następny rodzaj transakcji, często występujący w księgach bitcoina, polega na podziale jednego wejścia na wiele wyjść odpowiadających wielu odbiorcom (rysunek 2.6). Transakcje tego typu są czasem przeprowadzane przez podmioty handlowe w celu dystrybucji środków (np. w trakcie przetwarzania wypłat dla wielu pracowników).



Rysunek 2.5. Transakcja konsolidacyjna łącząca środki



Rysunek 2.6. Transakcja służąca do dystrybucji środków

Tworzenie transakcji

Oprogramowanie portfela Alice obejmuje kod do wyboru odpowiednich wejść i wyjść w celu utworzenia transakcji zgodnej z poleceniami Alice. Musi ona jedynie podać docelowy adres, kwotę i opłatę transakcyjną, a resztą zajmie się oprogramowanie portfela. Co ważne, jeśli oprogramowanie zna kontrolowane przez siebie wejścia, to potrafi tworzyć transakcje także w trybie offline. Przypomina to wypisywanie czeku w domu i późniejsze przesyłanie go do banku w kopercie. Podobnie transakcja nie wymaga w trakcie tworzenia i podpisywania połączenia z siecią bitcoina.

Wybór odpowiednich wejść

Oprogramowanie portfela Alice najpierw musi znaleźć wejścia, które pozwalają zapłacić kwotę, jaką właścicielka chce przesłać Bobowi. Większość portfeli śledzi wszystkie dostępne wyjścia powiązane z adresami z tego portfela. Dlatego portfel Alice zawiera kopię wyjść z transakcji Joego, utworzonej w wyniku zapłaty gotówką (zob. punkt „Pozyskiwanie pierwszych bitcoinów"). Oprogramowanie portfela działające na węźle kompletnym zawiera kopie niewydanych wyjść ze wszystkich

potwierdzonych transakcji, nazywanych *niewydanymi wyjściami transakcji* (ang. *unspent transaction output,* **UTXO**). Ponieważ jednak węzły kompletne zużywają więcej zasobów, większość portfeli używa prostych klientów, śledzących tylko wyjścia UTXO danego użytkownika.

W tym przypadku to jedno UTXO wystarcza do zapłacenia za podcast. Gdyby było inaczej, oprogramowanie portfela musiałoby przejrzeć listę mniejszych niewydanych wyjść, co przypomina wybieranie monet z portmonetki w celu uzbierania wystarczającej kwoty. W obu sytuacjach może się okazać, że konieczne będzie wypłacenie reszty. Jest to opisane w następnym punkcie dotyczącym generowania wyjść transakcji (płatności) przez oprogramowanie portfela.

Generowanie wyjść

Wyjście transakcji jest generowane w postaci skryptu, który mówi coś w rodzaju: „To wyjście jest przekazywane temu, kto przedstawi podpis oparty na kluczu odpowiadającemu publicznemu adresowi Boba". Ponieważ tylko Bob posiada portfel z kluczami powiązanymi z tym adresem, to tylko on może przedstawić potrzebny podpis i uzyskać dostęp do danego wyjścia. W ten sposób Alice ogranicza dostęp do wyjścia za pomocą wymogu przedstawienia podpisu przez Boba.

Z tą transakcją powiązane jest też drugie wyjście, ponieważ środki Alice są warte więcej, niż kosztuje podcast. Płatność reszty dla Alice jest generowana jako wyjście w tej samej transakcji, co płatność dla Boba. Portfel rozdziela więc środki Alice na dwie płatności: jedną dla Boba i drugą zwracaną Alice. Alice może wykorzystać (wydać) odpowiadające reszcie wyjście w następnej transakcji.

Wreszcie, aby transakcja została szybko przetworzona przez sieć, oprogramowanie portfela dodaje niewielką opłatę. Nie jest ona bezpośrednio podawana w transakcji. Opłata ta jest widoczna w różnicy między wejściami a wyjściami. Ta opłata transakcyjna jest pobierana przez górnika za umieszczenie transakcji w bloku rejestrowanym w łańcuchu bloków.

