O kryptowalutach słów kilka
Autor tekstu: **Sylwia Gałązka**

Kto z Was, Czytelnicy i Czytelniczki, pamięta jeszcze czasy bez e-mailów? Pisanie listów na kolorowej papeterii, czerwone i zielone skrzynki Poczty Polskiej ? (I czy ktokolwiek chociaż raz skorzystał z tych zielonych?)

Miało to swój niezaprzeczalny urok, to prawda, ale jednak trudno sobie wyobrazić dzisiaj życie bez poczty elektronicznej. Tak to już jest, że nawet wtedy, kiedy pojawia się nowa technologia i znacząco ułatwia nam wszystkim życie, zachowujemy pewien sentyment do starszych rozwiązań. Kto wie, może już za kilka lat będziemy po raz kolejny zmuszeni wybrać między sentymentem a pragmatycznością w związku z pojawieniem się tzw. kryptowalut.

Spieszę z wyjaśnieniem: Kryptowaluty, czyli inaczej mówiąc waluty kryptograficzne — to względnie nowy, mało znany ale całkiem rewolucyjny system płatności za pośrednictwem internetu. Pierwszą w historii i zarazem najpopularniejszą jak do tej pory kryptowalutą jest Bitcoin (BTC). Ten niepozorny z początku wynalazek niejakiego Satoshi Nakamoto trafia obecnie z pewną regularnością na pierwsze strony takich gazet jak Wall Street Journal, skupiając na sobie coraz większą uwagę inwestorów. Chociaż bitcoin istnieje od 5 lat, zainteresowanie nim wzrosło znienacka w 2013 roku, wywołując ogromną bańkę spekulacyjną, dzięki której w szczytowych momentach jeden BTC był wart nawet 1200 dolarów! Niestety, ostatnio usłyszeliśmy o nim po raz kolejny w związku ze znacznie mniej korzystną wiadomością: Mt. Gox, największa i najstarsza giełda wymiany BTC na dolar amerykański, ogłosiła niedawno bankructwo. Media szumnie obwieściły — po raz kolejny — koniec bitcoina, co zdarzało się już kilkukrotnie przy okazji mniejszych czy większych komplikacji, ale ten jakoś nie nadchodzi. O dziwo, tragiczna dla wielu wiadomość o bankructwie Mt. Gox nie spowodowała długotrwałego i drastycznego spadku kursów — po kilkunastu godzinach można już było zaobserwować powolny wzrost i powrót do normalności, co świadczy jedynie o tym, jak wielu wierzy w przyszłość kryptowalut.

No dobrze, ale co to tak właściwie jest i na czym polega?

Zacznijmy od początków. W 2008 roku osoba bądź grupa osób, ukrywających się pod pseudonimem „Satoshi Nakamoto" publikuje pracę, w której przedstawia projekt międzynarodowej, zdecentralizowanej waluty, opartej na kryptografii klucza publicznego, w której transakcje byłyby realizowane nie przez bank, a rozproszoną siatkę użytkowników na wzór sieci p2p. Na podstawie tego dokumentu powołuje następnie do życia Bitcoin, a ponieważ oprogramowanie doń jest oparte na otwartym kodzie źródłowym, w ciągu kilku lat dochodzi do namnożenia się wszelkiej maści alternatywnych walut, takich jak Litecoin, Peercoin czy Dogecoin. Niektóre z nich są zwykłymi kopiami, inne starają się wprowadzać innowacje. W obecnej chwili jest ich już kilkadziesiąt i ciągle powstają nowe! Większość z nich co prawda po krótkim czasie wymiera, nie zdobywszy popularności, jednak co najmniej kilka jest warte zainteresowania i w dalszej części artykułu postaram się je przybliżyć.

Wracając do naszego porównania z pocztą i emailem: Wyobraźmy sobie, że piszemy list. Wysłanie listu wymaga, aby po stronie zarówno nadawcy jak i adresata znajdował się Urząd Pocztowy, który przyjmie, przewiezie i dostarczy nasz list na miejsce. Urząd Pocztowy zatrudnia armię listonoszy i innych pracowników, której utrzymanie kosztuje, a więc płacimy za ich usługi kupując odpowiedniej wartości znaczek. Następnie pozostaje nam już tylko uzbroić się w cierpliwość i czekać. A gdybyśmy chcieli wysłać maila? Możemy to zrobić za darmo, nieporównywalnie szybciej, no i wyeliminowaliśmy przy okazji całą masę pośredników. I takie właśnie możliwości oferuje nam użycie kryptograficznych pieniędzy. Posiadając kilka takich przykładowych „monet", jestem w stanie w ułamek sekundy wysłać je do dowolnej osoby na Ziemi, bez żadnych dodatkowych opłat, a do tego robię to osobiście. Moje środki znajdują się w cyfrowym „portfelu", a więc mogę dokonywać płatności online — lub nawet zbliżeniowo, używając telefonu, jeśli jest wyposażony w NFC — ale jednocześnie pozostaję w najdosłowniejszym sensie posiadaczką moich pieniędzy: nie oddaję ich na przechowanie do banku czy innej instytucji, mając doń zaufanie, że zawsze będzie wypłacalna.

