https://wyborcza.pl/magazyn/7,124059,28472880,blockchain-blok-kopacze-co-to-u-licha-ten-bitcoin-spokojnie.html

Wojciech Cellary 2022-05-21

Bitcoin

Bitcoin – ponadnarodowa cyfrowa kryptowalutą – jest niezwykłym fenomenem naszych czasów, prawdziwym czarnym łabędziem rynków finansowych, którego nikt nie przewidział. Wartość bitcoina od zera doszła do 60 tys. dolarów, by aktualnie spaść do ok. 31 tys. Ponieważ liczba bitcoinów jest ograniczona do 21 milionów, to przy tej cenie ich sumaryczna wartość wynosi około 650 miliardów dolarów. To mniej więcej 6 razy tyle, ile wynoszą roczne dochody budżetu państwa polskiego. Szacuje się, że 28 milionów ludzi posiada bitcoiny.

Jednak jak to się dzieje, że za bitcoinem nie stoi żadna instytucja, nie podlega on żadnemu państwu, bankowi, ani korporacji, jest rozproszony na około 13 tys. komputerów na całym świecie, nie ma centralnego serwera zarządzającego i jest praktycznie niemożliwy do zhakowania?

Bitcoin jest zbudowany mając za fundament łańcuch bloków (ang. blockchain), w których są zapisane transakcje płatności bitcoinami. Z kolei łańcuch bloków wykorzystuje dwie techniki kryptograficzne: funkcję skrótu i cyfrowy podpis.

Funkcja skrótu zamienia dowolny dokument cyfrowy na 256-bitową liczbę binarną zwaną „skrótem”. Ma ona taką właściwość, że jeśli zmieni się choćby jeden bit w dokumencie, to wygeneruje zupełnie inny skrót. Można dzięki temu wykryć, czy ktoś sfałszował ten dokument.

Cyfrowy podpis wiąże się ze szczególnym rodzajem szyfrowania. Wyobraźmy sobie drzwi z zamkiem, do którego są dwa różne klucze – zupełnie niepodobne do siebie. Ten zamek jest taki dziwny, że jeśli zamknie się go jednym kluczem, to można go otworzyć tylko tym drugim. Nie można go otworzyć tym kluczem, którym się go zamknęło.

Każdy, kto chce się cyfrowo podpisać, ma takie dwa klucze kryptograficzne. Jeden z nich jest jawny i publiczny – można go podać całemu światu. Drugi jest prywatny i tajny – właściciel nikomu nie może go udostępnić, jeśli nie chce dopuścić do fałszerstwa lub kradzieży.

Cyfrowy podpis polega na tym, że z podpisywanego dokumentu tworzy się skrót, szyfruje go przy użyciu swojego klucza prywatnego i dołącza do dokumentu. Każdy może teraz sprawdzić, czy dokument nie został sfałszowany. W tym celu należy odszyfrować załączony skrót kluczem publicznym osoby podpisanej, który jest jawny, utworzyć własny skrót z dokumentu i je porównać. Jeśli są takie same, to dokument nie został sfałszowany.

Bitcoin uważa się za cyfrową gotówkę, ale tak naprawdę to jest system księgowy. Każdy bitcoin i każda jego część jest przypisana do właściciela – nie ma bezpańskich bitcoinów. Płatność bitcoinami polega na zarejestrowaniu transakcji, w której obecny właściciel bitcoina, lub jego części, identyfikowany pseudonimem zawierającym jego klucz publiczny, przekazuje prawo ich własności do nich komuś innemu, również identyfikowanemu pseudonimem z jego kluczem publicznym. W transakcji jest podane skąd obecny właściciel bitcoinów je wziął, czyli są podane identyfikatory transakcji, w których ktoś mu je przekazał. Dzięki temu można prześledzić drogę każdego bitcoina i jego części od powstania do obecnego właściciela, przy czym właściciele nie są identyfikowani imieniem i nazwiskiem, tylko pseudonimami. Mamy więc do czynienia z pełną transparentnością operacji finansowych bitcoinami, ale na poziomie pseudonimów.

Każda transakcja jest podpisana cyfrowo przez aktualnego właściciela bitcoinów, więc nie można jej zmienić. Po zarejestrowaniu transakcji, tylko wskazany w niej odbiorca bitcoinów identyfikowany pseudonimem ze swoim kluczem publicznym może je wydać, bo tylko on ma klucz prywatny od pary, którym może podpisać cyfrowo następną transakcję przekazania własności bitcoina lub jego części komuś innemu.

Transakcje są grupowane w bloki. W jednym bloku może być od kilku do kilku tysięcy transakcji. Bloki są ze sobą połączone w łańcuch. To znaczy, że każdy blok ma swojego rodzica, który ma swojego rodzica, i tak dalej, aż do pierwszego bloku utworzonego na samym początku. Bloki mają nagłówki i są identyfikowane skrótem nagłówka. Jednym z elementów nagłówka jest skrót rodzica. To jest bardzo mocne zabezpieczenie, bo gdyby ktoś zmienił cokolwiek w jakimś bloku w środku łańcucha, na przykład sfałszował transakcję, to zmieniłby się skrót nagłówka tego bloku, co wymagałoby zmiany skrótu nagłówka bloku-dziecka, bo w nagłówku bloku-dziecka jest zapisany skrót nagłówka rodzica, co z w konsekwencji wymagałoby zmiany skrótu nagłówka bloku-wnuka itd. Obliczenie skrótu nagłówka jest jednak bardzo trudne, bo musi on spełniać określone warunki. Wymaga się na przykład, aby taki skrót miał 60 zerowych bitów na początku. Aby to osiągnąć, modyfikuje się w nagłówku bloku element zwany „niuansem”, oblicza skrót nagłówka i sprawdza, czy ma 60 zer na początku. Jeśli nie, to znowu modyfikuje się niuans itd. Jeśli ktoś ma wyspecjalizowany komputer wykonujący 1 bilion (10^{12}) skrótów na sekundę, to jest w stanie znaleźć rozwiązanie średnio co 59 dni. Dla porównania dobry komputer osobisty może obliczyć około 10 milionów (10^7) skrótów na sekundę. Ale jeśli ktoś ma dużo szczęścia, to może odpowiedni niuans znaleźć od razu. Tę czynność poszukiwania właściwego niuansu nazywa się „kopaniem”, a ludzi, którzy się tym zajmują – „kopaczami”.

