Scientia PAUperum

Bitcoin

Pojawienie się pieniądza kilka tysięcy lat temu, jako pośrednika wymiany towarowej, było kluczowym czynnikiem determinującym szybkość i kierunek tworzenia się społeczeństw ludzkich oraz rozwoju cywilizacji. Jego historia obejmuje pierwsze formy wymiany barterowej, gdzie rolę pieniądza może pełnić w zasadzie dowolny towar, poprzez bardziej uniwersalne środki płatnicze, głównie metale szlachetne, następnie pieniądz papierowy − stanowiący dokument potwierdzający prawa własności do kruszcu, do obecnego systemu walut fiducjarnych, istniejących w cyfrowych rejestrach banków i opierających się jedynie na zaufaniu do instytucji je emitujących. W erze informacji w sposób naturalny nadszedł więc czas na kolejną odsłonę wirtualizacji pieniądza, czyli na kryptowaluty.

Bitcoin (BTC) został zaproponowany przez osobę lub grupę osób pod pseudonimem Satoshi Nakamoto w 2008 roku. Jest to system sieci równoprawnych użytkowników (peer-to-peer), przechowujący informację o przeprowadzonych transakcjach. Można to sobie wyobrazić jako rozproszony publiczny rejestr księgowy w formie łańcucha bloków (blockchain), zawierający całą historię transakcji, a jego kopię ma każdy zainteresowany użytkownik sieci. Pozwala to bez pośrednictwa centralnego serwera (np. banku) na ustalenie, kto ile bitcoinów posiada w danym momencie. Dopuszczalna przez protokół maksymalna liczba bitcoinów nie może przekraczać 21 mln, a każdy dzieli się na 100 mln satoshi.

Przeprowadzenie transakcji bitcoinem polega na przesyłaniu do sieci zaszyfrowanej informacji o transferze określonej liczby bitcoinów pomiędzy adresami. Informację może odczytać każdy za pomocą klucza publicznego, ale formułować je może tylko posiadacz klucza prywatnego danego adresu. Za weryfikację transakcji w sieci Bitcoin (pisana dużą literą oznacza cały system) odpowiadają inni użytkownicy tej sieci – wtedy zwani górnikami – podejmujący się potwierdzania transakcji przez skuteczne włączenie bloku tych transakcji do łańcucha bloków. Polega to na zebraniu krążących po sieci Bitcoin transakcji (maksymalna pojemność bloku to 1 MB), a następnie kompresji informacji w nich zawartych za pomocą funkcji skrótu (haszującej). Wynik kompresji danego bloku transakcji, aby mógł być włączony do łańcucha, musi mieć szczególną postać – posiadać określoną liczbę zer na początku. Ustala to algorytm Bitcoina, dopasowujący trudność tak, że nowy blok jest dołączany co kilka minut. Określony wynik można uzyskać tylko metodą prób i błędów poprzez dodanie liczby zwanej „nonce” do transakcji w bloku. Praca górnika polega właśnie na szukaniu „nonce” i jest nazwana kopaniem (mining), przez analogię do wydobywania złota. Za wykonaną pracę otrzymuje się przydzieloną przez protokół Bitcoina nagrodę w postaci nowych – niejako wydobytych – bitcoinów. Nagroda jest zmniejszana o połowę co 210 tys. bloków i w ten sposób maleje wraz ze zbliżaniem się do maksymalnej liczby 21 mln BTC. Obecnie nagroda wynosi 6,25 BTC. Nagroda zostaje uznana po stu następujących po tym bloku dołączeniach bloków kolejnych, co jest traktowane jako ostateczne jej potwierdzenie. W przypadku równoległego zaistnienia dwóch bloków w tym samym czasie dochodzi chwilowo do rozdwojenia łańcucha. Działa wtedy zasada najdłuższego łańcucha. Obowiązujący staje się ten blok, do którego przyłączono więcej kolejnych. W ten sposób dochodzi do konsensusu pomiędzy użytkownikami sieci. Ten mechanizm nazywany jest dowodem pracy (proof of work). Górnikiem może zostać każdy, jednak przy wzroście aktywności użytkowników sieci potrzebne są do tego coraz większe zasoby obliczeniowe, a więc i energetyczne. Dla zachęty przewidziane są opłaty od nadawcy zlecenia za jego przetworzenie.

Bitcoin od swoich narodzin – wykopania pierwszego bloku w 2009 roku – przeżył spektakularny rozwój. W pierwszej nieoficjalnej transakcji, zawartej na forum internetowym w maju 2010, za dwie pizze warte wtedy około 30 USD zapłacono 10 000 BTC. W lipcu 2010 została uruchomiona pierwsza giełda umożliwiająca zorganizowaną wymianę BTC na USD – platforma Mt.Gox, a w grudniu 2017 roku za 1 BTC na giełdach kryptowalut płacono już blisko 20 tys. USD. Co naturalne i w zasadzie typowe dla wszystkich rynków, po tak gwałtownych wzrostach notowań przyszło załamanie. Zdarzyło się w grudniu 2018, że 1 BTC kupiono już tylko za 3 tys. USD. W roku 2020 zaczęła się jednak kolejna hossa. Obecnie (luty 2021) wycena BTC przekracza 50 tys. USD, a kapitalizacja wszystkich bitcoinów zbliża się do 1 bln USD. Dzienny ich obrót na giełdach jest rzędu kilkunastu miliardów USD. Zaczynają się nim także interesować duzi gracze, jak PayPal, który w październiku 2020 udostępnił użytkownikom możliwość przechowywania BTC oraz jego konwersję na tradycyjne waluty. Także Tesla Elona Muska ogłosiła, że w styczniu 2021 zainwestowała w BTC równowartość 1,5 mld USD. Powszechne użycie BTC jako środka płatniczego jest trudne, bo sieć Bitcoin może potwierdzić maksymalnie kilka transakcji na sekundę. Istnieją jednak miejsca, gdzie można zapłacić bezpośrednio za pomocą BTC, np. w sklepie internetowym konsoli Xbox Microsoftu. Również w dużych polskich miastach w galeriach handlowych można natknąć się na tzw. bitomaty, pozwalające zamienić BTC ze swojego adresu na wypłacone złotówki.

Fenomen Bitcoina jest także niezwykle ważny z perspektywy poznania naukowych aspektów funkcjonowania rynków. Po raz pierwszy w historii doświadczamy tu możliwości w pełni ilościowej analizy dynamiki rynku finansowego od jego powstania do, w zasadzie, pełnej już dojrzałości. Po okresie początkowej kilkuletniej ‘niezdarności’ charakterystyki statystyczne jego wyceny, typu rozkłady stóp zwrotu czy różnorakie korelacje czasowe, w ciągu ostatnich 5 lat stają się praktycznie nieodróżnialne od tych dla starych uznanych światowych rynków, takich jak rynki akcji, towarów, obligacji czy tradycyjnej wymiany walut. Ilościowe analizy prowadzące do takich wniosków zostały przez nas przeprowadzone i w obszernej postaci zostały właśnie opublikowane w Physics Reports 901 (2021) 1-82
https://doi.org/10.1016/j.physrep.2020.10.005.

STANISŁAW DROŻDŻ & MARCIN WĄTOREK
Instytut Fizyki Jądrowej PAN oraz Politechnika Krakowska