Obejrzyj transakcję Alice na rzecz Bob's Store (*https://oreil.ly/GwBq1*)

Dodawanie transakcji do łańcucha bloków

Transakcja wygenerowana przez oprogramowanie portfela Alice obejmuje wszystko, co jest potrzebne do potwierdzenia własności środków i określenia nowych właścicieli. Następnie ta transakcja musi zostać przesłana do sieci bitcoina, gdzie stanie się częścią łańcucha bloków. W następnym punkcie dowiesz się, w jaki sposób transakcja staje się częścią nowego bloku i jak wygląda „kopanie" bloku. Dalej zobaczysz, że nowy blok po dodaniu do łańcucha staje się coraz bardziej wiarygodny wraz z dodawaniem kolejnych bloków.

Przesyłanie transakcji

Ponieważ transakcja obejmuje wszystkie informacje niezbędne do jej przetworzenia, nie ma znaczenia, jak i gdzie zostanie ona przesłana do sieci bitcoina. Jest to sieć typu P2P. Każdy klient funkcjonuje w niej, łącząc się z kilkoma innymi klientami. Sieć bitcoina służy do rozsyłania transakcji i bloków do wszystkich jej użytkowników.

Jak rozsyłane są dane?

Węzły równorzędne (ang. *peers*) w sieci bitcoina to programy, które dysponują zarówno algorytmami, jak i danymi niezbędnymi do pełnej weryfikacji poprawności nowej transakcji. Połączenia między węzłami równorzędnymi często wizualizuje się jako krawędzie (linie) grafu, w którym same węzły są wierzchołkami (kropkami). Węzły równorzędne są często nazywane „węzłami z kompletną weryfikacją", w skrócie *węzłami kompletnymi*.

Oprogramowanie portfela Alice może przesłać nową transakcję do dowolnego węzła bitcoina korzystającego z połączenia dowolnego rodzaju: przewodowego, Wi-Fi, mobilnego itd. Może też wysłać transakcję do innego programu (takiego jak eksplorator bloków), który przekaże ją do węzła. Portfel Alice nie musi być bezpośrednio połączony z portfelem Boba i nie musi korzystać z połączenia internetowego oferowanego przez Boba, choć oba te rozwiązania są możliwe. Każdy węzeł otrzymujący prawidłową transakcję, z którą się jeszcze nie zetknął, natychmiast przekazuje ją do wszystkich pozostałych powiązanych węzłów. Ta technika rozsyłania nosi nazwę „plotkowania" (ang. *gossiping*). W ten sposób transakcja jest szybko rozsyłana w sieci P2P i w przeciągu kilku sekund dociera do dużego odsetka węzłów.

Perspektywa Boba

Jeśli oprogramowanie portfela Boba jest bezpośrednio połączone z oprogramowaniem portfela Alice, portfel Boba może być pierwszym węzłem, który otrzyma transakcję. Jednak nawet jeżeli portfel Alice prześle transakcję za pośrednictwem innych węzłów, dotrze ona do portfela Boba w przeciągu kilku sekund. Portfel Boba natychmiast zidentyfikuje transakcję Alice jako przychodzącą płatność, ponieważ zawiera ona wyjścia zgodne z kluczami Boba. Oprogramowanie portfela Boba może też niezależnie zweryfikować, że transakcja ma prawidłowy format. Jeśli Bob używa własnego węzła kompletnego, jego portfel może również sprawdzić, czy transakcja Alice wydaje tylko poprawne wyjścia UTXO.

Kopanie bitcoinów

Transakcja Alice jest teraz rozsyłana w sieci bitcoina. Jednak transakcja staje się częścią *łańcucha bloków* dopiero po jej zweryfikowaniu i umieszczeniu w bloku w wyniku procesu nazywanego *kopaniem*. Szczegółowe objaśnienie tego procesu zawiera rozdział 12.

System ochrony przed fałszerstwami w sieci bitcoina jest oparty na obliczeniach. Transakcje są łączone w *bloki*. Bloki zawierają niewielki nagłówek, który musi być uformowany w bardzo konkretny sposób, co wymaga przeprowadzenia ogromnej ilości obliczeń. Proces kopania ma dwa cele:

- Górnicy zyskują uczciwe przychody tylko z tworzenia bloków, które są zgodne ze wszystkimi *regułami uzgadniania konsensusu* w sieci bitcoina. Zwykle motywuje ich to do dołączania wyłącznie poprawnych transakcji do bloków. Pozwala to użytkownikom opcjonalnie zakładać, że każda transakcja w bloku jest transakcją poprawną.

