Jak działa Bitcoin?

Autor**: Silas Barta, Robert P. Murphy**

Fragment III rozdziału książki Zrozumieć Bitcoina, wydanej po polsku przez wydawnictwo Fijorr Publishing

Termin „Bitcoin" obejmuje dwie powiązane, ale odrębne koncepcje. Gdy używamy małej litery („bitcoin"), chodzi nam o poszczególne jednostki fiducjarnej kryptowaluty. Gdy piszemy „Bitcoin" wielką literą, mamy na myśli protokół, w oparciu o który działa zdecentralizowana sieć, za pomocą której łączą się tysiące komputerów na całym świecie, tworząc coś w rodzaju „publicznego rejestru" — znanego pod nazwą łańcucha bloków — przechowującego w pełni jawny zapis wszystkich zatwierdzonych transakcji dokonanych przy użyciu bitcoinów od chwili rozruchu systemu na początku 2009 roku. W skrócie, słowo to obejmuje swym znaczeniem zarówno niemającą pokrycia walutę cyfrową, jak i zdecentralizowany system płatności w internecie.

Jak czytamy na oficjalnej stronie projektu, „aby funkcjonować bez centralnej kontroli czy banków, Bitcoin korzysta z technologii *peer-to-peer.* Zarządzanie transakcjami i emisja bitcoinów odbywa się kolektywnie poprzez sieć"[1]. Każdy może pobrać na swój komputer odpowiednie oprogramowanie i włączyć się do procesu generowania („kopania"[2]) nowych bitcoinów i potwierdzania dokonywanych w systemie transakcji.

Aby w pełni zrozumieć, jak działa Bitcoin, trzeba pojąć subtelne kwestie związane z kryptografią opartą na kluczu publicznym, które omawiamy w następnych sekcjach. Teraz jednak skupimy się na przedstawieniu pewnej analogii, która pozwoli zrozumieć ekonomiczną stronę Bitcoina bez konieczności zagłębiania się w zagadnienia techniczne.

---

[1] Zob. Bitcoin — Otwarta waluta P2P, http://bitcoin.org.

[2] W świecie Bitcoina przyjęło się stosowanie słownictwa związanego z górnictwem — wszystkie terminy dotyczące kreowania nowych jednostek kryptowaluty nawiązują do kopania, górników i kopalń. Ma to budzić skojarzenie z procesem wydobywania złota, który — podobnie jak tworzenie nowych jednostek waluty Bitcoin i odwrotnie niż w wypadku państwowych walut dekretowych — wymaga wkładu pracy (mocy obliczeniowej).

Analogia pozwalająca zrozumieć podstawowe aspekty bitcoina[3]

Wyobraź sobie społeczność, która posługuje się pieniądzem opartym na liczbach naturalnych od 1 do 21 milionów. W każdym momencie ktoś jest „właścicielem" liczby 8, ktoś inny liczby 34 323 i tak dalej.

Przypuśćmy, że Bill pragnie kupić samochód od Sally, a etykieta cenowa na masce głosi, że kosztuje on „dwie liczby". Tak się składa, że Bill znajduje się w posiadaniu liczb 18 i 112. Oddaje je zatem Sally, a ona daje mu samochód. Społeczność dostrzega dwa fakty tytuł własności samochodu został przeniesiony z Sally na Billa, a Sally stała się właścicielką liczb 18 i 112.

W tej fikcyjnej społeczności istnieje branża zatrudniająca tysiące księgowych zajmujących się rejestrowaniem tytułów własności do wszystkich 21 milionów liczb całkowitych. Każdy z księgowych przechowuje gigantyczną kopię rejestru w postaci arkusza kalkulacyjnego Excel. Zawiera on kolumny ponumerowane od 1 do 21 milionów oraz wiersze zawierające każdą transakcję dotyczącą każdej liczby. W momencie, gdy Bill kupił od Sally samochód, księgowi znajdujący się w zasięgu słuchu od miejsca transakcji zmodyfikowali swoje pliki Excel, wpisując „Aktualnie w posiadaniu Sally" do komórek odpowiadających liczbom 18 i 112 w pierwszym wolnym wierszu. Gdybyśmy spojrzeli do poprzedniego wiersza, zobaczylibyśmy, że w komórkach odpowiadających tym liczbom zapisane było „Aktualnie w posiadaniu Billa", gdyż był on ich właścicielem, zanim oddał je Sally.

