DOI: 10.15199/13.2015.12.13

Ethereum. Rozwój zastosowań technologii Bitcoina

prof. dr. inż. WOJCIECH NOWAKOWSKI

Instytut Maszyn Matematycznych

Artykuł „Bitcoin: A Peer-to-Peer Electronic Cash System" [1] opublikowany w 2008 roku przez Satoshi Nakamoto – nieznanego wcześniej autora, spowodował wykładniczo narastający proces nowych zdarzeń informatycznych, finansowych i prawnych. Po początkowym dwuletnim okresie mozolnego wzrostu, nastąpił wykładniczy wzrost zainteresowania Bitcoinem oraz istotne i coraz szybsze zmiany. Kryptowaluta Bitcoin – jak nazwał ją autor: *a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution,* oparta na technologii łańcucha bloków (ang. *blockchain*) pojawiła się w sieci i na rynku, a jej kurs stale rósł.

Rozwój zastosowań technologii łańcucha bloków nabrał prędkości i obecnie odbywa się w dwóch kierunkach. Pierwszy, to powoływanie do życia ciągle nowych kryptowalut [2]. Jest ich już kilkaset. Nie jest to zaskakujące, bowiem kryptowaluta jest po prostu mniejszym lub większym kodem informatycznym, ulokowanym w sieci. By wprowadzić nową kryptowalutę nie potrzeba ani zezwolenia, ani kapitału. Siła nowo wykreowanej kryptowaluty wynika jedynie z popytu na jej walory. Musi więc powstać tylko społeczność, która stworzy własny rynek wymiany.

Drugi kierunek to ulepszanie Bitcoina, a przede wszystkim ekspansja tego systemu w nowe dziedziny aplikacyjne. Niewielu tylko dostrzegło niemal nieograniczone możliwości informatycznego protokołu Bitcoina i zupełnie pozawalutowych zastosowań tej pierwszej kryptowaluty w historii [4].

Pierwszą na świecie kryptowalutę Bitcoin tworzy oprogramowanie typu *open source* w sieci tysięcy komputerów na całym świecie. Na tej podstawie zbudowana jest już duża infrastruktura tworząca prężnie rozwijający się ekosystem oraz szeroki, nieustannie rozrastający się rynek, którego kapitalizacja sięga 10 miliardów dolarów. Wielu niezależnych hakerów oraz innowacyjnych inwestorów dostrzegło wielki potencjał tego systemu. Dlatego też z każdym dniem powstaje wiele aplikacji, których skrypt opiera się w całości lub fragmencie na protokole Bitcoina. Na bazie tego protokołu zbudowano już takie aplikacje jak *Twister*, będący portalem społecznościowym zbliżonym swoją funkcjonalnością do popularnego Twittera, *Bitmessage* który jest komunikatorem umożliwiającym przesyłanie zaszyfrowanych wiadomości oraz *Namecoin* funkcjonujący jako zdecentralizowany system rejestracji domen i zarządzania ich własnością.

Znacznie ciekawsze niż tworzenie klonów Bitcoina jest więc, jak się okazuje, tworzenie nowych informatycznych światów opartych na uniwersalnych cechach technologii Bitcoina. Niewątpliwie znaczącym, dojrzałym i ekscytującym projektem na tej ścieżce rozwoju jest właśnie Ethereum [3, 5].

Ethereum

Bitcoin jest ogólnie znany jako portal płatności oparty na genialnym protokole. Protokół ten pozwala jednak na stworzenie całego wachlarza innych aplikacji internetowych, nie tylko kryptowalutowych. Przykładem jest nie tylko wspomniany już *Namecoin*, który jest jednocześnie walutą i systemem rejestracji domen internetowych. ale też np. *Colored Coins* pozwalający na przypisywanie Bitcoinom określonych dóbr, w tym obligacji lub konkretnych dóbr materialnych.

Rys. 1. Logo platformy Ethereum (ethereum.org)
Fig. 1. Ethereum platform logo (ethereum.org)

Ethereum jest platformą i językiem programowania, które łączy zalety wspomnianych wcześniej rozwiązań oferując jednocześnie coś więcej. Założeniem Ethereum jest umożliwienie każdemu kto tylko zechce tworzenie aplikacji i udostępnianie jej. „Ether" – waluta, z której system korzysta, jest tylko medium wymiany w ramach zdecentralizowanej sieci potencjalnych odbiorców niezależnie stworzonych aplikacji.

„Ethereum" może służyć do kodyfikowania, decentralizacji oraz obrotu wszystkim, co można sobie wyobrazić. Może on zostać użyty w akcie głosowania, na rynku domen, obrotach finansowych, w crowdfundingu, wspomagać zarządzanie firmą, zawieranie kontraktów i umów, w tym również tzw. *smart contracts*, czyli umów opartych na protokołach komputerowych.