- Kopanie obecnie skutkuje utworzeniem dla każdego bloku nowych bitcoinów, co przypomina dodruk pieniędzy przez banki centralne. Liczba bitcoinów generowanych dla bloków jest ograniczona i zmniejsza się z czasem zgodnie z ustalonym harmonogramem „emisji" bitcoinów.

Kopanie pomaga znaleźć równowagę między kosztami a zyskami. W tym procesie elektryczność jest używana do rozwiązywania problemu matematycznego. Skuteczny górnik otrzymuje *nagrodę* w postaci nowych bitcoinów i opłat transakcyjnych. Jednak aby otrzymać nagrodę, trzeba poprawnie przeprowadzić walidację wszystkich transakcji zgodnie z regułami uzgadniania *konsensusu*. Ta delikatna równowaga zapewnia bezpieczeństwo bitcoina mimo braku centralnej jednostki nadrzędnej.

Proces kopania został zaprojektowany jako zdecentralizowana loteria. Każdy górnik może stworzyć własny los poprzez utworzenie *bloku kandydującego*, który zawiera nowe transakcje oraz pewne dodatkowe pola danych. Górnik wprowadza swojego kandydata do specjalnego algorytmu, który przekształca („haszuje") dane, generując dane wyjściowe zupełnie niepodobne do wejściowych. Ta *funkcja skrótu* zawsze generuje te same dane wyjściowe dla określonych danych wejściowych — ale nikt nie może przewidzieć, jak będzie wyglądać wyjście dla nowego wejścia, nawet jeśli to wejście różni się tylko nieznacznie od poprzedniego. Jeśli wyjście funkcji skrótu pasuje do szablonu zdefiniowanego przez protokół bitcoina, górnik wygrywa loterię i użytkownicy bitcoina akceptują blok wraz z jego transakcjami jako poprawny. W przeciwnym razie górnik dokonuje niewielkiej zmiany w swoim bloku kandydującym i próbuje jeszcze raz. Kiedy piszę te słowa, liczba bloków kandydujących, które górnicy muszą wypróbować przed znalezieniem zwycięskiej kombinacji, wynosi około 160 miliardów bilionów. Właśnie tyle razy trzeba wykonać funkcję skrótu.

Jednak po znalezieniu zwycięskiej kombinacji każdy może zweryfikować poprawność bloku poprzez wykonanie funkcji skrótu tylko jeden raz. Sprawia to, że poprawny blok jest czymś, czego utworzenie wymaga niewiarygodnej ilości pracy, ale czego weryfikacja jest banalnie prosta. Prosty proces weryfikacji probabilistycznie dowodzi, że praca została wykonana, więc dane wymagane do wygenerowania tego dowodu — w tym przypadku blok — są nazywane *dowodem pracy* (ang. *proof of work*, **PoW**).

Kolejność dodawania transakcji do nowego bloku zależy od wysokości opłaty transakcyjnej i kilku innych kryteriów. Każdy górnik rozpoczyna kopanie nowego bloku zaraz po tym, jak otrzyma z sieci poprzedni blok, co stanowi informację o tym, że poprzednią iterację loterii wygrał ktoś inny. Górnik natychmiast tworzy nowy blok kandydujący z odwołaniem do poprzedniego bloku, zapełnia go transakcjami i rozpoczyna obliczanie Proof-of-Work dla nowego bloku. Każdy górnik dodaje do swojego bloku specjalną transakcję, reprezentującą wypłatę na adres bitcoin określonego górnika nagrody za dany blok i sumy opłat transakcyjnych za wszystkie transakcje z danego bloku kandydującego. Jeśli górnik znajdzie rozwiązanie oznaczające, że jego blok jest prawidłowy, „wygrywa" nagrodę, ponieważ dany blok trafia do globalnego łańcucha, co sprawia, że górnik może wydać środki z transakcji wypłaty nagrody. Górnicy, którzy są członkami kopalni, konfigurują oprogramowanie w taki sposób, aby w nowych blokach nagroda była przesyłana na adres kopalni. Z tego adresu udziały są rozdzielane między górników proporcjonalnie do ilości pracy wykonanej w ostatniej rundzie.