Dodatkowo mogę zachować przy tym pewną anonimowość, pomimo tego, że każda transakcja jest zapisywana na stałe w publicznym „bloku". Każdy może sprawdzić stan każdego portfela i jego historię wykonanych operacji, ale nie da się do tego portfela połączyć z konkretną osobą — chyba że sama ujawni, że jest jego właścicielem. Z tego powodu bitcoin zdobył też — niestety — sporą popularność w ciemnych zakamarkach internetu, jak choćby zamknięta przez amerykańską policję giełda Silk Road, gdzie handlowano narkotykami, bronią i nielegalnymi rodzajami pornografii. Warto jednak zauważyć, że dokładnie te same wady posiada też gotówka.

Hej ho, hej ho… czyli jak zostać kryptogórnikiem

No dobrze, załóżmy, że mamy już portfel interesującej nas kryptowaluty. Co dalej? Skąd wziąć środki?

Najłatwiej byłoby po prostu wymienić kilka złotówek, euro bądź dolarów na którejś z kilku dostępnych giełd. Jeżeli jednak jesteśmy posiadaczami komputera z dobrej jakości kartą graficzną, możemy spróbować tzw. kopania lub inaczej miningu.

Jak wiemy, transakcje wykonywane w kryptograficznych pieniądzach są weryfikowane przez siatkę p2p. Nie ma jednej centralnej serwerowni, ale ktoś musi się jednak tym zajmować — gdyby nikt nie pilnował poprawności danych, moglibyśmy przecież wydać albo otrzymać te same środki po kilka razy! Na szczęście, użytkownicy na całym świecie „wypożyczają" moc obliczeniową swoich komputerów, aby system mógł sprawnie działać. Specjalny program wykrywa bloki zaszyfrowanych transakcji i potwierdza ich zgodność, rozwiązując zadanie matematyczne, tzw. hash. Kiedy praca nad jednym takim blokiem dobiegnie końca, użytkownik lub użytkownicy, którzy pomogli w jego rozwiązaniu otrzymują zapłatę w postaci nowo wygenerowanych „monet". W ten sposób siatka domowych komputerów, która przetwarza transakcje w kryptowalutach, jest jednocześnie ich emitentem. Proces ten zwykło się nazywać kopaniem, przez analogię do wykopywania cennego kruszcu z kopalni. Osoby zaangażowane w tego typu działalność często określają się też mianem górników.

Początkowo używano do tego celu procesorów (CPU). Szybko jednak okazało się, że do obliczania zgodności hashy dużo lepiej nadają się karty graficzne (GPU). Kopanie tym sposobem stało się na tyle opłacalne, że zaczęto budować w tym celu specjalne „koparki" — komputery poskładane z najtańszych części, ale wyposażone w trzy do pięciu wysokiej jakości kart graficznych, których jedynym zadaniem było kopać, kopać, kopać...

Rozpoczął się specyficzny wyścig zbrojeń. Masowo powykupywano ze sklepów najmocniejsze karty, szczególnie te z rodziny ATI Radeon. Wreszcie na rynku pojawiły się dedykowane urządzenia, tzw ASIC (Application-specific integrated circuit) które poza kopaniem nie mają żadnego innego zastosowania, ale za to są znacznie wydajniejsze i zużywają znacznie mniej energii.

Pojawienie się tych ostatnich podzieliło górniczą społeczność na przeciwników i zwolenników ASIC, przy czym większość zdaje się uważać je za zagrożenie dla decentralizacji i niezależności kryptowalut.