Wszyscy księgowi, oprócz odnotowywania transakcji, które sami zaobserwowali, co jakiś czas porównują swoje rejestry z rejestrami prowadzonymi przez innych księgowych. Jeżeli w rejestrach swoich kolegów po fachu wykryją transakcje dotyczące innych liczb, których sami nie zanotowali (ponieważ odbyły się poza ich zasięgiem), je także wprowadzają do własnych rejestrów. W efekcie w każdym momencie wszyscy księgowi przechowują w swoich rejestrach kompletną historię wszystkich dokonanych w systemie transakcji.

W przedstawionej powyżej analogii mamy do czynienia z systemem znajdującym się w „stanie końcowym", czyli w czasie, gdy wszystkie bitcoiny zostały już „wydobyte". Sytuacja taka nastąpi gdzieś w okolicach roku 2100, gdy

[3] Treść niniejszego podrozdziału pochodzi z artykułu Murphy'ego *The Economics of Bitcoin.*

(niemal) wszystkie 21 milionów bitcoinów znajdzie się w rękach społeczeństwa[4]. W rzeczywistości, gdy ludzie dokonują transakcji przy użyciu sieci Bitcoin, przekazują sobie wzajemnie tytuły własności do pewnych ilości bitcoinów w zamian za inne dobra lub usługi. Transfer ten jest dokonywany za pośrednictwem sieci komputerów wykonujących obliczenia służące do zmiany „kluczy publicznych" przypisywanych do poszczególnych „sprzedanych" bitcoinów. W naszej analogii sieci tej odpowiadali księgowi przechowujący imiona posiadaczy poszczególnych liczb.

Jaką rolę odgrywa w tym kryptografia, czyli problem z anonimowymi właścicielami

Po pierwsze, musimy od razu wyjaśnić, że choć w kontekście Bitcoina często można spotkać się z terminem „szyfrowanie", w istocie nie dochodzi tu do żadnego szyfrowania, gdyż nie stanowiłoby ono rozwiązania problemu, z jakim muszą zmierzyć się użytkownicy tej technologii. Nie jest ich celem ukrywanie informacji o przeprowadzonych transakcjach, lecz raczej ich uwierzytelnienie[5].

Powróćmy do naszego fikcyjnego świata, w którym żyją Bill i Sally i w którym pieniądz opiera się na powszechnie akceptowanych tytułach „własności" względem 21 milionów liczb całkowitych. Zaprezentowany w tej historyjce

[4] Dokładniej rzecz ujmując, całkowita liczba „wydobytych" bitcoinów nigdy nie osiągnie 21 milionów, gdyż protokół gwarantuje, że nagrody dla górników za wydobycie nowego bloku będą zmniejszane i zaokrąglane w dół aż do zera (co nastąpi około 2140 roku). Przewiduje się, że począwszy od 2108 roku nagroda uzyskiwana przez górników za każdy blok wynosić będzie zaledwie milionową część bitcoina i będzie wciąż maleć (z przewidywaniami co do liczby wydobytych bitcoinów w określonym czasie w przyszłości oraz liczby bitcoinów stanowiących aktualną nagrodę za kolejny blok można zapoznać się pod adresem: https://en.bitcoin.it/wiki/Controlled_supply#Projected_Bitcoins_Long_Term). Inna komplikacja wynika stąd, że niektóre bitcoiny bądź ich ułamki zostaną nieodwracalnie „utracone" wraz ze śmiercią ich właścicieli, utratą kluczy prywatnych i tak dalej. Dlatego mimo że będą one „wydobyte", nie będzie możliwe ich wykorzystanie w transakcjach, co oznacza wykluczenie ich z całkowitej, efektywnej „podaży bitcoinów". Analogią mogą być tutaj złote monety, które poszły na dno mórz lub oceanów razem z zatopionymi okrętami.

[5] Zamieszanie może wynikać stąd, że zarówno szyfrowanie, jak i uwierzytelnianie są pojęciami pochodzącymi ze świata kryptografii. Można tu mówić o pewnym dualizmie w tym sensie, że w wypadku systemów opartych na kluczu publicznym podpisywanie wiadomości przypomina jej odszyfrowywanie, a weryfikacja jej autentyczności szyfrowanie. Należy jednak wyraźnie zaznaczyć, że istota działania sieci Bitcoin nie opiera się na szyfrowaniu komunikacji, choć wielu ludzi mylnie twierdzi, że tak właśnie jest.

