Marcin Szymankiewicz

₿ITC0IN

Wirtualna waluta internetu

one press
Helion

Redaktor prowadzący: Barbara Gancarz-Wójcicka
Projekt okładki: Jan Paluch

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?bitcoi
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-246-8099-3

Printed in Poland.

Spis treści

Rozdział 2.

Zasada funkcjonowania bitcoina

Jak funkcjonuje bitcoin?

Aby zrozumieć ideę bitcoina, trzeba poznać chociaż część teoretycznych podstaw jego funkcjonowania. W tym rozdziale poruszymy sporo kwestii technicznych, aby przybliżyć w jak najprostszy sposób używane w dalszej części książki pojęcia bloku, wydobywania czy transakcji. Ponieważ sporo operacji w sieci Bitcoin opiera się na kryptografii, nie sposób również omówić zasady działania wirtualnej waluty bez przybliżenia podstawowych pojęć z tej dziedziny.

Kryptografia

Słowo „kryptografia" odmieniane jest przez wszystkie przypadki w rozmaitych definicjach bitcoina. Nic dziwnego, w końcu to właśnie algorytmy szyfrujące i działania matematyczne stanowią podstawę działania wirtualnej waluty. Mimo że większość informacji, jak chociażby historia transakcji, jest jawna, szyfrowanie odgrywa kluczową rolę w zabezpieczeniach mechanizmów bitcoina. Kryptowaluta, jak nieraz zwany jest bitcoin, korzysta przede wszystkim z kryptograficznych funkcji skrótu oraz kryptografii klucza publicznego.

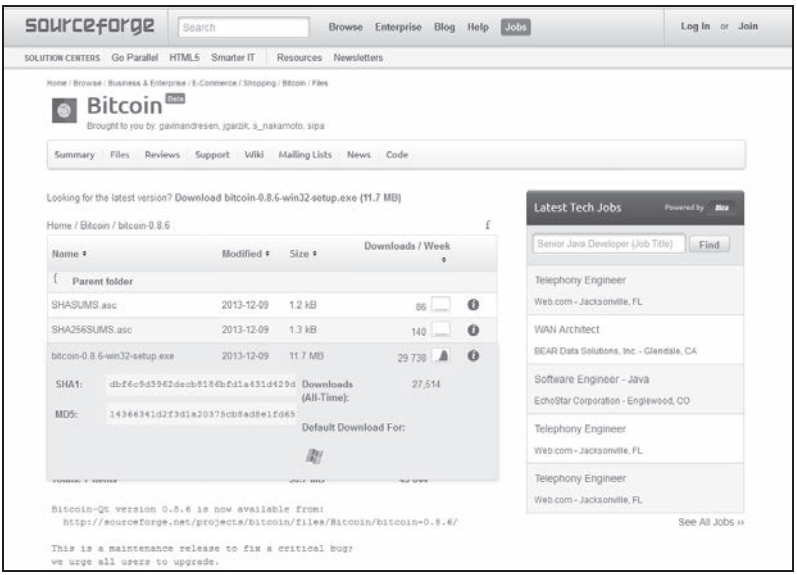
Funkcje skrótu (ang. hash function)

Funkcja skrótu, zwana także funkcją haszującą, jest algorytmem komputerowym, uruchamianym na pewnych danych wejściowych. Wynikiem działania tej funkcji jest skrót (hash) o stałej długości. Dla przykładu znana i popularna w internecie funkcja MD5 generuje skrót o stałej, 32-znakowej długości, składający się ze znaków 0 – 9 oraz a – f. Spróbujmy wywołać taką funkcję dla przykładowych danych wejściowych, czyli ciągu „Bitcoin2013". Możemy tego dokonać między innymi w licznych generatorach online lub w systemie operacyjnym Linux, używając komendy `md5sum`. W obu przypadkach otrzymamy taki sam skrót, widoczny na rysunku 2.1.

Rysunek 2.1. Jeden z popularnych w internecie generatorów hashy

Obliczenie jednego hashu MD5 jest bardzo szybkie. W teście przeprowadzonym na przykładowej maszynie klasy domowego komputera PC 1000 hashy MD5 obliczanych było w przeciągu 1,246 sekundy, co daje przybliżoną prędkość 803 hashy na sekundę.

Funkcja haszująca ma zawsze taki sam wynik dla tych samych danych wejściowych i często możemy spotkać się z nią przy pobieraniu plików z internetu. Obok nazwy pliku znajduje się zapisany hash. Na pobranym pliku możemy wywołać funkcję haszującą na lokalnym dysku i sprawdzić, czy zwróciła ona taki hash, jaki widnieje na stronie internetowej. Dzięki temu zyskujemy pewność, że plik został pobrany w całości i nie został po drodze zmodyfikowany (rysunek 2.2).



Rysunek 2.2. Strona pobrań klienta Bitcoin-qt na sourceforge.net. Obok pliku wykonywalnego EXE widnieją hashe SHA1 oraz MD5, które można wykorzystać do weryfikacji pliku po pobraniu

Funkcja skrótu jest jednostronna, ponieważ na podstawie hashu nie jesteśmy w stanie odtworzyć danych wejściowych, które posłużyły do jego wygenerowania. Poza nielicznymi przypadkami, które zostaną omówione na końcu tej sekcji, odtworzenie źródłowych danych jest często niemożliwe w zadowalającym czasie.