Transakcja Alice trafia do sieci i do puli niezweryfikowanych transakcji. Po stwierdzeniu poprawności transakcji przez węzeł kompletny transakcja ta trafia do nowego bloku kandydującego. Mniej więcej pięć minut po przesłaniu transakcji przez portfel Alice jakiś górnik znajduje rozwiązanie i ogłasza je w sieci. Inni górnicy potwierdzają poprawność zwycięskiego bloku, a następnie zaczynają nową loterię związaną z generowaniem następnego bloku.

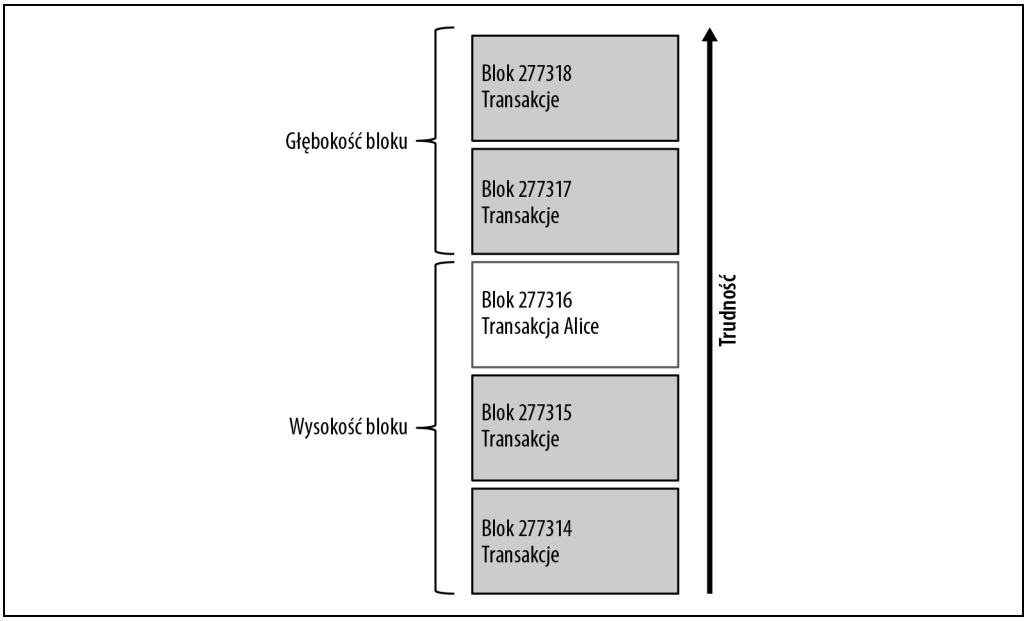
Zwycięski blok z transakcją Alice staje się częścią łańcucha bloków. Blok zawierający transakcję Alice jest liczony jako jedno *potwierdzenie* tej transakcji. Kiedy blok z transakcją Alice zostanie rozesłany po sieci, utworzenie alternatywnego bloku z inną wersją transakcji Alice (na przykład transakcją, która nie opłaca Boba) wymagałoby wykonania takiej samej ilości pracy, jaką wszystkim górnikom bitcoina zajęłoby utworzenie zupełnie nowego bloku. Kiedy do wyboru jest wiele alternatywnych bloków, kompletne węzły Bitcoina wybierają łańcuch poprawnych bloków z największym łącznym dowodem pracy, nazywany *najlepszym łańcuchem bloków*. Aby cała sieć zaakceptowała alternatywny blok, na podstawie tego alternatywnego bloku musiałby zostać wykopany dodatkowy nowy blok.

Oznacza to, że górnicy mają wybór. Mogą pracować z Alice nad alternatywą dla transakcji, w której opłaca ona Boba; być może Alice jest skłonna zapłacić górnikom część pieniędzy, które zapłaciłaby Bobowi. Takie nieuczciwe zachowanie wymagałoby nakładu pracy potrzebnego do utworzenia dwóch bloków. Natomiast górnicy, którzy postępują uczciwie, mogą utworzyć jeden nowy blok i otrzymać wszystkie opłaty za dołączone do niego transakcje plus subwencję za blok. Zwykle nieuczciwość, czyli tworzenie dwóch bloków za niewielką dodatkową opłatę, jest znacznie mniej opłacalna niż uczciwe utworzenie nowego bloku, przez co celowa zmiana potwierdzonej transakcji jest mało prawdopodobna. Dlatego Bob może zacząć zakładać, że płatność Alice jest godna zaufania.