Przykładem takich umów mogą być zakłady sportowe [8]. Zainteresowani obstawiają np. która z dwóch drużyn piłkarskich wygra, następnie system potwierdza wynik i wypłaca pieniądze zwycięzcy bez udziału jakichkolwiek pośredników. Taki zakład ma formę kontraktu, ale nie wyłącznie, pomiędzy dwiema osobami. Kontrakty realizowane na platformie Ethereum funkcjonują autonomicznie jako mechanizmy napędzane przez *blockchain*. Każdy taki kontrakt będzie miał swój własny skrypt i skrypt ten będzie uruchamiany przy każdej z transakcji wysłanej w jego ramach. Załóżmy np., że oso-

ba X powierza osobie Y swoje fundusze w obawie przed ich utratą w przypadku kradzieży jej klucza prywatnego. Osoba X może z własnej woli wypłacać 1% funduszy dziennie, a za przyzwoleniem osoby Y, wypłacanie funduszy nie jest dla osoby X ograniczone. Osoba Y jest jednocześnie upoważniona przez skrypt do wybierania 0,05% dziennie i nie ma możliwości przekroczenia tego odsetku. Jeśli osobie X ktoś rzeczywiście ukradnie klucz, może się ona udać z prośbą do osoby Y o przeniesienie funduszy zanim ukradzione zostanie więcej niż 1%. Osoba Y będzie w stanie odzyskać fundusze, a w przypadku, gdy ona sama nie będzie godna zaufania, osoba X może sama wycofać wspomniane fundusze dwudziestokrotnie szybciej od osoby Y.

Ethereum pozwala na tworzenie wielu rodzajów podobnych skryptów. Można więc stwierdzić, że Ethereum umożliwia skorzystanie z potencjału oprogramowania Bitcoina (ale nie tego samego oprogramowania) każdemu, kto zechce z niego skorzystać, dając niezależność od osób trzecich takich jak banki czy bukmacherzy.

Vitalik Buterin (patrz ramka)

Vitalik Buterin to 19-letni haker, który zaproponował aby wiele innych aplikacji mogło skorzystać z oprogramowania Bitcoin. Zdecydował się połączyć siły z kilkoma innymi programistami i stworzył Ethereum.

System Bitcoina istnieje już od dawna i jest nieustannie ulepszany. Jednak to, co czyni go bezpiecznym, jednocześnie ogranicza możliwości jego rozwijania. Jednym z zagrożeń stojącym przed Ethereum jest więc to, że po przerzuceniu się dużej liczby developerów z Bitcoina na nowy system, powstałby olbrzymi blockchain, którego nie będzie łatwo ogarnąć. Biorąc również pod uwagę ewentualne problemy z bezpieczeństwem i stabilnością, próbny „rollout" sieci jest pomysłem więcej, niż sensownym. Nie ulega jednak wątpliwości, że tego typu projekty to manifestacja kolejnego po Bitcoinie kroku w kierunku niezależności wobec rządów oraz wielkich korporacji. Gdy prace się zakończą, w ręce internautów oddane zostanie kolejne narzędzie pozwalające im rozwiązać we własnym zakresie problemy do tej pory wymagające ingerencji osób trzecich. Dlatego projektowi warto bacznie się przyglądać.

Ethereum to w zamyśle usługa *online*, która pozwala na zbudowanie praktycznie dowolnej aplikacji na wzór Bitcoin i uruchomienie jej w ramach całej sieci obejmującej maszyny zrzeszone w projekcie Ethereum. Bitcoin jest sposobem na wiarygodne przechowywanie i przenoszenie obiektów cyfrowych lub części informacji pomiędzy jego użytkownikami. Dziś służy przede wszystkim przechowywaniu i przesyłaniu cyfrowych pieniędzy, jednak ten sam system może doprowadzić do powstania nowego typu sieci społecznościowych, systemów przechowywania danych i rynków papierów wartościowych. Dzięki protokołom zbliżonym do Bitcoina wszystko

Rys. 2. Informacja o Ethereum na portalu (www.ethreum.org). Fig. 2. Ethereum info (www.ethreum.org)

to może działać bez pomocy organu centralnego likwidując przy tym czynnik ludzki, który prowadzi często do spornych sytuacji i nieprawidłowości w funkcjonowaniu lub egzekucji pewnych zobowiązań.

