Górnictwo bitcoina

Co wytwarzają górnicy bitcoina

Górnictwo bitcoina nie wytwarza tylko samego bitcoina, ale również ciepło. Współczesne koparki podgrzewają powietrze do około 50 stopni Celsjusza i jest to produkt odpadowy z górnictwa bitcoina. To ciepło można wykorzystać do ogrzewania procesów technologicznych, wielopiętrowych budynków, szklarni, magazynów, podgrzewać wodę do basenów, saun i budynków użyteczności publicznej. Ciepła woda w miejskich wodociągach może być pozyskiwania jako efekt uboczny procesu wykopywania bitcoina.

Współczesne generacje koparek bitcoina współpracują z technologią wymiany ciepła przez płyny, dlatego są one praktycznie bezgłośne i przede wszystkim mogą dostarczać ciepłą wodę do budynków. Wystarczająco zminiaturyzowane urządzenia wielkości pudełka do butów, które można podłączyć do bojlera są w stanie zapewniać ciepłą wodę w domkach jednorodzinnych.

Najnowsza generacja koparek bitcoina będzie wykorzystywać przejście fazowe z fazy ciekłej na gaz i ponownie do ciekłej, przez co stanie się dużo bardziej wydajna i przede wszystkim pozwoli generować wyższe temperatury, co poszerzy zakres potencjalnych zastosowań.

Jak pracują górnicy bitcoina

Moc górnicza (inaczej moc zabezpieczeń) sieci bitcoin w ostatnim czasie dynamicznie rośnie i przekracza już 500 egzahashy (500,000,000,000,000,000,000), czyli 500 kwintylionów (wedle notacji amerykańskiej wielkich liczb) albo tryliardów (wedle notacji polskiej) operacji na sekundę. Każda pojedyncza operacja składa się z dodania liczby, dopisania do treści niuansu (ang. *nonce*), do aktualnego bloku danych o transakcjach bitcoinem i wyliczenia podsumowania (ang. *hash*) tak utworzonego dokumentu.

Hash (liczba wynikająca z dokumentu) to podsumowanie dokumentu poprzez nadanie mu unikatowego numeru, albo inaczej utworzenie z wiadomości unikatowej liczby, coś jak odcisku palca. Każdy dokument posiada konkretny i tylko jeden, tak jak unikatowe linie papilarne posiada każdy człowiek. Ta sama wiadomość zawsze wygeneruję tę samą liczbę podsumowania, czyli ten sam hash. Zmiana nawet jednego przecinka w wiadomości (z której tworzy się hash) wygeneruje już inną liczbę i to nie trochę inną, a zupełnie inną liczbę. Co krytycznie istotne, nie można przewidzieć jaka to będzie liczba. Dlatego aby uzyskać liczbę należącą do podgrupy możliwych do wygenerowania liczb, trzeba próbować zmieniać treść wiadomości i żmudnie generować kolejne ich podsumowania, aż do czasu uzyskania hasha należącego do danej podgrupy. Na tym polega praca w dowodzie pracy (ang. *proof of work*).

Metoda generowania hashy o nazwie SHA-256 wykorzystywana w górnictwie bitcoina generuje hash jako binarną liczbę mającą maksymalnie 256 cyfr, czyli w systemie szesnastkowym będzie to liczba mająca 64 cyfry. W systemie dziesiętnym największa liczba mająca 64 cyfry w systemie szesnastkowym (albo 256 w systemie dwójkowym) to 1,158 razy 10 do 77 potęgi, czyli 1158 i 74 zera. Hash musi zawsze wygenerować tę samą liczbę cyfr, dlatego jeśli liczba jest mała, wtedy ma ona z przodu określoną liczbę zer, stanowiących o liczbie miejsc znaczących, które nie są wykorzystywane.

Górnictwo bitcoina to wyliczanie hashy (albo inaczej tak zwanego ang. *message digest*) z bloku danych na jakich zapisane są transakcje bitcoina. Jest to nadawanie każdej stronie (pojedynczy blok danych) z historii transakcji (łańcuch bloków) unikatowej liczby podsumowania. Jednak liczba ta musi mieścić się w pewnej podgrupie możliwych do wygenerowania liczb (hashy podsumowań). Dlatego trzeba zmienić treść bloku danych, aż będzie on mógł wygenerować podsumowanie mieszczące się w podgrupie możliwych hashy.

Zmienianie zawartości bloku danych (treści podsumowywanej wiadomości) tak, aby nie zamazać, czy nie zmienić historii transakcji, odbywa się poprzez dodawanie niuansu do bloku danych (ang. *nonce*), czyli po prostu losowej liczby i sprawdzanie, czy tak zmieniony blok wygeneruje hash poniżej danej wartości (liczby granicznej). Hash mniejszy od danej liczby (ang. *target*), to hash nie wykorzystujący określonej ilości miejsc znaczących albo inaczej mający z przodu określoną liczbę zer.

Ponieważ metoda SHA-256 generuje praktycznie losowo liczbę podsumowującą (deterministycznie będzie to zawsze ta sama liczba, ale nie wiemy z jakiej treści powstanie jaka liczba podsumowania) trudność w znalezieniu liczby mniejszej od wartości granicznej rośnie wraz z obniżeniem wymogu jej maksymalnej wielkości. W systemie binarnym (kiedy liczbę podsumowującą przedstawimy w postaci 256 cyfr) z każdym kolejnym zerem na początku trudność w znalezieniu odpowiedniego niuansu rośnie dwukrotnie. Trzeba bowiem statystycznie (zwykle) wykonać dwa razy więcej operacji (podstawień kolejnych niuansów), aby znaleźć rezultat, który nas usatysfakcjonuje.