Dobrze znane funkcje skrótu to wspomniana już MD5 czy SHA-256, które generują odpowiednio 32- i 64-znakowy skrót, używając znaków heksadecymalnych (cyfry 0 – 9 oraz litery a – f). W projekcie Bitcoin wykorzystywana jest ta druga funkcja, ze względu na to, że funkcja MD5 jest już raczej przestarzała i nie może zapewnić odpowiedniego poziomu bezpieczeństwa.

Dla wymienionych wyżej funkcji skrótu bardzo mała zmiana w źródłowym zbiorze danych spowoduje, że wynikowy hash będzie zupełnie inny niż oryginalny. Taki mechanizm pozwala upewnić się, że obrabiany zbiór danych, którym może być tekst, plik lub

też blok transakcji bitcoina, nie został zmieniony przez nieuprawnionego użytkownika. Przyjrzyjmy się, jak wygląda to na bardzo prostym przykładzie. Obliczymy skrót SHA-256 dla wyrażeń „Ala ma kota" oraz „Ola ma kota". Te dwa zdania różnią się tylko jednym znakiem — w pierwszym z nich występuje duża litera A, w drugim duża litera O. Skrót można obliczyć z wykorzystaniem polecenia linuksowego `sha256sum`, jak również innych programów bądź generatorów online. Oto obliczony skrót SHA-256 z dwóch różnych wyrażeń:

„Ala ma kota"
```
124bfb6284d82f3b1105f88e3e7a0ee02d0e525193413c05b75041917022cd6e
```

„Ola ma kota"
```
36ad917e863b5321bff77734fd52888ccf03c503bd51f649cb1ed4c28a19e5ef
```

Oba hashe mają kompletnie inną wartość i w żaden sposób nie zdradzają, że pochodzą z tak bardzo zbliżonych do siebie wejściowych łańcuchów znaków.

W sieci Bitcoin funkcje skrótu używane są między innymi przy obliczaniu adresu Bitcoin, który wynika bezpośrednio z powiązanego z nim klucza prywatnego. Dzięki nieodwracalnemu działaniu funkcji haszujących udostępnienie swojego adresu Bitcoin publicznie nie pociąga za sobą ryzyka poznania związanego z nim klucza prywatnego. Z drugiej strony dzięki łatwemu obliczaniu hashu z zadanego łańcucha wejściowego użytkownik posiadający klucz prywatny jest w stanie bardzo szybko dowieść, że dany adres Bitcoin należy właśnie do niego. Funkcje haszujące używane są także do obliczania sum kontrolnych bloków transakcji oraz w celu zapewnienia integralności łańcucha bloków, co będzie opisane w dalszej części książki.

Wirtualny pieniądz — praktyczne zastosowanie

Zanim na świecie pojawiły się pieniądze, w handlu dominowała wymiana towarowa. Była ona jednak dość niewygodna, więc już w VII wieku p.n.e. złotnicy i kupcy zaczęli wybijać z drogocennych kruszców monety przeznaczone do płacenia za towar. Ten pomysł szybko podchwycili władcy poszczególnych państw i miast. Bitego pieniądza używamy do dziś, ale wraz z rozwojem internetu część rozliczeń przenieśliśmy do sieci. Powstanie wirtualnej waluty było nieuniknione — VEN, pierwszy popularny, samodzielny e-pieniądz, pojawił się w serwisie Facebook w 2007 roku. W 2009 roku za sprawą Satoshiego Nakamoto na scenę finansów wkroczył bitcoin — anonimowa, niezależna waluta, oparta na korzystającej z niej społeczności, algorytmie kryptograficznym oraz modelu peer-to-peer. Waluta ta występuje w ograniczonej liczbie 21 mln sztuk wydobywanych przez użytkowników bitcoina.

Książka *Bitcoin. Wirtualna waluta internetu* to synteza wiedzy na temat wirtualnego pieniądza. Na początku autor wprowadza czytelnika w świat pieniądza — od jego historii do czasów obecnych. Wspomina, gdzie możemy spotkać się z walutą bitcoin. Następnie przedstawia zasady, na jakich działa bitcoin: jak jest wymieniany, zapisywany i rozpowszechniany. Kolejny rozdział to praktyka wirtualnej waluty: opisano tu przechowywanie, transakcje, metody pozyskiwania e-pieniądza. Spora część publikacji została poświęcona bezpieczeństwu w świecie wirtualnym, czyli prywatności użytkowników waluty, obronie przed cyberprzestępcami i kwestii nielegalnych transakcji przy użyciu bitcoina.

Marcin Szymankiewicz — absolwent informatyki na Politechnice Poznańskiej, specjalista do spraw bezpieczeństwa IT w międzynarodowej korporacji. Entuzjasta sieci komputerowych i bezpieczeństwa IT. Zainteresował się bitcoinem podczas konfigurowania koparki obsługiwanej przez system Linux. Wcześniej pracował jako programista i menedżer projektów informatycznych. Prowadził też własną działalność.

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

Helion

Cena 29,90 zł
ISBN 978-83-246-8099-3
9 788324 680993