Przewidując, że Bitcoin będzie zjawiskiem znacznie większym niż powszechnie sądzono, Vitalik Buterin porzucił uniwersytet i zaczął podróżować po świecie, biorąc udział w licznych spotkaniach sympatyków Bitcoina, przyglądając się różnym projektom typu *open source*. Ethereum jest wynikiem tych wszystkich doświadczeń.

Mówiąc inaczej pomysł Ethereum polega na nadbudowaniu nowych rozwiązań na istniejący protokół. Bitcoin magazynuje wszystkie transakcje w publicznym rejestrze zwanym łańcuchem bloków. Rejestr ten leży również, jak już wspomniano, u podstaw aplikacji typu Twistera czy BitMessage. Ethereum wykorzystuje swoją własną wersję takiego rejestru wzbogacona o najróżniejsze aplikacje, które będą mogły być tworzone w uproszczonej wersji języka Python. Ethereum Script, bo tak nazywa się ten język umożliwia tworzenie aplikacji przystosowanych do łańcucha bloków Ethereum.

Ethereum nie korzysta z sieci peer-to-peer Bitcoina

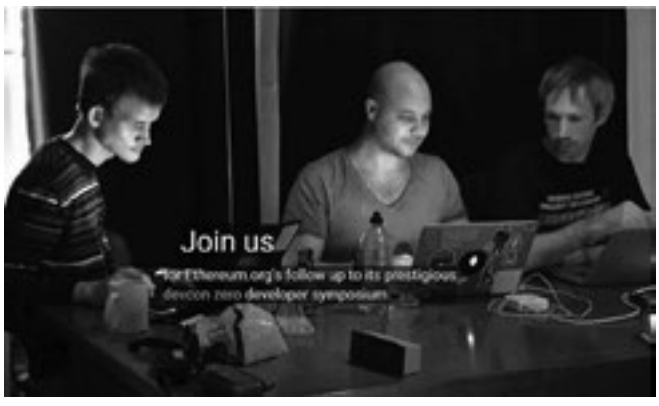
Vitalik Buterin przyjął założenie, że konieczne jest stworzenie zupełnie nowego systemu. Bowiem, jak sam napisał w artykule dla Bitcoin Magazine, mimo że Bitcoin radzi sobie świetnie jako samodzielna kryptowaluta mając przy tym znakomitą cechę skalowalności (nawet tzw. „lekkie klienty", które nie przechowują blockchaina na komputerze ze względu na wolny przesył danych mogą sprawdzić, czy wysłana do nich transakcja rzeczywiście dotarła za pomocą opisanego w Bitcoin Whitepaper protokołu „uproszczone potwierdzenie płatności" (ang. *simplified payment verification*, SPV) [10]. Kiedy jednak na Bitcoina „nałoży" się modyfikacje w rodzaju Colored Coins czy Mastercoin, pojawia się problem. W przypadku pierwszego rozwiązania nie wystarczy użycie wspomnianego wcześniej protokołu SPV do stwierdzenia jakiego koloru jest bitcoin opatrzony specjalnym opisem. By potwierdzić jego istnienie konieczne jest prześledzenie losów tego bitcoina od początku, przeprowadzając jednocześnie test SPV na każdym kroku procedury. Czasami taka wsteczna kontrola przebiega z wykładniczo narastającymi trudnościami. W przypadku zaś programu Mastercoin, nie ma możliwości stwierdzenia czegokolwiek bez sprawdzenia każdej transakcji z osobna.

Ethereum ma za zadanie obejść te problemy. Założeniem nie jest jednocześnie, by system stał się rozwiązaniem spełniającym wszystkie wymagania wszelkich możliwych aplikacji. Podstawową jego funkcją ma być pełnienie roli lepszego niż Bitcoin fundamentalnego protokołu, stanowiącego bazę dla innych zdecentralizowanych aplikacji przy wykorzystaniu flagowych zalet Ethereum: skalowalności i wydajności.

Należy podkreslić, że system Ethereum nie korzysta z sieci peer-to-peer Bitcoina. Nie korzysta też jego oprogramowania. Buterin i jego zespół budują zupełnie nowy system, który będzie działał w ramach własnej sieci i oddzielnym łańcuchu bloków. Jednak w Ethereum, wykorzystano wiele pomysłów i rozwiązań z oprogramowania Bitcoin. Na przykład wszystkie transakcje Bitcoin są przechowywane w tzw. łańcuchu bloków (ang. block chain), pełniącym funkcje globalnej księgi rachunkowej obejmującej każdą transakcję Bitcoin która kiedykolwiek miała miejsce. Jest to więc rodzaj zaszyfrowanej bazy danych z której można korzystać do zasilania innych aplikacji. Ethereum będzie napędzać jeszcze wiele aplikacji oferując, jak już wspomniano język Ethereum Script. Taki system może potencjalnie napędzać każdą aplikację od systemów przechowywania w stylu Dropbox aż po niestandardowe kryptowaluty. Zespół Ethereum udostępnił już klienta alfa, działającego na zasadzie idei proof-of-concept, natomiast sam kod będzie otwarty do wglądu dla każdego programisty, podobnie jak ma to miejsce w przypadku Bitcoin.