Producentom tworzącym kolejne, coraz wydajniejsze generacje ASIC bardziej opłaca się bowiem zaprzęgać je do pracy i zagarniać pokaźne zyski z kopania, niż sprzedawać je konsumentom — i tak niestety rzeczywiście się dzieje. Jest to ogromny problem szczególnie w przypadku Bitcoina oraz spokrewnionych z nim walut opartych na algorytmie SHA-256. Wystarczy bowiem, że jeden podmiot zgromadzi 51% całej mocy obliczeniowej, która utrzymuje Bitcoin w obiegu, a będzie w stanie wpływać na jego właściwości czy nawet fałszować transakcje.

Na szczęście, oprócz SHA-256 istnieją jeszcze waluty oparte na algorytmie Scrypt. Posiada on kilka istotnych różnic (jak wymóg większej ilości pamięci RAM), które sprawiają, że tworzenie dla niego maszyn ASIC jest (w tej chwili) nieopłacalne. Dzięki temu zjadacze chleba wyposażeni w jedną bądź kilka kart graficznych są jeszcze w stanie na nich zarabiać. Pierwszą walutą opartą na Scrypt był Litecoin, powstały w październiku 2011r. Od tego czasu przytłaczająca większość nowych kryptowalut, które mnożą się w tej chwili niczym króliki na wiosnę, jest oparta właśnie na tym algorytmie. Część z nich to w prostej linii kopie Litecoina, część jednak stara się wprowadzić jakieś modyfikacje i ulepszenia, które w razie pojawienia się urządzeń ASIC zdolnych poradzić sobie ze Scryptem (które podobno mają się pokazać już w drugiej połowie tego roku) stanowiłyby dodatkowe zabezpieczenie.

Nie tylko Bitcoin

Wynalazek pana Nakamoto doczekał się mnóstwa naśladowców i innowatorów. I bardzo dobrze, bo ma też swoje wady. Przykładowo — ostateczna liczba wszystkich bitcoinów, jakie kiedykolwiek znajdą się w obiegu, jest ustalona odgórnie i zawarta w kodzie, a wynosi 21 milionów. Po wykopaniu ostatniego bitcoina górnicy będą więc zarabiać już tylko na opłatach za transakcje, które co prawda pozostaną dobrowolne, ale będą zapewne stopniowo rosły, żeby zachęcić górnika do szybszego przetworzenia bloku. Nikt przecież nie będzie chciał czekać godzinami, aż jego przelew dotrze i zostanie potwierdzony! Do tego liczba aktywnych górników prawdopodobnie będzie malała — bo po co upierać się przy bitcoinie, skoro mamy do wyboru tyle alternatywnych walut? Lepiej przecież poszukać tej najbardziej opłacalnej i na nią właśnie przestawić swoje maszyny.

Kolejną wadą — paradoksalnie — jest wysoka wartość bitcoina. W chwili pisania tego artykułu jest to 1670 zł za 1 BTC. Oznacza to, że gdybyśmy mieli płacić bitcoinami na co dzień, większość płatności odbywałaby się w ułamkach — przykładowo 0,001191 BTC za bochenek chleba. Jak widać, nie byłoby to zbyt praktyczne. Potrzebna nam więc waluta, której wartość w przybliżeniu odpowiadałaby 1 dolarowi, euro czy choćby złotówce, żeby dało się nią wygodnie operować. Na szczęście, mamy w tej kwestii spory wybór.

Litecoin, czyli pierwsza kryptowaluta oparta na algorytmie Scrypt, określana jest czasami jako „srebro" przez analogię do bitcoina, który stał się kryptograficznym „złotem". Jej twórcy chwalą szybkość przeprowadzania transakcji (średnio 2,5 minuty, gdzie w przypadku bitcoina 10 minut to minimum). Ostateczna ilość wszystkich wyprodukowanych jednostek ma wynosić docelowo 84 miliony, a wartość pojedynczej w chwili obecnej wynosi 13.7$ czyli ok. 41 zł.

Peercoin zmodyfikował nieco mechanizm kopania: wynagradza się użytkownika proporcjonalnie nie tylko do wykonanej pracy, ale i sumy posiadanych monet i czasu, jaki spędziły leżakując w portfelu. W związku z tym jest mało prawdopodobne, aby Peercoin czy jego klony oparte na tym pomyśle zyskały dużą popularność jako środek płatniczy, stworzono go raczej z myślą o długoterminowym przechowywaniu funduszy.

Dogecoin to stosunkowo nowa kryptowaluta i — nie ukrywam — moim zdaniem jedna z ciekawszych. Istnieje zaledwie od trzech miesięcy, ale zdobyła w tym krótkim czasie niespodziewaną popularność.

W jaki sposób?

