Bitcoin: złoto XXI wieku

Łukasz MAZUREK[*]

Czym jest Bitcoin? Najkrótsza odpowiedź na to pytanie brzmi: *kryptowalutą*. Ale nie w takim sensie *krypto-*, jak w słowie *kryptoreklama*. Pierwszy człon tego terminu pochodzi od kryptologii, czyli nauki kojarzącej nam się głównie z szyframi i maszyną szyfrującą Enigma używaną przez Niemców podczas wojny. To właśnie twierdzenia i konstrukcje z tej dziedziny stoją za funkcjonowaniem i bezpieczeństwem Bitcoina.

Pomysły na wprowadzenie cyfrowej alternatywy dla tradycyjnych walut sięgają lat osiemdziesiątych ubiegłego wieku. Jednak dopiero w 2009 roku Satoshiemu Nakamoto udało się stworzyć system, który przyciągnął miliony użytkowników wykonujących dziennie 100 000 transakcji o łącznej wartości przekraczającej 100 milionów dolarów. Co takiego zadecydowało o tym, że zaufaliśmy Bitcoinowi? Czy naprawdę potrzebowaliśmy kryptowaluty? Przecież bezpieczeństwo tradycyjnych systemów bankowych też opiera się na kryptologii – ze stroną internetową banku łączymy się połączeniem szyfrowanym, dostęp do konta jest zabezpieczony hasłem, karty płatnicze mają chip, który uniemożliwia ich skopiowanie... Czyż nasze pieniądze nie są bezpieczne? Oczywiście, że są. Pod warunkiem, że bank nie postanowi np. zabrać nam części oszczędności lub ograniczyć możliwości wypłaty, jak to niedawno miało miejsce w wyniku kryzysu na Cyprze i w Grecji. Gdyby walutą obowiązującą w tych krajach był bitcoin, do takich sytuacji nie mogłoby dojść. O sukcesie Bitcoina zadecydowało wcale nie to, że transakcje są tanie i szybkie, ale przede wszystkim to, że jest to pierwsza waluta całkowicie zdecentralizowana, tj. pozbawiona centralnego emitenta, który mógłby np. dodrukowywać pieniądze, kontrolować nasze konta, czy w inny sposób wpływać na działanie systemu.

Przelew bitcoinów w dowolne miejsce na świecie kosztuje około 20 gr, zajmuje około 10 minut i nie wymaga zakładania żadnego konta. Bitcoiny można łatwo kupić na giełdach, a nawet gdzieniegdzie w bankomatach. Można je też *wydobyć* jako *górnik*.

Skoro nikt tego interesu nie pilnuje, to jakim cudem to wszystko działa i do tego jeszcze jest bezpieczne? Otóż to nie jest do końca tak, że Bitcoina nikt nie kontroluje. Należałoby raczej powiedzieć, że Bitcoina kontrolują wszyscy użytkownicy (dokładniej: wszyscy użytkownicy, którzy są *górnikami*, ale o tym za chwilę). I właśnie to rozproszenie odpowiedzialności pomiędzy użytkowników sprawia, że możemy czuć się bezpiecznie. Upraszczając sprawę, można powiedzieć, że aby z Bitcoinem stało się coś złego, musiałaby się zmówić ponad połowa jego użytkowników. Na szczęście taki scenariusz wydaje się mało prawdopodobny – większość z nich ma swój interes w tym, aby system działał prawidłowo.

Skąd się bierze wartość pojedynczego bitcoina? Terminy *wydobywanie* i *górnik* (używane w dalszej części artykułu) sugerują podobieństwo do złota. Podobnie jak w przypadku tego szlachetnego kruszcu bitcoiny trudno się wydobywa, a ich zasoby na świecie są ograniczone. Te cechy zupełnie wystarczają – z punktu widzenia ekonomii – do umówienia się, że Bitcoin jest pełnoprawnym środkiem płatniczym. (Choć tak naprawdę odzwierciedla on nic więcej, jak tylko dowód na wykonanie pewnej znacznej pracy obliczeniowej.)