system bardzo szybko napotyka istotny problem — jak mianowicie księgowi mają zweryfikować tożsamość osób próbujących dokonać transakcji za pomocą liczb? Bill naprawdę był właścicielem liczb 18 i 112. Stać go było na zakup samochodu od Sally, gdyż zażyczyła sobie w zamian „dwóch liczb" (a w społeczności tej każdy wie, że „liczby" to liczby naturalne z zakresu 1 do 21 milionów, gdyż żadne inne nie są uważane za pieniądz). Księgowi mogą łatwo sprawdzić, czy Bill widnieje jako właściciel tych dwóch liczb w ich rejestrach. Jak jednak mogą mieć pewność, że osoba, która próbuje kupić od Sally samochód, naprawdę jest Billem z ich rejestrów? Musi istnieć jakiś sposób, by prawdziwy Bill mógł udowodnić każdemu, że to jego imię widnieje w publicznych rejestrach transakcji. Aby można było zapobiec oszustwom polegającym na wydawaniu cudzych pieniędzy przez nieuprawnione do tego osoby trzecie, musi istnieć mechanizm, za pomocą którego jedynie prawdziwy Bill będzie mógł przekonać księgowych, że jest sobą samym.

W tym właśnie miejscu w świecie rzeczywistym do akcji wkracza skomplikowany mechanizm kryptografii opartej na kluczach publicznych i prywatnych. W dalszych rozdziałach zajmiemy się możliwie najbardziej intuicyjnym wyjaśnieniem tych kwestii, teraz jednak wolimy skupić się na przedstawieniu sposobu działania sieci Bitcoin zrozumiałym nawet dla ludzi, którzy nie są zainteresowani żadnymi szczegółami technicznymi.

Niestety, w tym momencie nasza opowieść o Billu i Sally stanie się nieco dziwaczna, gdyż nie udało nam się znaleźć odpowiedniej analogii do opisania tego aspektu technologii Bitcoin, o którym zamierzamy mówić. Dlatego bez dalszego owijania w bawełnę przyjmijmy, że ludzie z naszego fikcyjnego świata księgowości opartej na 21 milionach liczb całkowitych radzą sobie z weryfikacją tożsamości następująco.

Za każdym razem, gdy dochodzi do zmiany właściciela liczb, nowy właściciel musi wymyślić zagadkę, na którą tylko on jeden zna prawidłową odpowiedź. W dodatku członkowie naszej społeczności są na tyle bystrzy, że zawsze potrafią zorientować się, czy odpowiedź na podaną zagadkę jest poprawna, gdy tylko ją usłyszą, jednak nie na tyle kreatywni, aby sami odkryć poprawne rozwiązanie.

Gdy Bill otrzymał liczby 18 i 112 jako zapłatę od swojego pracodawcy (co miesiąc szef płaci mu dwoma liczbami), księgowi powiedzieli mu:

W porządku, Bill, aby zabezpieczyć swój tytuł własności do tych dwóch liczb, musisz wymyślić powiązaną z nimi zagadkę. Jej treść wraz z twoim imieniem zostanie zapisana w naszym rejestrze w odpowiadających tym liczbom kolumnach. Gdy zechcesz wydać swoje liczby, po prostu zgłosisz się do nas i podasz odpowiedź na zagadkę. Umożliwimy przekazanie tych liczb nowemu właścicielowi tylko wówczas, gdy osoba podająca się za „Billa" poda nam poprawne rozwiązanie. Weź pod uwagę, że w chwili, gdy zechcesz dokonać transakcji, możesz znajdować się po drugiej stronie miasta wśród obcych księgowych. Dlatego nie wystarczy, że my wiemy, jak wyglądasz. Musimy zapisać podaną przez ciebie zagadkę, a ona zostanie skopiowana tysiące razy wraz z informacją o dokonaniu tej transakcji, aby powiadomić o niej całą społeczność. Dzięki temu każdy księgowy będzie posiadał w swoim rejestrze „Billa" i zagadkę przypisaną do liczb w twoim posiadaniu.

Po chwili zastanowienia Bill wymyśla nową, oryginalną zagadkę: „Kiedy drzwi nie są drzwiami?", księgowi skrupulatnie zapisują ją i wkrótce zostaje ona skopiowana i rozpowszechniona w całej społeczności.

