SEKRETY ₿ITCOINA I INNYCH KRYPTOWALUT

Jak zmienić **wirtualne pieniądze** w realne **zyski**

Dominik **Homa**

ØNE press

Helion

Redaktor prowadzący: Magdalena Dragon-Philipczyk
Projekt okładki: Damian Rebuś

Materiały graficzne na okładce zostały wykorzystane za zgodą Shutterstock.

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

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

ISBN: 978-83-283-0364-5

Printed in Poland.

Spis treści

2 Jak działa protokół Bitcoin?

„Moim zdaniem to niesamowite, że w świecie bitcoina algorytm przejmuje funkcje typowe dla [rządu]”.
— Al Gore, były wiceprezydent Stanów Zjednoczonych, laureat Pokojowej Nagrody Nobla

Rozdział ten jest poświęcony problematyce typowo technicznej i opisuje zasady działania protokołu Bitcoin. Zapoznanie się z tymi zasadami nie jest konieczne do zrozumienia dalszej części książki, ale z pewnością może być przydatne. Znajdziesz tu odpowiedzi na wiele pytań i dowiesz się, czym jest *mining*, czyli wydobywanie bitcoinów.

Bitcoin jest protokołem i jako elektroniczny system płatności składa się z trzech elementów:

- kryptografii klucza publicznego,
- sieci *peer-to-peer*,
- dowodu pracy (ang. proof of work).

Protokół to zbiór zasad umożliwiających urządzeniom nawiązanie łączności w celu wymiany informacji. Przykładem takiego protokołu może być np. TCP/IP, który został opracowany, aby możliwe było tworzenie sieci komputerowych.

Dlaczego protokół Bitcoin korzysta z kryptografii? Aby w świecie realnym zabezpieczyć gotówkę, papiery wartościowe itp., wykorzystujemy sejfy, zamki, alarmy czy składamy depozyty w banku. W świecie bitów w celu zabezpieczenia ważnych danych stosujemy kryptografię.

Kryptografia zapewnia bezpieczeństwo między innymi w handlu elektronicznym, np. podczas dokonywania płatności kartami bankowymi. Ma to na celu uniemożliwienie kradzieży lub podszywania się pod kogoś innego.

W jaki sposób informacje przesyłane za pośrednictwem protokołu Bitcoin mogą stać się pieniędzmi? Przyjmijmy, że pewna osoba, np. Paweł, ma walutę cyfrową, którą chce wydać. W świecie cyfrowym, gdzie możemy kopiować pliki, posiadanie waluty cyfrowej stwarza problem, który polega na tym, że wysyłając do kogoś nasze bitcoiny, możemy zachować ich kopię.

Jak zapobiec sytuacji, w której Paweł mógłby wysyłać wielokrotnie te same bitcoiny innym użytkownikom, zapewniając sobie niewyczerpane źródło pieniędzy? W jaki sposób możemy sprawić, aby nie można było podrobić bitcoinów Pawła i używać ich jako należących do innej osoby?

To tylko dwa z wielu problemów, z którymi musi poradzić sobie protokół Bitcoin, aby można było używać informacji jako pieniędzy.

Aby zapewnić ochronę takich pieniędzy przed podrabianiem i kradzieżą, protokół Bitcoin korzysta z kryptografii klucza publicznego.

2.1. Kryptografia klucza publicznego

Kryptografia klucza publicznego oznacza dwa różne klucze: prywatny oraz publiczny.

Idea kryptografii z kluczem publicznym może być obrazowo przedstawiona w następujący sposób. Wyobraźmy sobie, że jesteśmy właścicielem samozatrzaskującej się kłódki i tylko my posiadamy do niej klucz. Taką odblokowaną kłódkę możemy wysłać naszemu znajomemu (odblokowaną kłódką jest klucz publiczny, który w protokole Bitcoin jest adresem naszego portfela).

Nasz znajomy może przy jej użyciu zabezpieczyć przesyłkę (wysłać bitcoiny). Aby to zrobić, nie potrzebuje klucza do kłódki, gdyż wystarczy ją zatrzasnąć.