Możesz obejrzeć blok zawierający transakcję Alice (*https://oreil.ly/7v_lH*).

Mniej więcej 19 minut po rozesłaniu bloku zawierającego transakcję Alice inny górnik wykopuje nowy blok. Ponieważ nowy blok jest tworzony na podstawie bloku, który zawierał transakcję Alice (co przekłada się na dwa potwierdzenia transakcji Alice), transakcję tę można teraz zmienić tylko poprzez wykopanie dwóch alternatywnych bloków — i zbudowanie nowego bloku na ich podstawie — a zatem trzeba by było wykopać trzy bloki, żeby Alice odzyskała pieniądze, które wysłała Bobowi. Każdy blok wykopany z uwzględnieniem bloku zawierającego transakcję Alice stanowi dodatkowe potwierdzenie tej transakcji. Wraz z pojawianiem się kolejnych bloków wycofanie transakcji staje się coraz trudniejsze, dlatego Bob jest coraz bardziej pewien, że płatność Alice jest bezpieczna.

Na rysunku 2.7 pokazano blok obejmujący transakcję Alice. Wcześniej znajdują się setki tysięcy bloków powiązanych ze sobą w łańcuch aż do bloku nr 0, czyli *bloku początkowego* (ang. *genesis block*). Wraz ze wzrostem „wysokości" nowych bloków rośnie też trudność obliczeń dla całego łańcucha. Uznaje się, że blok potwierdzony więcej niż sześć razy jest bardzo trudny do usunięcia, ponieważ przeliczenie sześciu bloków (plus utworzenie jednego nowego) wymagałoby bardzo długich obliczeń. Proces kopania i budowania dzięki niemu zaufania jest szczegółowo opisany w rozdziale 12.



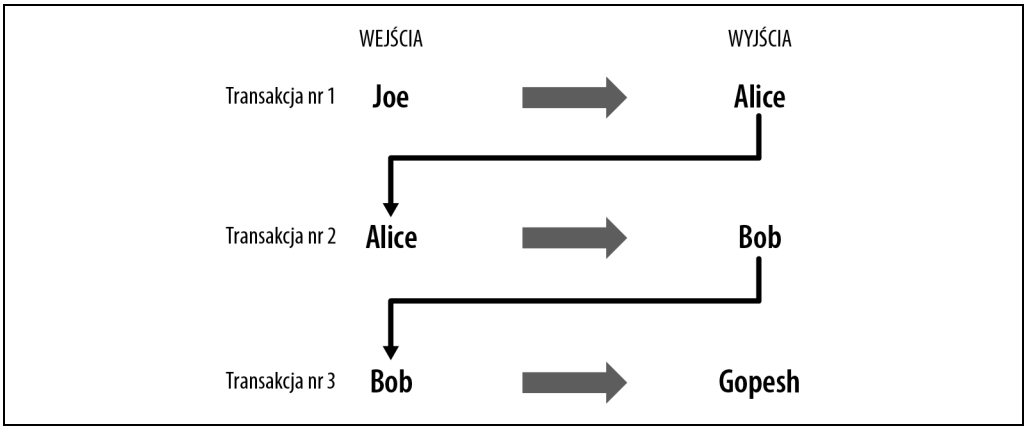
Rysunek 2.7. Transakcja Alice dołączona do bloku

Wydawanie środków z transakcji

Gdy transakcja Alice znajdzie się w łańcuchu jako część bloku, staje się widoczna dla wszystkich aplikacji bitcoina. Każdy kompletny węzeł bitcoina może niezależnie zweryfikować, że transakcja jest prawidłowa i że można wydać przesłane środki. Węzły kompletne weryfikują każde przeniesienie środków od momentu wstępnego wygenerowania bitcoinów w danym bloku przez kolejne transakcje po dotarcie funduszy na adres Boba. Klienty proste mogą przeprowadzić uproszczoną weryfikację płatności poprzez potwierdzenie, że transakcja znajduje się w łańcuchu bloków, a po niej wykopanych zostało już kilka innych bloków. Gwarantuje to, że górnicy ponieśli znaczne nakłady pracy w celu jej zatwierdzenia (zob. punkt „Klienty proste").