Sieć Ethereum wykorzystuje własną technologię wydobycia, Dagger. W celu zapewnienia, że proces wydobycia będzie uczciwy zastosowano niektóre rozwiązania znane z algorytmu górnictwa opartego na architekturze typu *scrypt*, który jest już używany przez kryptowaluty np. w litecoin. Agorytm ten został tak zaprojektowany, aby był bardzo przyjazny dla procesorów typu CPU i znacznie mniej przyjazny dla górników korzystających z układów scalonych typu ASIC po to, aby obecna elita zaawansowanych górników wykorzystujących dziesiątki lub setki maszyn opartych o technologię typu ASIC nie uzyskała nieuczciwej przewagi. Programiści Ethereum ujawnili już wersję oprogramowania, która zawiera język skryptowy Ethereum tak przejrzysty, jak języki C++, Java i Python. Użytkownicy mogą kodować zautomatyzowane umowy i kontrakty, które w rzeczywistości będą reprezentowane przez boty (programy typu robot) mogące wysyłać i odbierać jednostki waluty Ether po spełnieniu pewnych warunków. Chodzi o to, by język kodowania Ethereum umożliwiał wysyłanie pieniędzy za pomocą poleceń, gdy spełnione zostaną warunki zapisane w umowie w postaci odpowiednich linijek kodu.

Ethereum nie jest osamotniony w swoich wysokich ambicjach. Istnieje wiele projektów próbujących dodać inteligentne umowy (ang. *smart contracts*) oraz inne nowe narzędzia i funkcjonalności do systemu Bitcoin. Niektóre z nich, jak QixCoin i Bitcloud budują własne sieci. Inni, jak Colored Coins i Mastercoin, opierają swoje działanie na istniejącej sieci bitcoin. Buterin przyczynił się do powstania zarówno projektu Colored Coins jak i Mastercoin, ale ostatecznie zdecydował, że bardziej sensowne będzie stworzenie zupełnie nowego systemu.



Rys. 3. Zespół Ethereum zaprasza do udziału w pierwszym symozjum o tym systemie (www.ethreum.org)
Fig. 3. Ethereum team invites you to attend the first symposium of this system (www.ethreum.org)

„Widziałem naprawdę inteligentnych ludzi walących swoimi mądrymi głowami o mur podczas prac przy koncepcji Kolorowych Bitmonet (Colored Coins), i ostatecznie zdałem sobie sprawę, że napotykane trudności nie wynikają z ich niewiedzy bądź niewystarczającego doświadczenia. W rzeczywistości problem byłby łatwy do rozwiązania, jednak ludzie mają trudności, ponieważ protokół na którym opiera się system Bitcoin nie nadaje się do nadbudowywania takich zaawansowanych aplikacji" powiedział.

Najwyraźniej instytucje bankowe połknęły haczyk i mimo spadkowej tendencji kursu Bitcoin, do tego ekosystemu wciąż napływa nowy kapitał. W 2014 roku łączna suma funduszy pochodzących z *venture capital* przeznaczonych na rozwój start-upów opierających swoje działanie o system Bitcoin wyniosła 335 mln dolarów, co stanowi znaczną część środków jakie do tej pory zostały zainwestowane w firmy związane z kryptowalutami. Np. firma Coinbase Inc. otrzymała w styczniu 2015 roku 75 mln USD na inwestycje z szanowanych na świecie instytucji finansowych, m. in. The New York Stock Exchange (NYSE), USAA, BBVA oraz największego japońskiego operatora telefonii komórkowej NTT DoCoMo Inc. Tym samym, po raz pierwszy tradycyjne instytucje finansowe objęły bezpośrednie udziały w przedsiębiorstwie związanym z Bitcoinem. Dyrektor Wykonawczy BBVA Ventures, Jay Reinemann, skomentował to wydarzenie następująco: „Coinbase oferuje kompleksowe usługi dla konsumentów, przedsiębiorców oraz programistów działając na najważniejsze aspekty tego szybko rozwijającego się ekosystemu". To przykład, że świat finansów dostrzegł potencjał Bitcoina oraz technologii blockchain.