Tak zabezpieczoną przesyłkę może nadać do nas. Ponieważ posiadamy klucz do kłódki (czyli klucz prywatny), jesteśmy w stanie otworzyć ją i dostać się do zabezpieczonej zawartości. Oczywiście w praktyce nie wykorzystuje się kłódek, tylko odpowiednie formuły matematyczne. Cała ta procedura pozwala w skuteczny sposób uwierzytelniać transakcje pomiędzy węzłami w sieci Bitcoin.

Kluczem publicznym w systemie Bitcoin jest wspomniany nasz adres portfela bitcoinowego. Taki adres możemy wygenerować między innymi w programie zainstalowanym na naszym komputerze, np. w *Bitcoin Wallet* (portfel Bitcoin). Adres Bitcoin składa się z ciągu 34 znaków cyfr i liter i może wyglądać tak:

```
1JgaU5bHHueeTa7jrXBj2aPLGKgbgx6WFy
```

Dany adres naszego portfela jest odpowiednikiem numeru konta bankowego. Jeśli chcemy, aby przesłano do nas bitcoiny, podajemy swój adres. W praktyce wysyłanie bitcoinów jest bardzo proste — wystarczy skopiować adres osoby, której chcemy wysłać bitcoiny, wpisać sumę, jaką chcemy przesłać, i kliknąć „wyślij”.

Aby zrozumieć, co dzieje się w protokole Bitcoin podczas wysyłania bitcoinów i jak działa kryptografia klucza publicznego, posłużę się przykładami. Paweł chce przesłać bitcoiny Markowi, więc pisze do niego wiadomość (podczas wysyłania bitcoinów nie jest konieczne pisanie wiadomości — przedstawiony przykład ma na celu zobrazowanie działania protokołu): „Ja, Paweł, wysyłam Markowi jednego bitcoina". Następnie podpisuje wiadomość podpisem cyfrowym, tj. szyfruje ją prywatnym kluczem kryptograficznym, i obwieszcza ciąg bitów całemu światu.

Marek lub dowolny inny użytkownik może użyć klucza publicznego Pawła, aby sprawdzić, czy osobą, która napisała wiadomość „Ja, Paweł, wysyłam Markowi jednego bitcoina", rzeczywiście był Paweł. Nikt inny nie mógł wygenerować takiego ciągu bitów, więc Paweł nie mógł później zaprzeczyć, mówiąc: „Nie, ja nie wysłałem Markowi jednego bitcoina".

Protokół z wykorzystaniem kryptografii pozwala zatem na ustalenie, iż Paweł naprawdę oświadczył, że wysłał Markowi jednego bitcoina.

Po wyeliminowaniu problemu z duplikacją i kradzieżą pojawia się kolejny kłopot.

Paweł może wysyłać Markowi wielokrotnie ten sam ciąg bitów (monet). Przyjmijmy, że Marek odbiera 10 kopii podpisanych wiadomości „Ja, Paweł, wysyłam Markowi jednego bitcoina".

Aby uniknąć takiej sytuacji, protokół Bitcoin potrzebuje etykiety lub numeru seryjnego każdej transakcji. Paweł pisałby wtedy: „Ja, Paweł, wysyłam Markowi jednego bitcoina z numerem seryjnym 1234567", „Ja, Paweł, wysyłam Markowi jednego bitcoina z numerem seryjnym 7868765" itd. Dzięki temu Marek wiedziałby, że za każdym razem został wysłany inny bitcoin.

Aby taki sposób działał, potrzebujemy zaufanego źródła wydawania numerów seryjnych. Zobaczmy, jak mogłoby to wyglądać, gdyby zaufanym źródłem był bank.

Paweł idzie do banku i mówi: „Chcę pobrać jednego bitcoina ze swojego konta". Bank pomniejsza konto Pawła o jednego bitcoina i przydziela numer seryjny 1234567 do wydanej monety. Wówczas Paweł wysyła wiadomość do Marka: „Ja, Paweł, wysyłam do Marka jednego bitcoina o numerze seryjnym 1234567", ale Marek przed akceptacją przelewu kontaktuje się z bankiem i pyta, czy bitcoin z numerem 1234567 należy do Pawła i czy Paweł nie wydał go już wcześniej.