Jak dokładnie działa Bitcoin? Spróbujmy odtworzyć rozumowanie Satoshiego Nakamoto, które doprowadziło go do skonstruowania tego systemu.

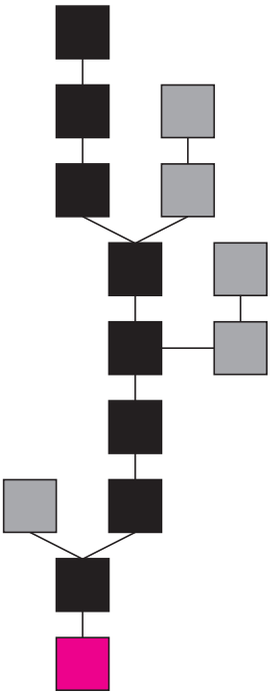
W cyfrowej walucie posiadanie pieniędzy odzwierciedlone jest przez znajomość pewnego ciągu zer i jedynek. Taki ciąg można łatwo skopiować – jak więc zapobiec sytuacji, w której pewna moneta zostałaby wydana dwa razy? W Bitcoinie problem ten jest rozwiązany przez jedną powszechnie dostępną księgę transakcyjną, w której zapisane są kolejno wszystkie transakcje, które zostały wykonane od początku istnienia systemu. I tu dochodzimy do sedna, czyli do pytania, jak utrzymać funkcjonowanie takiej księgi, nie powołując w tym celu centralnej instytucji za to odpowiedzialnej? Tym właśnie zajmują się *górnicy*.

Wbrew powszechnej opinii użytkownicy Bitcoina nie są anonimowi. Wręcz przeciwnie! Ten system jest w pełni transparentny – każdy ma wgląd w historię wszystkich transakcji i może dokładnie prześledzić przepływ gotówki w sieci.

Aby zostać górnikiem, wystarczy mieć komputer z wystarczającą ilością miejsca na przechowanie lokalnej kopii księgi transakcyjnej. Księga ta ma strukturę *łańcucha bloków* i aktualnie składa się z około 400 000 bloków transakcji i zajmuje około 60 GB. Wydobywanie bitcoinów polega na rozwiązywaniu pewnej zagadki matematycznej związanej z transakcjami, które pojawiły się w sieci od czasu opublikowania ostatniego bloku. Na tego, kto pierwszy rozwiąże zagadkę, czeka niemała nagroda – w latach 2016–2019 ma ona wynosić 12,5 bitcoina, czyli około 20 000 zł. Aby odebrać nagrodę, zwycięzca *publikuje wydobyty blok*, tzn. rozsyła do całej sieci nowy blok zawierający: rozwiązanie

Wraz z opublikowaniem nowego bloku w sieci pojawia się 12,5 nowych bitcoinów przeznaczonych na nagrodę dla górnika, który go wydobył (ta kwota maleje dwukrotnie co około 3 lata, przez co łączna ilość bitcoinów jest ograniczona). Poza tą nagrodą zwycięzca otrzymuje również wszystkie opłaty transakcyjne z tego bloku, co stanowi motywację, aby górnicy uwzględniali w swoich blokach wszystkie transakcje krążące po sieci, a nie publikowali np. bloków z pustą listą transakcji.

[*]Instytut Informatyki, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski



zagadki, listę nowych transakcji w sieci oraz specjalną transakcję przelewającą wydobyte bitcoiny na swoje konto. Następnie każdy z górników sprawdza, czy rozwiązanie zagadki podane przez zwycięzcę jest prawidłowe, po czym wydłuża swoją kopię łańcucha bloków o blok zwycięzcy.