Przez to łatwo już jest ustanowić mechanizm określający trudność kopania zmieniając ilość zer na początku jako obowiązkowy format dla hashy. Tak właśnie regulowana jest mniej więcej co dwa tygodnie trudność kopania bitcoina. Jest ona automatycznie regulowana, aby wszystkim zaangażowanym w zabezpieczanie sieci bitcoin górnikom średnio co 10 minut udawało się odnaleźć pasujący niuans. Kiedy mocy obliczeniowej przybywa trudność jest zwiększana, gdy z kolei dostępna moc obliczeniowa maleje, trudność jest zmniejszana (ang. *difficulty adjustment*), tak aby emisja nowego bitcoina była mniej więcej regularna.

Atak 51% mocy obliczeniowej

Przy tak zorganizowanych zasadach współpracy międzyludzkiej atak nawet większości mocy obliczeniowej na bitcoina (górników mających łącznie większość zdolności górniczej) byłby nieskuteczny. Taka większość, pomimo tego, że nie jest to zwyczajna większość górników, lecz przede wszystkim większość zdolności górniczych, nie byłaby w stanie zmienić historii transakcji bitcoinem, ponadto nie mogłaby wydrukować dodatkowego bitcoina, ani zmienić zasad ogólnych takich jak limit łącznej liczby bitcoinów możliwych do wykopania (21 milionów), czy ilości bitcoinów nagrody za każdy wykopany blok (przyspieszenie tempa wykopywania bitcoina).

Taki spisek górników jednakże byłby w stanie kontrolować zawartość 51% wykopywanych bloków, mógłby więc część z nich wypuszczać puste albo wszystkie wypuszczać puste, przez co przepustowość sieci bitcoin spadłaby o połowę (dokładnie o 51%) i mogła zatwierdzać np. 3 a nie 7 transakcji na sekundę. Jest to tak zwany atak odmowy usługi, który do tego jest rozproszony, bo umożliwia go grupa podmiotów, a nie jeden (ang. *DDOS – Distributed Denial Of Service*).

Efektem takiego ataku będzie zwielokrotnienie wartości opłat za transakcje bitcoinem (ang. *fees*), ponieważ przelewy będą rywalizowały o dwa razy mniejszą dostępność miejsca (aby je uwiecznić na bloku danych). To z kolei spowoduje, że kopanie bitcoina stanie się wielokrotnie bardziej opłacalne, przez co do kopania bitcoina dołączy wielu nowych górników. Łączna moc kopania bitcoina wzrośnie, przez co redukcji ulegnie udział spiskowców i z czasem 51% spadnie do poziomu, w którym atak tego rodzaju będzie bardzo nieskuteczny i przede wszystkim nadal bardzo kosztowny.

Dysponowanie mocą obliczeniową 51% oznacza, że średnio 51% nowych bloków będzie wykopywanych przez daną grupę, a pozostałe 49% przez pozostałych górników (a nie że wszystkie nowe bloki są pod kontrolą grupy mającej większość mocy obliczeniowej). Mając przewagę mocy obliczeniowej nie można przelać czyjeś bitcoiny na własne konto, ponieważ oprócz mocy obliczeniowej uwieczniającej taką operację trzeba też dysponować kluczem prywatnym do autoryzacji przelewu.

Przy takich zdolnościach pojawia się jednak teoretyczna możliwość zrobienia przelewu na czyjeś konto, poczekania 10 minut, aż dany przelew znajdzie się na bloku (odbiorca otrzyma jedno potwierdzenie) i otrzymania czegoś w zamian (na przykład równowartości bitcoinów przy zamianie ich na dolary). Następnie trzeba przepisać historię transakcji (wyprzedzając pozostałych górników w tworzeniu nowych bloków) z wersją rejestru już bez tego przelewu, aby zachować wydane uprzednio bitcoiny.

Już sama możliwość podwójnego wydania własnych bitcoinów zakłada, że sieć będzie na coś takiego pozwalać i nie będzie na taki scenariusz w ogóle gotowa. W rzeczywistości wszystkie stowarzyszenia, których moc kopania przekracza 50% zdolności generowania hashy przez wszystkich górników są podejrzewane z definicji o taką działalność.

Dlatego scenariusz, w którym taka szajka górników wykona przelew na przykład na giełdę kryptowalutową, następnie szybko wycofa swój stan posiadania do postaci dolarów i wycofa z giełdy te dolary, by następnie zmienić historię transakcji na taką, w której nie doszło do przelania bitcoina na konto giełdy (przypomina to cofnięcie czasu), jest bardzo mało prawdopodobny.

Po pierwsze taka grupa musiałaby od nowa wykopać wszystkie bloki od momentu pierwszego przelewu, co automatycznie oznacza, że ich moc musiałby mocno przekraczać 50%, ale nawet gdyby się to udało, odtąd każdy wprowadziłby sztuczne opóźnienia przy transakcjach z takim oszukańczym podmiotem. By uchronić się przez ponownym atakiem tego rodzaju wystarczy czekać wystarczająco długo (10, czy 12 potwierdzeń, czyli 2 godziny czekania wystarcza by transakcji nie można było już cofnąć, ponieważ trzeba przepisać zbyt wiele bloków ściągając się przy tym z resztą sieci).

dr Zbigniew Galar

P.S.

Autor nie zachęca do zakupu bitcoina, nie odradza zakupu bitcoina, zachęca natomiast do edukacji na temat bitcoina oraz zdecydowanie odradza zakup jakiejkolwiek innej niezdecentralizowanej kryptograficznej waluty.