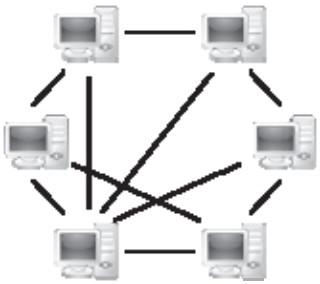
Jeśli obydwa warunki są spełnione, Marek mówi bankowi, że chce zaakceptować transfer bitcoina, a bank aktualizuje swoją bazę informacji, w której zaznacza, że teraz bitcoin o numerze 1234567 należy do Marka.

Wersja takiego rozwiązania jest obiecująca, ale powodowałoby to uzależnienie się od zewnętrznej instytucji, która posiadałaby ogromną władzę. W jaki sposób wykluczyć tę sytuację? Otóż można wykorzystać sieć P2P.

2.2. Sieć P2P (peer-to-peer)

Sieć P2P tworzona jest przez system klientów (programów zainstalowanych na poszczególnych komputerach), które komunikują się bezpośrednio ze sobą jako równorzędne węzły sieci. Oznacza to, że nie ma centralnej jednostki zarządzania i przetwarzania transakcji. Każdy komputer podłączony do sieci P2P jest częścią całości tego systemu.

Obecnie najpopularniejszą implementacją modelu P2P są programy do wymiany plików w internecie, np. BitTorrent, gdzie każdy komputer odgrywa rolę serwera, przyjmując połączenia od innych użytkowników sieci, oraz klienta, wysyłając pliki i (lub) pobierając je bezpośrednio z innych komputerów działających w tej samej sieci P2P. Topologię takiej sieci ilustruje rysunek 2.1.



Rysunek 2.1. Schemat przedstawiający sieć typu P2P

Na takiej samej zasadzie działa sieć Bitcoin, co sprawia, że jest ona zdecentralizowana i nie można jej wyłączyć, ponieważ konieczne byłoby wyłączenie wszystkich tworzących ją komputerów.

Inaczej mówiąc, pomysł polega na tym, aby wszyscy stali się bankiem — kolektywnie w sieci P2P. Czyli każdy użytkownik przechowuje informacje o tym, do kogo należą dane bitcoiny. Ten rejestr nazywa się „łańcuchem bloków" lub „łańcuchem transakcji" (ang. *blockchain*). *Blockchain* to kompletny rejestr wszystkich transakcji, jakie przeprowadzono od początku powstania systemu Bitcoin.

Załóżmy teraz, że Paweł chce wysłać do Marka bitcoina o numerze 1234567. Pojawia się kolejny problem, tzw. „podwójne wydawanie" (ang. *double-spending*), ponieważ Paweł może w tym samym czasie (przed aktualizacją łańcucha transakcji) wysłać bitcoina o numerze 1234567 również Wojtkowi.

To może wydawać się trudne — Marek od razu po otrzymaniu bitcoina może zaktualizować swój łańcuch bloków i ogłosić wszystkim w sieci, także Wojtkowi, że jest posiadaczem bitcoina. Istnieje zatem bardzo krótka chwila, w której Paweł może wielokrotnie wydawać tego samego bitcoina.

Tak czy inaczej, takie rozwiązanie dawałoby możliwość oszukiwania innych. Istnieją również techniki, które mogłyby wydłużyć czas Pawła i umożliwić mu wielokrotne wydawanie tego samego

bitcoina, np. poprzez zerwanie lub wydłużenie komunikacji w systemie pomiędzy Markiem i Wojtkiem.

Z jakiego rozwiązania w takim razie korzysta protokół Bitcoin, aby uniknąć problemu z podwójnym wydawaniem?

Otóż Marek i Wojtek nie próbują aktualizować transakcji samodzielnie, lecz wysyłają wiadomość o możliwości transakcji z Pawłem do całej sieci użytkowników systemu i proszą o rozstrzygnięcie, czy transakcja jest poprawna. Jeśli użytkownicy wspólnie zdecydują, że transakcja jest poprawna, to Marek może zaakceptować wysłanego do niego bitcoina i wszyscy zaktualizują swój łańcuch bloków. To skutecznie rozwiązuje problem z podwójnym wydawaniem bitcoinów. Jeśli Paweł będzie chciał wydać te same bitcoiny kilkakrotnie, to inne osoby w sieci to zauważą i transakcja nie dojdzie do skutku.