Bob może teraz wydać wyjście z danej transakcji (oraz z innych). Może np. zapłacić zleceniobiorcy lub dostawcy, przekazując nowym właścicielom środki z płatności Alice za podcast. Gdy Bob wydaje płatności otrzymane od Alice i innych klientów, przedłuża łańcuch transakcji. Załóżmy, że Bob płaci projektantowi nowej witryny, Gopeshowi. Teraz łańcuch transakcji wygląda tak jak na rysunku 2.8.

W tym rozdziale zobaczyłeś, w jaki sposób transakcje tworzą łańcuch przekazywania wartości między właścicielami. Prześledziłeś też transakcję Alice od momentu jej utworzenia w portfelu przez sieć bitcoina po górników, którzy zarejestrowali transakcję w łańcuchu bloków. W dalszych rozdziałach poznasz konkretne technologie związane z portfelami, podpisami, transakcjami, siecią i kopaniem.



Rysunek 2.8. Transakcja Alice w łańcuchu transakcji od Joego do Gopesha

To podstawowe źródło technicznej wiedzy o bitcoinie. Żadna inna pozycja nie jest tak wyczerpująca ani aktualna!

Olaoluwa Osuntokun, Lightning Labs

W świecie finansów nic nie wywołało takiego poruszenia jak pojawienie się bitcoina. Wprowadzony w 2009 roku, stał się pierwszą zdecentralizowaną cyfrową walutą, co położyło podwaliny pod rynek wart miliardy dolarów. Dodatkowo ujawnił potencjał technologii blockchain, która stanowi fundament kryptowalut. Ogrom możliwości, jakie oferuje bitcoin, sprawia, że znajduje on zastosowanie w licznych branżach. Aby móc w pełni korzystać z jego zalet, należy dokładnie zrozumieć zasady, na których się opiera.

To trzecie, uzupełnione i zaktualizowane wydanie cenionego przewodnika dla każdego, kto chce dołączyć do świata bitcoina, zwanego „internetem pieniędzy". Znajdziesz tu wszelkie kluczowe informacje, podane w jasny, zrozumiały sposób i poparte rzeczywistymi przykładami. Dołączone fragmenty kodu świetnie ilustrują kluczowe koncepcje. To wydanie zawiera mnóstwo najnowszych informacji, w tym opis struktury transakcji, MAST, P2C, wielopodpisów bezskryptowych, a także mechanizmów Taproot i Tapscript. Dzięki lekturze zrozumiesz też tematykę bloków kompaktowych, łańcucha bloków signet, BIP8 i szybkich rozpraw.

Zrozum, co się dzieje „pod maską" bitcoina i jak współdziałają poszczególne elementy tej technologii!

Mark „Murch" Erhardt, Chaincode Labs

W książce:

- solidne podstawy bitcoina i łańcucha bloków
- techniczne aspekty bitcoina i waluty kryptograficznej
- sieć bitcoina, architektura P2P, cykl życia transakcji i kwestie bezpieczeństwa
- najnowsze rozwiązania, w tym Taproot, Tapscript, podpisy Schnorra
- opis nowych, zaawansowanych zastosowań bitcoina

Andreas M. Antonopoulos jest cenionym znawcą technologii łańcucha bloków, przedsiębiorcą, autorem i prelegentem. Posiada dwa patenty z dziedziny sieci i bezpieczeństwa. Ma dar przekazywania skomplikowanych zagadnień w taki sposób, że stają się łatwe do zrozumienia.

David A. Harding jest autorem tekstów technicznych dotyczących oprogramowania open source. Jest też współautorem newslettera Bitcoin Optech i dokumentacji dla deweloperów. Należy do komitetu grantowego Brink.dev.

Helion
helion.pl
HELION S.A.
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-289-1564-0
9 788328 915640
Cena: 99,00 zł