Doge to mem internetowy, znany w polski wersji jako „pieseł": najprościej mówiąc, jest to zdjęcie psa japońskiej rasy Shiba Inu z wyrazem bezbrzeżnego zdumienia zastygłym na uśmiechniętym pysku. Pewien Australijczyk, niejaki Jackson Palmer, zażartował sobie na Twitterze, chcąc wyśmiać mnożące się w zawrotnym tempie wtórne kopie Litecoina: „Inwestuję w Dogecoin, to będzie natępny wielki przebój!" W odpowiedzi został wręcz zasypany zachętami i prośbami, aby takowy przebój stworzyć. Niedługo po tym skontaktował się z nim Billy Markus, programista z Oregonu, który podjął się zadania — i tak powstała pierwsza kryptowaluta stworzona z powodu żartu. Paradoksalnie, być może właśnie to „niepoważne" podejście sprawiło, że w ciągu trzech miesięcy od powstania Dogecoin zajmuje już czwarte miejsce pod względem kapitalizacji rynku kryptowalut i zaczyna się wokół niego rozkręcać pokaźny biznes. Dogecoin podbił serca internautów, a co najważniejsze sprzedawców, i w tej chwili możemy już zapłacić dogecoinami za najróżniejsze dobra począwszy od kart upominkowych, po komputery, koszulki i inne akcesoria, a skończywszy na… domu, który pewien mieszkaniec Minnesoty postanowił wystawić na sprzedaż za 100 milionów Doge, lub 135 tysięcy dolarów. Od strony technicznej, Dogecoin jest oparty w prostej linii na algorytmie Scrypt, ale jest go w obiegu ogromna ilość, bo aż 55 miliardów, co powoduje, że wartość pojedynczego Dogecoina jest znikoma: wynosi około 0.0011 centa, a tysiąc dogecoinów to ok. 1,6 dolara. Być może ułatwia to od strony psychologicznej posługiwanie się Dogecoinem, bo jakoś nie szkoda wydawać monety, której wartość mierzy się ułamkiem centa.

Zdecydowanie największym atutem Dogecoina jest zorganizowana wokół niego społeczność. Fani tego niecodziennego projektu mają wyrobioną w środowisku opinię sympatycznych, przyjaźnie

nastawionych do nowicjuszy, i co ciekawe, szczerze zainteresowanych większym zróżnicowaniem w swoich szeregach, m.in. przez zwiększanie uczestnictwa kobiet. Nade wszystko jednak udało im się zasłynąć dzięki akcjom charytatywnym: tylko w zeszłym miesiącu zebrano równowartość 30 tysięcy USD (w dogecoinach, rzecz jasna!) na rzecz fundacji szkolącej psy do pomocy niepełnosprawnym dzieciom, a następnie drugie tyle, aby sfinansować jamajskiej drużynie bobslejowej oraz indyjskiemu saneczkarzowi wyjazd na zimowe igrzyska w Sochi. Całkiem nieźle, jak na walutę, która powstała w wyniku żartu i nie liczy sobie jeszcze nawet 100 dni!

Na koniec ciekawostka — **AURORAcoin**, czyli moneta, która zgodnie z ambitnym planem twórców ma zostać rozdana 25 marca wszystkim zarejestrowanym obywatelom Islandii, a następnie zastąpić islandzką koronę, którą tamtejszy rząd systematycznie dewaluuje od kilku dekad. Jeżeli plan się powiedzie, Islandia może zostać pierwszym w historii ludzkości krajem, gdzie na skalę masową przyjęło się użycie krypto-płatności. Wszystko zależy od Islandczyków — a wieść niesie, że jest to naród niechętny bankom, a otwarty na nowinki technologiczne.

Mam nadzieję, że udało mi się zainteresować przynajmniej część czytelników i czytelniczek Racjonalisty tym niezwykle zajmującym tematem. Nawet, jeśli za rok jeszcze nie będziemy w stanie zapłacić bitcoinami czy dogecoinami za zakupy w księgarni bądź warzywniaku, warto uważnie obserwować rozwój tej technologii. Sądzę, że ma w sobie ogromny potencjał, który dopiero czeka na odkrycie.

Sylwia Gałązka
Była członkini zarządu Polskiego Stowarzyszenia Racjonalistów.
Mieszka w Łodzi.

Pokaż inne teksty autora

(Publikacja: 02-05-2014 Ostatnia zmiana: 03-05-2014)
Oryginał.. (http://www.racjonalista.pl/kk.php/s,9645)