W przykładzie wygląda to tak, że Paweł wysyła bitcoina do Marka: „Ja, Paweł, wysyłam Markowi jednego bitcoina z numerem 1234567" i dostarcza podpisaną wiadomość Markowi. Marek zamiast odwoływać się do własnej kopii łańcucha bloków, wysyła informację do całej sieci. Inni użytkownicy sprawdzają, czy Paweł posiada bitcoina o numerze 1234567. Jeśli posiada, to sieć wysyła wiadomość: „Tak, Paweł posiada bitcoina o numerze 1234567; bitcoin ten może być zatem wysłany Markowi". Gdy wiadomość taką wyśle wystarczająca liczba osób, każdy zaktualizuje swój łańcuch bloków, by pokazać, że bitcoin 1234567 należy teraz do Marka, a transakcja została zakończona powodzeniem.

Co to znaczy „wiadomość wyśle wystarczająca liczba osób"? Nie możemy zakładać, że każdy użytkownik sieci wyśle taką wiadomość, ponieważ nie wiemy, kto jest w sieci Bitcoin — nie możemy określić stałej części użytkowników sieci.

Pojawia się kolejne zagrożenie. Paweł mógłby przejąć dużą część sieci Bitcoin, np. poprzez zautomatyzowany system kreujący

dużą liczbę oddzielnych „użytkowników", o których reszta nie wie, że są powiązani.

Podobnie jak poprzednio, Paweł próbuje wysłać swojego bitcoina o numerze 1234567 równocześnie do Marka i Wojtka. Gdy Marek i Wojtek proszą sieć o sprawdzenie poprawności transakcji, Paweł zasypuje sieć informacjami ze swojego zautomatyzowanego systemu, że transakcja jest pozytywna. Marek i Wojtek mogliby więc zostać oszukani.

Istnieje sprytny sposób zapobiegania tego typu sytuacjom. Nazywa się on dowodem pracy (ang. *proof-of-work*).

2.3. Dowód pracy

Dowód pracy zapobiega wielokrotnym przelewom tej samej kwoty do różnych użytkowników. Jest to rodzaj rozproszonego serwera czasowego, który używa łańcuchowych dowodów matematycznych wykonywanych działań. Takie sformułowanie możemy przeczytać w definicji. Ale jak to wygląda w praktyce?

Pomysł ten wymaga skompilowania dwóch rozwiązań, które mogą wydawać się mało intuicyjne.

Po pierwsze, w protokole Bitcoin umyślnie zostało wprowadzone podwyższenie złożoności obliczeniowej, aby zweryfikowanie transakcji w sieci stało się obliczeniowo kosztowne.

Po drugie, sieć Bitcoin wynagradza użytkowników, którzy sprawdzają poprawność transakcji.

To rozwiązanie eliminuje problem z wykreowaniem przez Pawła dużej liczby kontrolowanych przez niego użytkowników sieci, ponieważ każdy z nich musiałby dysponować dużą mocą obliczeniową. Aby oszustwo mogło się powieść, wymagałoby niewyobrażalnie dużej mocy obliczeniowej, co czyni je nieekonomicznym lub nierealnym.

Aby lepiej przybliżyć dowód pracy, posłużę się przykładem.

Paweł wysyła do Marka bitcoina: „Ja, Paweł, wysyłam do Marka jednego bitcoina o numerze 1234567". Gdy ta informacja zostaje przekazana do sieci, pojawia się automatycznie u każdego użytkownika i trafia do kolejki, w której trzymane są wykonywane transakcje, ale które nie zostały jeszcze zaakceptowane przez sieć.

Na przykład kolejka Kuby, jednego z użytkowników sieci, może wyglądać tak:

Ja, Kuba, wysyłam Agnieszce jednego bitcoina o numerze 1357910.

Ja, Mateusz, wysyłam Weronice jednego bitcoina o numerze 3465021.

Ja, Paweł, wysyłam Markowi jednego bitcoina o numerze 1234567.