W tym momencie uważnego Czytelnika może zaniepokoić założenie, że wszyscy górnicy bezwarunkowo akceptują nowy blok (o ile tylko zwycięzca nie oszukał z rozwiązaniem zagadki) i tym samym akceptują wypłatę nagrody dla zwycięzcy. Nietrudno wyobrazić sobie złośliwego górnika, który nie zamierza godzić się z wypłatą nagrody komu innemu. Taki górnik może postanowić, że nie uzna ostatniego wydobytego bloku i będzie kontynuował rozwiązywanie starej zagadki, tj. będzie próbował dobudować swój blok do przedostatniego bloku z łańcucha uznawanego przez resztę sieci i tym samym doprowadzić do rozgałęzienia łańcucha. Jednak w Bitcoinie nie mogą istnieć równolegle dwie wersje wydarzeń – w przypadku rozgałęzienia łańcucha za poprawną uznawana jest zawsze dłuższa z gałęzi. Zatem, aby złośliwy górnik mógł wykorzystać nagrodę za swój blok, musiałby sam zbudować dłuższy łańcuch niż cała reszta uczciwych górników pracujących razem. Dlatego na początku artykułu pisałem, że *musiałaby się zmówić ponad połowa użytkowników*. Z tego względu każdemu górnikowi opłaca się akceptować wszystkie bloki publikowane przez konkurencję i zawsze pracować na najdłuższym znanym łańcuchu.

Zagadka, którą rozwiązują górnicy, brzmi następująco:

Mając dane: B – *ostatni opublikowany blok oraz* L – *listę transakcji, które pojawiły się w sieci od czasu opublikowania bloku* B, *znajdź takie* x, *że* $H(B, L, x) < 2^m$, *gdzie* H *to pewna* (*znana*) *funkcja haszująca, która zwraca wartość całkowitą z przedziału* $[0, 2^n - 1]$ *z rozkładem jednostajnym, a* m *to pewna liczba mniejsza od* n *zwana* ***trudnością***.

Funkcja H zachowuje się losowo – górnicy sprawdzają więc kolejno różne wartości x w nadziei, że trafią na wynik funkcji mniejszy niż 2^m. Zauważmy, że im mniejsze m, tym zagadka jest trudniejsza (prawdopodobieństwo sukcesu w pojedynczej próbie wynosi $2^m/2^n$), dlatego zmieniając m, można regulować czas, jaki jest potrzebny, aby ktoś w sieci ją rozwiązał. Wygląda na łatwy sposób zarobienia pieniędzy? Nasz komputer coś sobie liczy – tak naprawdę rzuca kostką i sprawdza, czy trafił – i jak trafi, to wygrywa. 20 000 zł do wygrania co 10 minut, taka loteria. Trzeba jednak pamiętać, że moc obliczeniowa zwykłego komputera jest około 10^{11} razy mniejsza niż moc całej sieci Bitcoina, więc szansa, że to akurat my wydobędziemy najbliższy blok, jest niesłychanie mała. Dlatego do wydobywania bitcoinów wykorzystuje się specjalnie do tego celu stworzone urządzenia, tzw. *koparki bitcoinów*, które osiągają o wiele większą moc obliczeniową od zwykłych komputerów. Poza tym górnicy łączą swoje siły, pracując w *kopalniach* – wspólnie rozwiązują tę samą zagadkę, a ewentualną wygraną dzielą się proporcjonalnie do swojego wkładu w wykonaną pracę.

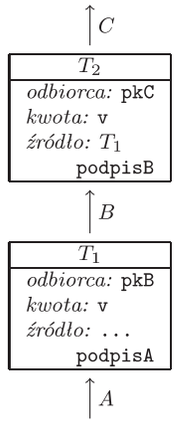
Zgodnie z protokołem Bitcoina parametr m jest co dwa tygodnie dostosowywany do aktualnej łącznej mocy obliczeniowej wszystkich górników, tak aby wydobycie nowego bloku zajmowało całej sieci średnio około 10 minut.

Jaki to ma związek z kryptologią? Rolę funkcji H pełni w Bitcoinie znana funkcja haszująca SHA-256. Kryptolodzy wierzą (choć nikt tego nie udowodnił), że funkcja ta zachowuje się na tyle losowo, że nie jesteśmy w stanie przewidzieć, dla jakich argumentów jej wartość będzie mniejsza od 2^m, a dla jakich większa. Nawet znajomość wartości tej funkcji obliczonych wcześniej dla milionów różnych argumentów w żaden sposób nie ułatwia nam odpowiedzi na pytanie, jaka będzie wartość dla kolejnego argumentu. Dlatego wierzymy, że nie ma *sprytniejszych* użytkowników, którzy by lepiej zgadywali rozwiązania zagadki, i prawdopodobieństwo wygranej jest zawsze proporcjonalne do ilości wykonanej pracy, bez względu na to, w jakiej kolejności testujemy kolejne wartości x.