Kilka dni później pewien złoczyńca próbuje podszyć się pod Billa, by kupić biżuterię kosztującą „jedną liczbę". Mówi najbliższym księgowym: „Nazywam się Bill i jestem właścicielem liczby 112, każdy może się o tym przekonać, zaglądając do publicznych rejestrów. Przekazuję zatem liczbę 112 temu jubilerowi w zamian za biżuterię". Księgowi odpowiadają: „Dobrze, Bill, ale musimy najpierw zweryfikować twoją tożsamość. Jakie jest rozwiązanie zagadki brzmiącej: «Kiedy drzwi nie są drzwiami?»". Złoczyńca głowi się i głowi, ale nie zna odpowiedzi. W końcu mówi: „Gdy drzwi nie są drzwiami!". Księgowi spoglądają po sobie, drapią się po głowach i jednomyślnie odpowiadają: „Nie, to durna odpowiedź, rozwiązanie zagadki jest inne". Odmawiają zarejestrowania transakcji, a złoczyńca nie otrzymuje biżuterii.

Wróćmy teraz do naszej pierwotnej sytuacji – Bill chce kupić samochód od Sally za „dwie liczby" i ogłasza pobliskim księgowym, że jest właścicielem liczb 18 i 112 i może to udowodnić, podając prawidłową odpowiedź na przypisaną do

nich zagadkę: „Drzwi nie są drzwiami, gdy są otwarte". Księgowi są usatysfakcjonowani, gdyż jest to prawidłowe rozwiązanie zagadki.

Zgadzają się zatem uznać, że mają do czynienia z prawdziwym Billem, i pozwalają na dokonanie transakcji. Zapisują więc „Sally" w następnych wolnych wierszach w kolumnach przypisanych do liczb 18 i 112 i zwracają się do Sally o podanie nowej zagadki, której rozwiązanie znane będzie tylko jej samej.

Przeniesienie analogii na sieć Bitcoin

Chociaż musieliśmy powyżej przedstawić bardzo uproszczoną historyjkę — wszak wymyślona przez nas zagadka Billa była bardzo łatwa do odgadnięcia — sądzimy, że stanowi ona przystępną analogię dla faktycznego funkcjonowania sieci Bitcoin. Bez wdawania się w szczegóły można powiedzieć, że istnieje sposób, w jaki faktyczny właściciel może przeprowadzić pewną operację matematyczną, którą można odwrócić jedynie znając konkretną liczbę. Ta liczba to tak zwany „klucz prywatny". W naszej historii takim kluczem prywatnym byłaby zdolność Billa do rozwiązania swojej zagadki, a sama treść rozwiązania stanowiłaby jego cyfrowy „podpis". W rzeczywistym świecie, gdy ktoś poda poprawną „sygnaturę" możliwą do wygenerowania tylko przez posiadacza odpowiedniego klucza prywatnego, sieć Bitcoin weryfikuje go jako legalnego właściciela. Przy obecnym poziomie technologii odgadnięcie cudzego klucza prywatnego i wygenerowanie w ten sposób poprawnej sygnatury osobie trzeciej zajęłoby tysiące lat. Dlatego nawet NSA, dysponująca potężnymi superkomputerami, nie może dokonywać transakcji przy użyciu cudzych bitcoinów, „fałszując" podpis tej osoby[6].

W rzeczywistym świecie właściciele bitcoinów nie muszą nawet korzystać ze swoich prawdziwych imion, aby zweryfikować swój tytuł własności do poszczególnych bitcoinów. Mogą korzystać z innych identyfikatorów. Identyfikatory te to widoczne dla wszystkich „klucze publiczne". W naszej analogii ich odpowiednikiem byłby na przykład pseudonim „SuperKoteł", który na życzenie Billa księgowi wpisywaliby do swoich rejestrów zamiast jego imienia.

[6] W rzeczywistości problemem nie jest próba wygenerowania „poprawnej" sygnatury bez dysponowania właściwym kluczem prywatnym, jest to bowiem właściwie niewykonalne. Grupa pozbawionych skrupułów ludzi dysponująca wystarczająco dużą mocą obliczeniową (mierzoną jako procentowy udział w mocy całej sieci) mogłaby jednak dokonać udanego ataku na Bitcoina. Problem ten omawiamy w dalszej części poradnika — tymczasem chcemy tylko zaznaczyć, że atak ten nie polegałby na fałszowaniu sygnatur.

Aby udowodnić, że jest faktycznie „SuperKotełem", Bill musiałby podać rozwiązanie wymyślonej wcześniej zagadki.