Kuba sprawdza poprawność transakcji z własną kopią łańcucha bloków i chce rozesłać wiadomość o poprawności tych transakcji do całej sieci. Jednak zanim będzie mógł to zrobić, będzie musiał rozwiązać trudną zagadkę matematyczną, nazwaną „dowodem pracy". Bez rozwiązania tej zagadki reszta sieci nie zaakceptuje jego pozytywnej weryfikacji transakcji.

Przyjrzyjmy się bliżej temu, na czym polega rozwiązywanie tej matematycznej zagadki.

2.4. Funkcja skrótu

Zacznijmy od wyjaśnienia, czym jest *funkcja skrótu*, inaczej: funkcja mieszająca lub funkcja haszująca. Jest to funkcja, która przyporządkowuje dowolnej wiadomości krótką wartość, zwykle posiadającą stały rozmiar (skrót wiadomości).

W informatyce funkcje skrótu pozwalają na ustalenie krótkich i łatwych do weryfikacji sygnatur dla dowolnie dużych zbiorów

danych. Takie sygnatury mogą chronić przed przypadkowymi lub celowo wprowadzonymi modyfikacjami danych, czyli pozwalają sprawdzić, czy zbiory pobrane z internetu są w oryginalnej postaci.

Bitcoin używa znanej funkcji skrótu SHA-256 (ang. *Secure Hash Algorithm*).

W jaki sposób ta funkcja skrótu haszuje? Posłużmy się przykładem. Powiedzmy, że funkcję skrótu oznaczymy jako `h`, a kolejkę Kuby z oczekującymi transakcjami nazwiemy `K` i przypiszemy jej wartość `K = "Kolejka"`. Kuba dodaje do kolejki numer `x=0` i haszuje kombinację.

```
h("Kolejka0") = 30dd4761a8bc8c4c7d6dbbbdb3ba7627734
ee02d983096cc698b89aa578bcf94
```

(Liczba wyjściowa jest zapisywana w systemie szesnastkowym).

Zagadka (dowód pracy), którą Kuba musi rozwiązać, polega na znalezieniu takiego `x`, by po dodaniu go do `K` i haszowaniu kombinacji wyjście zaczynało się w tym przykładzie od odpowiedniej liczby zer. Relatywnie prosty dowód pracy może wymagać trzech lub czterech zer na początku liczby, a bardziej złożony — o wiele dłuższej ich sekwencji.

W naszym przykładzie oznaczałoby to porażkę, ponieważ gdy `x=0`, wyjście funkcji nie zaczyna się zerem. Próba z `x=1` również nie przynosi pozytywnych rezultatów.

```
h("Kolejka1")=6c8cc2be495540c0c41c409dad55c3706ed49
bd4fb162ea3e4c5749c635a29fa
```

Po kolejnych próbach dla `x= 2,3,...` w końcu dla `x=10` otrzymujemy:

```
h("Kolejka10")=0e717707c2d4d6912737d4e83e3161805730
b82e4a3068381053d3eed1d8e90c
```

Wyjście funkcji zaczyna się od jednego `0`, ale żeby rozwiązać prosty dowód pracy, wyjście z funkcji haszującej powinno zaczynać

się ciągiem np. czterech 0. Jednak taki wynik nie będzie wystarczający, by rozwiązać jeszcze trudniejszy dowód pracy.

Rozwiązywanie zagadki utrudnia fakt, że wyjście z kryptograficznej funkcji haszującej zachowuje się jak liczba losowa — zmiana na wejściu chociażby jednego bita powoduje całkowitą zmianę wartości wyjściowej w sposób, który trudno przewidzieć. Jeśli więc chcemy mieć na wyjściu funkcji haszującej wartość zaczynającą się od 10 zer, Kuba będzie musiał średnio wypróbować $16^{10} \sim 10^{12}$ różnych kombinacji dla x, zanim znajdzie odpowiednią liczbę zer. To bardzo wymagające zadanie, do którego rozwiązania potrzebna jest ogromna moc obliczeniowa.

Oczywiście jest możliwe ustalanie stopnia trudności zagadki — poprzez wymaganie większej lub mniejszej liczby zer na wyjściu funkcji haszującej.