(Fot. Jan Miranda)

Vitalik Buterin programista i wizjoner technologii blockchain, znawca Bitcoina, twórca Ethereum (za co otrzymał World Technology Award 2014) urodził się w 1994 roku w Rosji, ale od najmłodszych lat mieszka w Kanadzie. Od poczatku interesował się matematyką i informatyką. Studiował informatykę na Uniwersytecie Waterloo, lecz studia te porzucił. Gdy po raz pierwszy zetknął się z Bitcoinem w 2011 roku, nie zainteresował się tą walutą. – Zignorowałem to powiedział. – Myślałem, że Bitcoin nie ma żadnej wartości, więc spisałem go na straty.
Przez kilka tygodni śledził jednak rozwój tego projektu. Pierwsze bitmonety otrzymał jako zapłatę za artykuły pisane dla serwisu Bitcoin Weekly. Na każdym publikowanym tekście zarabiał 5 bitmonet. Ta suma reprezentowała wówczas równowartość 3,75 dolarów. – To była moja pierwsza prawdziwa praca, za którą dostawałem około 1,30 dolarów za godzinę – powiedział.

Perspektywy Ethereum [3, 8, 9]

Mimo, że aplikacje, które opierają swoje działanie o sieć Bitcoin mają tę zaletę, że wykorzystują istniejącą infrastrukturę i korzystają z bezpieczeństwa jakie daje sam system, są one ograniczone przez architekturę i rozwiązania zastosowane w oprogramowaniu hosta (klienta Bitcoin). Przykładowo Bitcoin oferuje własny język skryptowy, jednak jest on obecnie ograniczony jedynie do zapewnienia i zagwarantowania bezpieczeństwa samego systemu. Ograniczenia te miały sens jedynie w początkowej fazie istnienia Bitcoin, gdy idee tworzące się wokół tej nowej waluty były nowe i niesprawdzone. Jednak teraz, kiedy Bitcoin wydaje się być systemem stabilnym i bezpiecznym, najwyższy czas, aby nieco poeksperymentować i znaleźć sposób na jego uelastycznienie.

Należy jednak pamiętać, że przed projektem Ethereum stoi kilka wyzwań. Wiele osób martwi się, że łańcuch bloków Ethereum będzie szybko rosnąć do niebotycznych rozmiarów jeśli znajdzie szerokie zastosowanie. Buterin uważa, że zespół może rozwiązać ten problem, ale nie może mieć zupełnej pewności do momentu, w którym sieć zacznie działać. Bezpieczeństwo jest kolejnym dużym problemem z jakim muszą się uporać programiści, dlatego niedawno zespół uruchomił sieć testową przed oficjalnym uruchomieniem projektu.

Innymi słowy obecne czasy to pierwsze dni dla tego typu nowatorskich rozwiązań programistycznych. Jednak Ethereum i inne krypto-platformy nowej generacji zarysowują bardzo atrakcyjny obraz naszej przyszłości internetowej. Taki, w którym użytkownicy, a nie rządy czy wielkie korporacje mają wszystko pod kontrolą. Budowanie takiej przyszłości to zadanie wymagające ogromnego wysiłku zarówno od programistów jak i całego społeczeństwa entuzjastów Bitcoin.

Literatura

[1] Satoshi Nakamoto: Bitcoin: A Peer-To-Peer Electronic Cash-System. http://pl.scribd.com/doc/275175747/Bitcoin-A-Peer-To-Peer-Electronic-Cash-System

[2] Wojciech Nowakowski: Postęp w technologii systemów kryptowalutowych. Elektronika 11/2015?

[3] Tomasz Szast: Projekt Ethereum odpowiedzią na bolączki systemu Bitcoin? http://paybit.pl/projekt-ethereum-odpowiedzia-na-bolaczki-systemu-bitcoin

[4] Wojciech Nowakowski: Technologie Bitcoina w Internecie Rzeczy (IoT)? Elektronika 10/2015, str. 58–60, DOI: 10.15199/13.2015.10.11

[5] ethereum.org

[6] Vitalik Buterin explains Ethereum. https://youtu.be/TDGq4aeevgY

[7] Stephan Tual: What is Ethereum? Film wideo (10 min). https://youtu.be/Clw-qf1sUZg

[8] Mateusz Kocot. Ethereum – „Bitcoin" który potrafi wszystko. http://bitcoinet.pl/2014/04/03/ethereum-bitcoin-ktory-potrafi-wszystko

[9] Vitalik Buterin: Cryptoeconomic Protocols In the Context of Wider Society. Part 1. https://youtu.be/S47iWiKKvLA Part2. http://youtu.be/qM8zkzFZVok

[10] http://satoshicounter.com/2015/07/14/satoshibooklet/