Przyczyną, dla której zwolennicy ochrony prywatności z takim entuzjazmem zareagowali na pojawienie się technologii Bitcoin, jest fakt, że Bill może ukryć to, jak wiele liczb posiada[7]. Może podać się za „SuperKoteła", gdy uwierzytelnia swój tytuł własności do liczb 18 i 112, ale już identyfikując się jako właściciel liczb 45 i 974, może przedstawić się jako „FanJamesaBonda". Bill posiada więc łącznie cztery liczby, ale nikt poza nim tego nie wie, dopóki rejestry księgowych własność liczb 18 i 112 przypisują pseudonimowi „SuperKoteł", a liczb 45 i 97 4 pseudonimowi „FanJamesaBonda". Nikt poza Billem nie wie, że oba identyfikatory należą do jednej i tej samej osoby.

Dla uproszczenia w naszej analogii przyjęliśmy, że wszystkie 21 milionów jednostek waluty zostało już „wydobytych". W rzeczywistości jednak proces uwierzytelniania dokonywanych w sieci transakcji jest ściśle związany z przyrostem całkowitej podaży bitcoinów. W 2009 roku, gdy sieć Bitcoin zaczęła funkcjonować, włączone do niej komputery — określane mianem „górników" — wraz z dokonaniem obliczeń niezbędnych do dodania pierwszego „bloku" transakcji do publicznego rejestru otrzymały 50 bitcoinów. W momencie pisania tego poradnika nagroda za dodanie nowego bloku spadła do 25 bitcoinów i będzie nadal maleć o połowę co każde 210 tysięcy bloków (czyli, jak się szacuje, co cztery lata, gdyż trudność obliczeniowa wiążąca się z wydobywaniem bloków jest automatycznie dostosowywana do mocy obliczeniowej całej sieci). Ostatecznie około roku 2140 całkowita liczba bitcoinów stanowiących nagrodę za wydobycie nowego bloku spadnie do zera, a całkowita podaż bitcoinów na świecie osiągnie maksymalną wartość nieco poniżej 21 milionów.

[7] I jakie to konkretnie liczby. Jest to przy tym prawdą tylko wówczas, gdy posiadacz bitcoinów stosuje się bezbłędnie do bardzo licznych zasad bezpieczeństwa wymaganych dla względnie skutecznego maskowania swojej tożsamości w internecie, gdyż obecnie za pomocą zaawansowanej analizy ruchu sieciowego możliwe jest przypisanie konkretnych transakcji w sieci Bitcoin do konkretnych osób. Nie wspominając już o całkowitej jawności wszystkich transakcji bitcoinowych, które opierają się na interakcji z tradycyjnym systemem bankowym. W praktyce naprawdę skuteczne ukrycie swojej tożsamości w internecie (a więc i w sieci Bitcoin) wymaga tak czasochłonnych i niewygodnych operacji oraz tak dużej wiedzy, że prawdopodobnie nikt nie jest zdolny zapewnić sobie całkowitej anonimowości (przyp. tłum.).

Twórca(y) Bitcoina mógł zasadniczo wygenerować wszystkie 21 milionów bitcoinów natychmiast, wraz z publikacją protokołu[8]. Jednak decyzja taka prawdopodobnie doprowadziłaby cały projekt do błyskawicznego upadku. Dzięki temu, że proces niezbędny do potwierdzania dokonywanych transakcji wiąże się z generowaniem nowych bitcoinów jako nagrody dla właścicieli komputerów biorących w nim udział, istnieje motywacja dla górników, aby poświęcali należącą do siebie moc obliczeniową temu celowi (oraz szerzeniu wiedzy o Bitcoinie w społeczeństwie w celu zwiększenia zainteresowania). Osoby pragnące wnieść opłatę transakcyjną w celu przyśpieszenia potwierdzenia swoich transakcji mogą to uczynić, jednak w początkowym stadium projektu nie jest to konieczne, gdyż górnicy potwierdzą nawet transakcje pozbawione jakichkolwiek opłat transakcyjnych. Mechanizm ten służy szybszemu rozpowszechnieniu technologii w społeczeństwie. […]

[8] Ponieważ oprogramowanie technologii Bitcoin jest dostępne dla każdego na zasadzie *open source,* inni ludzie stworzyli szybko własne kryptowaluty (nazywane „altcoinami"), a niektóre z nich opierały się na odmiennych schematach emisji. Przykładowo autorzy kryptowaluty Dogecoin nie ustalili żadnej górnej granicy dla liczby wyemitowanych jednostek.