W rzeczy samej, system Bitcoin gwarantuje dobrą kontrolę nad trudnością zagadki przez zastosowanie małej modyfikacji w powyżej opisanym przykładzie metody dowodu pracy.

Zamiast na wymaganiu odpowiedniej liczby zer zagadka opiera się na tym, by hash nagłówka bloku był równy numerowi znanemu jako cel albo mniejszy. Ten cel jest automatycznie dostosowywany przez system w odniesieniu do mocy obliczeniowej całej sieci, by średnio potwierdzenie bloków Bitcoina wymagało 10 minut.

Wracając do przykładu, przypuśćmy, że Kuba znalazł odpowiednie x, które daje mu pożądaną liczbę zer na początku. Wysyła on wtedy swój blok do sieci razem z odpowiednią znalezioną wartością x. Inni uczestnicy sieci mogą zweryfikować, że x jest poprawnym rozwiązaniem zagadki będącej dowodem pracy. Wówczas wszyscy aktualizują własne łańcuchy bloków, dodając nowy blok transakcji.

Pojawia się kolejny problem. Bez odpowiedniej zachęty nikt nie będzie chciał weryfikować transakcji poprzez udostępnianie

swojej mocy obliczeniowej, by pomagać potwierdzać transakcje innych osób.

W protokole Bitcoin ten proces potwierdzania nazywany jest **kopaniem** (ang. *mining*).

Każda osoba, która zweryfikowała blok transakcji, otrzymuje od systemu ustaloną liczbę bitcoinów jako zapłatę. Wszystkie bitcoiny, które są w obiegu, powstały właśnie w taki sposób, czyli jako nagrody za potwierdzanie transakcji.

System z puli 21 mln uwalnia kolejne bitcoiny; gdy powstawała ta książka, było uwolnionych 13 mln bitcoinów.

Na początku z każdego bloku transakcji uwalniano 50 bitcoinów. Po każdych 210 000 zweryfikowanych bloków (w przybliżeniu jest to co 4 lata) uwalniana nagroda jest zmniejszana o połowę. W historii systemu Bitcoin taka redukcja nagrody odbyła się już jeden raz i z początkowej nagrody 50 bitcoinów za blok spadła do 25 bitcoinów.

Takie zmniejszanie nagrody mniej więcej co 4 lata będzie kontynuowane do około 2140 roku. Wartość ostatniej nagrody spadnie wtedy poniżej 10^{-8} bitcoina za blok, czyli poniżej najmniejszej części bitcoina, nazwanej satoshi, odpowiednika jednego grosza (z tym że wartość 1 grosza to 0,01 złotego, a wartość 1 satoshi — 0,00000001 bitcoina).

Około 2140 roku podaż przestanie rosnąć, jednak nie spowoduje to eliminacji zachęty na potwierdzanie transakcji, ponieważ w protokole Bitcoin zastosowano możliwość ustalenia prowizji za transakcje trafiające do „górników", którzy pomagają je weryfikować.

Prowizje za transakcje początkowo wynosiły 0, ale kiedy bitcoin zdobył popularność, stopniowo rosły i gdy powstawała ta książka, wynosiły około 0,0001 BTC za jedną transakcję. Co to oznacza dla zwykłego użytkownika? W sieci Bitcoin opłaty za transakcje są

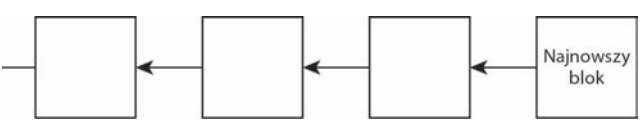
dobrowolne. Jeśli zaakceptujemy niską opłatę za naszą transakcję, zostanie ona zrealizowana szybciej niż ta, która nie ma opłaty.

Każda transakcja powoduje wpis, który potrzebuje odrobinę mocy obliczeniowej. Górnicy poprzez swoje dowody pracy konkurują ze sobą w szybkości potwierdzenia transakcji. Generalnie każdy górnik ma możliwość wygrania tej konkurencji na poziomie zależnym od tego, ile (procentowo) dostarcza mocy obliczeniowej. Powiedzmy, że dany górnik dostarcza 1% mocy obliczeniowej całej sieci, ma zatem 1% szansy na wygranie konkurencji i tym samym otrzymanie nagrody. Jeśli mu się to nie uda, przy wydobywaniu następnych bloków będzie miał kolejną możliwość.