Kopacze rozproszeni po całym świecie nie pracują za darmo. Za dołączenie bloku do łańcucha otrzymują nagrodę w bitcoinach, która pochodzi z dwóch źródeł. Po pierwsze, z opłat za transakcje – w każdej transakcji jest zawarta opłata dla kopacza. Po drugie, z nowych bitcoinów tworzonych z niczego w każdym bloku dołączonym do łańcucha.

Liczba nowotworzonych bitcoinów w każdym bloku zmniejsza się o połowę co 210 tys. bloków. Zaczęło się od 50 bitcoinów, a obecnie jest 6,25 bitcoina. Nagroda kopacza jest

całkiem spora. Przy cenie 31 tys. dolarów za bitcoin 6,25 bitcoina jest warte niecałe 200 tys. dolarów. Do tego dochodzą opłaty za transakcje, więc nagroda za blok może sięgnąć 250 tys. dolarów.

Oczywiście z tych pieniędzy trzeba pokryć koszty energii elektrycznej i wyspecjalizowanych komputerów, ale i tak nagroda jest pokaźna. Kopacze zaciekle rywalizują więc ze sobą, więc nowy blok jest średnio wykopywany co 10 minut, zatem co taki okres ktoś staje się bogatszy o 250 tys. dolarów, które dla niego zarabia jego komputer.

Łańcuch bloków bitcoina jest powielony na 13 tysiącach komputerów, nazywanych „pełnymi węzłami", rozsianych po całym świecie. Dlatego jest tak bardzo odporny na różnego rodzaju możliwe ataki. Istotna jest jednak synchronizacja danych na tych komputerach, aby każdy zawierał dokładną kopię łańcucha bloków.

Każda nowa transakcja, która pojawi się w sieci jest rozsyłana do kolejnych pełnych węzłów na zasadzie „podaj dalej". Każdy węzeł niezależnie weryfikuje ją, w szczególności sprawdza, skąd właściciel bitcoinów je wziął. Następnie grupuje otrzymane transakcje w blok, wpisuje do jego nagłówka skrót ostatniego bloku w łańcuchu i zaczyna kopać, czyli szukać odpowiedniego niuansu. Jeśli z trakcie kopania przyjdzie do niego nowy blok wskazujący na tego samego rodzica pochodzący od innego kopacza, to znaczy, że przegrał rywalizację i nie dostanie nagrody. Niezrażony sprawdza, których transakcji nie ma jeszcze w blokach, znowu tworzy z nich blok wskazując na aktualny ostatni blok w łańcuchu i zaczyna kopać licząc na to, że tym razem mu się poszczęści.

Problem pojawia się wówczas, gdy na dwóch końcach świata, dwaj kopacze wykopią blok wskazujący na tego samego rodzica w prawie tym samym czasie. To jest niedopuszczalna sytuacja, bo w łańcuchu rodzic może mieć tylko jedno dziecko. Chwilowo jednak ma dwoje, więc powstaje rozwidlenie łańcucha na dwie gałęzie. Zaczyna się wyścig, do której gałęzi będzie dołączonych więcej nowych bloków. Każdy nowy blok może bowiem mieć tylko jednego rodzica, albo z jednej gałęzi, albo z drugiej.

Po pewnym czasie, każdy węzeł, niezależnie od innych, stwierdzi, że do jednej gałęzi dołączono więcej bloków, czyli, że skumulowano w niej więcej pracy. Wówczas likwiduje tę drugą gałąź, czyli rozwiązuje zgromadzone w niej bloki, sprawdza, które transakcje są już w istniejących blokach, a które nie, z tych drugich tworzy kolejny blok wskazując ostatni zaakceptowany blok jako rodzica i zaczyna kopać. Cała sieć bitcoin odzyskuje spójność, czyli we wszystkich pełnych węzłach znów będzie taki sam łańcuch bloków. Wszystkie węzły bez żadnego centralnego serwera podejmują taką samą decyzję o likwidacji tej samej gałęzi rozwidlenia.

Tajemniczy Satoshi Nakamoto, który podobno jest twórcą bitcoina, wystosował takie symboliczne wezwanie. Hakerzy z całego świata, nawet nie próbujcie zhakować bitcoina, bo to się wam nie uda. Zamiast tego zapraszam was do zabezpieczania go przez kopanie, a ja wam zapłacę pobieranym opłatami i nowymi bitcoinami emitowanymi w każdym bloku bez

jakiegokolwiek banku centralnego. Połączenie emisji pieniądza z bezpieczeństwem jest wielką innowacją bitcoina.

Często pada pytanie, czy bitcoin jest bezpieczny? Jak wynika z powyższego opisu – tak, bardzo. Ale właściciel bitcoinów jest tak bezpieczny jak jego klucz prywatny. Jeśli go zgubi lub zapomni, to nigdy nie wyda swoich bitcoinów, które pozostaną w łańcuchu do końca świata. Jeśli pozwoli go sobie ukraść, to złodziej może wydać jego bitcoiny, a on nie będzie miał się nawet komu poskarżyć. Komputer łzy nie uroni.