KRYPTOWALUTY

WIRTUALNE ZŁOTO

Kryptowaluta to termin, który jest nieprzypadkowo zbudowany z dwóch elementów: członu _krypto-_ i rzeczownika _waluta_. Dr inż. Przemysław Kudłacik z Instytutu Informatyki Uniwersytetu Śląskiego wyjaśnia, że to w zasadzie środek rozliczeniowy, ale niezapisany w systemie komputerowym jakiegokolwiek banku, tylko utrzymywany przez tysiące komputerów rozsianych na całym świecie. Zbudowany jest na bazie technologii zwanej _blockchain_, czyli tzw. łańcucha bloków.

REWOLUCYJNA METODA

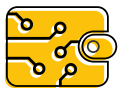
Zanim pojawiły się kryptowaluty, powstała kryptografia klucza publicznego, czyli kryptografia oparta na dwóch kluczach. Na czym ona polega? Jesteśmy przyzwyczajeni do zasady, że jeśli coś jest zaszyfrowane, to potrzebne jest hasło do odszyfrowania. Cóż z tego, że coś zaszyfrujemy, jeśli musimy w jakiś sposób przekazać hasło osobie, która ma tę wiadomość odczytać. Dlatego wymyślono kryptografię asymetryczną (kryptografia symetryczna oparta jest na jednym haśle, asymetryczna na dwóch hasłach). Metoda była rewolucyjna, bo pozwalała zaszyfrować coś jednym hasłem, ale aby odszyfrować, potrzebne było drugie hasło. To rozwiązanie jest dziś powszechnie wykorzystywane, m.in. przez bankowość elektroniczną, podpisy elektroniczne, wojsko, a także w zakresie bezpieczeństwa w internecie. Kryptografia jest także podstawą technologii kryptowalut.

WOLNOŚĆ, ANONIMOWOŚĆ I DECENTRALIZACJA

W 1982 roku amerykański naukowiec oraz kryptograf David Chaum zaproponował, aby wykorzystując kryptografię klucza publicznego, stworzyć wirtualną gotówkę działającą w sposób anonimowy. Była to istotna zmiana, gdyż podstawową cechą funkcjonujących wówczas nośników danych informatycznych były taśmy magnetyczne, co było związane z publicznym charakterem i otwartym dostępem do płatności online. Cyfrowa waluta według jego wizji miała być w pełni anonimowa, ale oparta na technologii niezupełnie przypominającej dzisiejszy _blockchain_. Pomysły Chauma stały się podwalinami tzw. ruchu _cypherpunks_, który narodził się w 1992 roku. Ludzie związani z tym ruchem stawiali na totalną prywatność, anonimowość i bez-

Fot. panoramaphotos - Freepik.com

> Czy coś, co nie istnieje fizycznie, może mieć wartość?



pieczeństwo poprzez wykorzystanie kryptografii.

W pewnym sensie był to powrót do tradycyjnej waluty, jaką było kiedyś złoto czy srebro. Zanim nastąpiły czasy cyfrowe, istniała nota bankowa, czyli banknot, który potwierdzał własność złota czy srebra (dolar amerykański miał kiedyś pokrycie w złocie). David Chaum zaproponował, żeby zamienić ową notę bankową w wartość cyfrową, do której będzie miał prawa tylko ten, kto ma klucz prywatny.

JAK POWSTAJĄ KRYPTOWALUTY?

Czy coś, co nie istnieje fizycznie, może mieć wartość? Złoto i srebro mają wartość, bo nie tylko istnieją fizycznie, ale potrzebne są konkretne nakłady finansowe, energia, zasoby, praca ludzi, aby je wytworzyć. Na Ziemi istnieje ponadto ograniczona podaż tych kruszców i nie da się złota czy srebra wydobyć więcej, niż jest w naturze. A jak jest z „kopaniem" kryptowalut?