Rozwiązanie to powoduje, że przy dużej mocy obliczeniowej oraz przy sporej konkurencji nieuczciwy górnik będzie miał małe szanse, aby zakłócić potwierdzanie transakcji.

Ważną sprawą w działaniu protokołu Bitcoin jest kolejność, w której przeprowadzane są transakcje. Jeśli sieć Bitcoin nie miałaby tego typu porządkowania, to w danym momencie mogłoby być niemożliwe określenie, do kogo należy dany bitcoin.

W protokole Bitcoin każdy nowy blok zawiera wskaźnik (hash wcześniejszego bloku) do ostatnio zweryfikowanego bloku w łańcuchu. Wskaźnik ten jest dodawany do zatwierdzonych już transakcji. Więc łańcuch bloków (*blockchain*) to liniowy łańcuch transakcji; bloki są ułożone jeden po drugim, przy czym ostatni z nich zawiera wskaźniki bloku wykonanego bezpośrednio przed nim. Schemat takiego liniowego łańcucha transakcji prezentuje rysunek 2.2.



Rysunek 2.2. Najnowszy blok wygenerowany z haszem bloku poprzedniego

Bitcoin — waluta przyszłości!

- **U progu wielkiej zmiany, czyli po co komu kryptowaluty**
- **Portfele i transakcje, czyli skąd wziąć bitcoina i jak nim obracać**
- **Na własnym podwórku, czyli jak przyjmować płatności we własnej firmie**
- **Prawo w Polsce i na świecie, czyli co należy wiedzieć o aspekcie prawnym bitcoina**

Wirtualna waluta bitcoin, choć nadal jest mało popularnym międzynarodowym środkiem płatniczym, budzi spore emocje. Jej możliwości są naprawdę oszałamiające! Nie podlega kontroli żadnego rządu ani instytucji finansowej, można ją zdobyć i pomnażać niezależnie od miejsca zamieszkania i wymieniać z innymi entuzjastami, a nawet zamienić na twardą walutę i wypłacić w bankomacie!

Ta książka ma za zadanie ułatwić Ci zorientowanie się w świecie bitcoina i innych kryptowalut. Autor nie ukrywa, że jego osobiste doświadczenia z tą walutą nie zawsze były pozytywne. Jest jednak pewien, że bitcoin to klucz do rewolucji na polu transakcji finansowych. Dowiedz się więc, czym dokładnie jest bitcoin, na jakich podstawach się opiera i jak się nim posługiwać. Zrozum, dlaczego ma zagorzałych zwolenników i równie zaciekłych przeciwników, co stanowi o jego sile i co go blokuje. Poznaj walutę przyszłości i przygotuj się na wielką zmianę!

Dominik Homa
jest absolwentem Wyższej Szkoły Informatyki i Zarządzania w Rzeszowie. Od 10 lat z powodzeniem prowadzi własną działalność gospodarczą z dziedziny IT; firmę założył jeszcze na studiach. Jest zapalonym eksploratorem internetu i nowych technologii, uczestniczy w licznych konferencjach i spotkaniach startupowych oraz związanych z tematyką kryptowalut. Jest twórcą strony akademiabitcoin.pl, aktywnym minerem i traderem, a także zwolennikiem wychodzenia poza schematy myślowe w wielu dziedzinach życia. Swoimi przemyśleniami dzieli się na stronie dominikhoma.com. Jest współautorem książki *Prawo w e-biznesie* (Onepress, 2015).

Patroni:

one press

Sprawdź najnowsze promocje: http://onepress.pl/promocje
Książki najchętniej czytane: http://onepress.pl/bestsellery
Zamów informacje o nowościach: http://onepress.pl/nowosci

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: onepress@onepress.pl
http://onepress.pl

cena: 34,90 zł

ISBN 978-83-283-0364-5

9 788328 303645

Helion