Kolejnym elementem Bitcoina, w którym nie obyłoby się bez kryptologii, są transakcje. Transakcja w Bitcoinie pełni rolę przelewu kwoty v między użytkownikami A i B. Spodziewalibyśmy się więc, że opis transakcji będzie wyglądał mniej więcej tak: {*nadawca*: A, *odbiorca*: B, *kwota*: v}.
W rzeczywistości sytuacja jest trochę bardziej skomplikowana – każdy użytkownik posiada swój tajny klucz prywatny oraz odpowiadający mu klucz

Rozwiązanie zadania F 906.
Bańkę stanowi sferyczna, cienka błonka wody z mydłem. Błonka ta ma dwie powierzchnie – wewnętrzną i zewnętrzną. Zaniedbując grubość błonki i przyjmując, że promienie obu sfer są jednakowe, znajdujemy ich całkowitą powierzchnię $S = 2 \cdot 4\pi R^2 = 8\pi R^2$. Biorąc pod uwagę, że przed powstaniem bańki powierzchnia wody mydlanej, z której bańka powstała, była zaniedbywalnie mała, można przyjąć, że powyższy wzór wyraża zmianę (przyrost) powierzchni wody mydlanej. Powiększenie powierzchni cieczy o ΔS wiąże się ze wzrostem energii powierzchniowej o ΔE, zgodnie ze wzorem $\Delta E = \sigma \cdot \Delta S$. Wykonywana przy nadmuchiwaniu bańki praca jest zużywana właśnie na powiększenie energii powierzchniowej, czyli $A = 8\pi R^2 \sigma$. Podstawiając wartości, otrzymujemy $A = 2{,}5 \cdot 10^{-3}$ J, czyli 2,5 mJ.

Jedyne dane powiązane z użytkownikiem Bitcoina to jego identyfikator – losowo wyglądający ciąg 34 liter i cyfr. Dlatego często mówi się o anonimowości Bitcoina, choć lepszym określeniem byłaby *pseudonimowość* – użytkownicy występują pod pseudonimami, nikt nie zna ich prawdziwych danych osobowych, jednak ich zachowanie jest w pełni jawne.



publiczny, który jednocześnie pełni rolę identyfikatora użytkownika. Są to klucze systemu cyfrowego podpisu ECDSA, który jest wykorzystywany do podpisywania i weryfikowania transakcji. I tak oto w miejsce odbiorcy mamy *klucz publiczny* odbiorcy `pkB`, a zamiast nadawcy mamy *źródło* wskazujące na inną transakcję, z której pochodzą środki nadawcy. Dodatkowo każda transakcja jest podpisana przez nadawcę (`podpisA`) przy użyciu jego klucza prywatnego.

Aby to sobie zobrazować, o Bitcoinie należy myśleć jak o sieci, w której transakcje stanowią węzły, a użytkownicy to połączenia pomiędzy nimi, nie na odwrót. Aby użytkownik B mógł zapłacić użytkownikowi C kwotę v, w sieci musi istnieć (niewydana) transakcja T_1 o kwocie v zaadresowana do B. Jeśli tylko taka transakcja istnieje, B może ją *wydać*, tworząc transakcję T_2, wpisując `pkC` (klucz publiczny użytkownika C) w pole odbiorcy i podpisując ją swoim podpisem. Taka transakcja jest następnie wysyłana do górników, którzy ją weryfikują, sprawdzając, czy `podpisB` na transakcji T_2 odpowiada kluczowi publicznemu `pkB` na transakcji T_1. Bezpieczeństwo algorytmu ECDSA gwarantuje nam, że transakcja zaadresowana do B nie zostanie wydana przez nikogo innego niż on sam.