Od początku istnienia bankowości cyfrowej ludzie zastanawiali się, jak zabezpieczyć bazy danych, ponieważ hakerzy nieustannie usiłują się do nich włamać. Często też infekują tysiące komputerów na całym świecie, aby jednocześnie łączyły się z danym bankiem i obciążały serwery, które pod tym naporem nie obsługują żądań. To tzw. ataki DDoS (ang. *Distributed Denial of Service*). W latach 90. XX wieku wymyślono sposób ochrony przed atakami DDoS. Pomysł narodził się przy pracy nad przeciwdziałaniem spamowi poczty e-mail. Cynthia Dwork i Moni Naor zaproponowali przeprowadzenie zadania kryptograficznego, które będzie wymagało zaangażowania części mocy obliczeniowej komputera. Ten swoisty rodzaj zagadki polegał na tym, aby przed wysłaniem maila komputer na podstawie jego treści rozwiązał zadanie kryptograficzne. Wynik zadania, czyli konkretna liczba, był dołączany do treści maila.

To rozwiązanie zostało również wykorzystane do implementacji „kopania" kryptowalut, a proces nazwano dowodem pracy (ang. *Proof of Work*). Zaangażowanie mocy obliczeniowej komputera ma kluczowe znaczenie. Jak zostało wspomniane wcześniej, żeby można zdobyć złoto czy srebro, musi być zaangażowana wiedza specjalistów, energia czy sprzęt. To samo jednak jest potrzebne, aby powstawały kryptowaluty, tylko one powstają w formie cyfrowej. Aby wirtualnym „górnikom" opłacało się wspieranie tego rozproszonego systemu informatycznego, wprowadzono rywalizację, w której komputery szukają pewnej specjalnej, dość złożonej liczby. Zadanie nie jest łatwe i potrzebna jest moc obliczeniowa komputera. Komputer, który najszybciej odnajdzie właściwą liczbę, wygrywa prawo dodania nowego bloku do łańcucha i otrzymuje nagrodę w kryptowalucie, a wyścig zaczyna się od nowa. W bitcoinie założono od samego początku i nie zmieniono do dzisiaj, że nowa strona (nowy blok) zwierająca transakcje klientów w bazie danych, czyli łańcuchu bloków, dodaje się średnio co 10 minut. Dodatkowym elementem motywujących do kopania jest uzyskiwanie prowizji od zatwierdzonych transakcji – można otrzymać zapłatę za wydobycie kryptowaluty oraz za walidację transakcji.

SATOSHI NAKAMOTO

To pseudonim osoby (lub grupy osób), która jest łączona z powstaniem bitcoina, czyli pierwszej kryptowaluty. To on wpadł na pomysł, żeby wykorzystać proces zagadki kryptograficznej do powstawania cyfrowego złota. Ogłosił to 31 października 2008 roku w manifeście pt. *Bitcoin: Elektroniczny system pieniężny peer-to-peer* (ang. *Bitcoin: A Peer-to-Peer Electronic Cash System*).

3 stycznia 2009 roku zostało napisanych 30 tys. linii kodu, co uważane jest za początek sieci Bitcoin. Od początku założono, że bitcoinów (BTC) będzie 21 milionów. Każdy BTC dzieli się na 100 mln części, tzw. *satoshi*, czyli bitcoinowych „groszy". Bitcoinów do systemu nikt nie może dosypać, w programie ograniczono, że za około 100 lat zostanie wydobyty ostatni BTC. Warto dodać, że większość bitcoinów już jest wydobyta (ok. 19 mln). Dlatego co 4 lata nagroda dla „górników" jest zmniejszana o połowę – jest to tzw. *halving*. 5 października 2009 roku Satoshi Nakamoto „wykopał" pierwszy blok i wygenerował 50 BTC. Po czterech latach „nagroda" wynosiła już 25 bitcoiny. Obecnie to 6,25 BTC.

WADY I ZALETY

Do największych zalet kryptowalut należy na pewno transparentność systemu, decentralizacja oraz solidne zabezpieczenia. Zauważono jednak, że model rywalizacji może prowadzić do ogromnego zużycia energii. Duże kontrowersje budzi także anonimowość. Brak przejrzystej informacji na temat użytkowników otwiera bowiem możliwości dla świata przestępczego.

dr Agnieszka Sikora

dr inż. Przemysław Kudłacik
Instytut Informatyki
Wydział Nauk Ścisłych i Technicznych
Uniwersytet Śląski
przemyslaw.kudlacik@us.edu.pl