Oczywiście, gdyby przedstawiony przeze mnie powyżej uproszczony opis był w pełni zgodny z rzeczywistością, Bitcoin byłby niesłychanie niepraktyczny – wszystkie transakcje musiałyby mieć tę samą wartość (jaką?). W rzeczywistości bitcoiny można w prosty sposób rozmieniać – każda transakcja może mieć kilku odbiorców i dzielić swoją wartość w dowolny sposób pomiędzy nich. Zatem chcąc wysłać użytkownikowi C tylko część kwoty v, użytkownik B może podać samego siebie jako drugiego odbiorcę transakcji T_2 i w ten sposób wziąć sobie *resztę*. Kwoty z mniejszych transakcji można też łączyć w większe, używając transakcji z kilkoma źródłami i w ten sposób wydać naraz kilka spośród swoich transakcji. Użytkownicy mogą więc tworzyć transakcje o dowolnej wartości, a majętność użytkownika określona jest przez sumę niewydanych i zaadresowanych do niego transakcji w sieci.

Z powyższego opisu można by wywnioskować, że Bitcoin służy jedynie do przelewania pieniędzy z jednego konta na drugie. Tymczasem jego możliwości są o wiele większe! Zamiast odbiorcy każda transakcja może mieć w sobie warunek (napisany w specjalnym języku programowania), który musi być spełniony, aby transakcja była poprawna. Można np. opublikować transakcję, którą może wydać pierwszy użytkownik, który poda rozkład na czynniki pierwsze jakiejś dużej liczby i w ten sposób stworzyć konkurs, który sam się rozstrzyga i sam wręcza nagrody. Można też o wiele więcej, ale to już temat na osobny artykuł.

Rozwiązanie zadania M 1496.
Zauważmy, że każda z liczb $1, \ldots, 2016$ jest wielokrotnością co najwyżej jednej z liczb $a_1, \ldots, a_n$. Jednocześnie wśród liczb $1, \ldots, 2016$ dokładnie $\left\lfloor \frac{2016}{a_i} \right\rfloor$ jest wielokrotnością liczby a_i. Stąd otrzymujemy

$$\left\lfloor \frac{2016}{a_1} \right\rfloor + \ldots + \left\lfloor \frac{2016}{a_n} \right\rfloor \leqslant 2016.$$

Ponieważ dla dowolnej liczby x prawdziwa jest nierówność $x - 1 < \lfloor x \rfloor$, więc

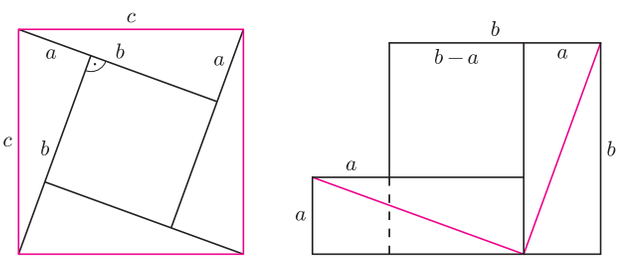
$$\left(\frac{2016}{a_1} - 1\right) + \ldots + \left(\frac{2016}{a_n} - 1\right) < 2016.$$

Dzieląc obie strony nierówności przez 2016 i przenosząc część wyrazów na prawą stronę, otrzymujemy tezę.

Kwadraty

*Jarosław GÓRNICKI**

Euklides w *Elementach* pisał: „... kwadrat jest tym, co równoboczne i prostokątne...". Oto kilka niebanalnych obserwacji, w których kwadrat jest jednym z bohaterów.



Rys. 1

(1) Badanie związków miarowych w kwadracie doprowadziło Pitagorejczyków (między innymi Hippasusa z Metapontu, V w. p.n.e.) do odkrycia, że $\sqrt{2}$, czyli długość przekątnej kwadratu jednostkowego nie jest ułamkiem zwykłym, a w konsekwencji do wyróżnienia liczb niewymiernych.
(2) Indyjski matematyk Bhāskara II (XII w.) w traktacie *Siddhānta Shiromani* (*Korona nauki*) podał dowód twierdzenia Pitagorasa w postaci rysunku 1 z napisem: Patrz!
(3) Kwadrat jest ciągłym obrazem odcinka (G. Peano, 1890).

*Katedra Matematyki, Politechnika Rzeszowska