DOI: 10.15199/13.2015.10.11

Technologie Bitcoina w Internecie Rzeczy (IoT)?

prof. dr. inż. WOJCIECH NOWAKOWSKI

Instytut Maszyn Matematycznych, Warszawa

„Blockchain tworzy krajom zarówno możliwości jak i wyzwania. Choć nie jest regulowany ani nadzorowany przez żaden bank centralny ..., to jednak stwarza nowe mechanizmy podatkowe, które mogą być wbudowane w łańcuch bloków, np. niewielki podatek od każdej transakcji... ...Innowacje takie jak bitcoin jeszcze przed rokiem 2023 będą miały wpływ na ekonomię globalną...”.

Z raportu Światowego Forum Ekonomicznego (World Wconomic Forum, WEF)
niezależnej organizacji ekonomicznej założonej w 1971 roku w Szwajcarii,
w której corocznych konferencjach uczestniczy ponad 2500 prezesów
najbogatszych światowych korporacji, liderów państw, intelektualistów i dziennikarzy.

Cechy systemu Bitcoin

Kryptowaluta Bitcoin zadebiutowała w 2009 roku i jakkolwiek zostało zaproponowanych już w sieci kilkaset różnych innych, to właśnie ten wirtualny środek płatniczy jest na świecie dominujący. Organy podatkowe, ścigania i regulacyjne prawie wszystkich rozwiniętych krajów świata nadal zajmują się badaniem tego zjawiska, jednak jeden problem jest nadal nierozwiązany – czy bitcoin jest pieniądzem legalnym, czy też nie.

Bitcoiny nie są emitowane przez żaden bank centralny i nie podlegają kontroli jakiekolwiek instytucji. Nowe jednostki bitcoina generowane są w sieci. Jednostki te nie istnieją w postaci fizycznej, tworzone są software'owo. Podobnie realizowane są wszelkie operacje jak. np. płatności P2P (ang. *peer-to-peer* – równy z równym, sieć w której wszystkie węzły są równorzędne), przelewy i przechowywanie na koncie. Ze względu na sieciowy charakter tych czynności, są one transgraniczne, a na dodatek prawie dokładnie anonimowe. Bitcoin jest za to ryzykowny – jego kurs zależy wyłącznie od podaży i popytu na ten środek płatniczy, a zmiany tego kursu mogą być w obu kierunkach szybkie i duże. Bitcoin jest więc międzynarodową walutą wirtualną i łatwym narzędziem realizacji płatności za towary i usługi w sklepach i firmach internetowych. Waluta ta jest ponadto przedmiotem obrotu na giełdach.

Bitcoin a prawo

Mimo upływu pięciu lat od narodzin kryptosystemu Bitcoin nie istnieją jak dotąd wyraźne regulacje, które ograniczają, porządkują lub zakazują jego stosowanie. Większość krajów nadal analizuje sposoby prawidłowej regulują tej kryptowaluty i nie ma jasnych ustaleń dotyczących jej legalności Bitcoin pozostaje więc w szarej strefie, bowiem jak zazwyczaj skok technologiczny pozostawił daleko w tyle regulacje prawne.

W USA stosunek instytucji państwowych do aplikacji Bitcoin jest ogólnie pozytywny. Kilka agencji rządowych podjęło działania w kierunku zapobiegania transakcjom nielegalnym. Wiele znaczących firm (np. Dish Network, Dell czy Overstock) chętnie przyjmują płatności w tej walucie. Bitcoin został też wprowadzony do transakcji na rynku instrumentów pochodnych i coraz częściej mówi się o jego uzasadnionej obecności. Zajmujący się gromadzeniem i analizą danych dotyczących transakcji finansowych w celu przeciwdziałania praniu pieniędzy, finansowaniu terroryzmu i innym rodzajom przestępstw finansowych amerykański urząd FinCEN zobowiązał już na początku 2013 roku do rejestracji i prowadzenia dokumentacji transakcji, przy czym bitcoin został zdefiniowany nie jako waluta, ale jako usługa w zakresie „pieniądza biznesu”. Podobnie jest w Australii i Kanadzie gdzie operacje bitcoinami są postrzegane jako transakcje barterowe, z których dochód jest opodatkowany.

W Unii Europejskiej nie wydano żadnej oficjalnej decyzji w sprawie legalności ani żadnych centralnych wytycznych – poszczególne kraje UE kształtują swój własny stosunek do tej kryptowaluty. W Finlandii i Belgii bitcoin jest traktowany nie jako waluta a towar, którego sprzedaż zwolniona jest z podatku VAT. Na Cyprze, obrót bitcoinami nie jest nielegalny, nie jest także kontrolowany i regulowan. Wielka Brytania wykazuje postawę pro – tworzy się otoczenie regulacyjne, aby wspierać te walutę. Podobnie jest w Bułgarii i Niemczech, gdzie bitcoiny są legalne, a nawet opodatkowane.

W wielu krajach stosunek do kryptowaluty Bitcoin oraz innych podobnych pomysłów jest negatywny, by nie powiedzieć wrogi. Na przykład w Wietnamie obrót bitcoinami traktowany jest jako działanie podejrzane , a nawet przestępcze, podejmowane w celu pranie brudnych pieniędzy. W Islandii, Boliwii, Kirgistanie i Ekwadorze powstały już regulacje prawne zakazujące obrotu tą kryptowalutą. W Rosji legalność obrotu bitcoinami jest kwestionowana, Ministerstwo Finansów Rosji planuje opracować ustawę o zakazie obrotu tą walutą jeszcze w tym roku. Najciekawsze i zróżnicowana jest sytuacja w Chinach. Jakkolwiek wszystkie banki i inne instytucje finansowe nie akceptują zawierania transakcji lub obrotu bitcoinami, to jednak na rynku prywatnym waluta ta kwitnie. Chiny to jeden z największych na świecie bitcoinowych obszarów płatności między osobami prywatnymi.

Rys. 1.
Fig. 1.

To nie tylko kryptowaluta. Łańcuch bloków

Jakkolwiek Bitcoin jako waluta i system płatniczy jest aplikacją interesującą, to jeszcze bardziej interesujące, zwłaszcza dla dużych firm informatycznych, są niektóre tylko procedury, jakie ten system płatniczy zastosował i upowszechnił. To przede wszystkim technologia łańcucha bloków (ang. *blockchain*), która może okazać się znacznie bardziej wartościowa dla przyszłości niż Bitcoin sam w sobie.

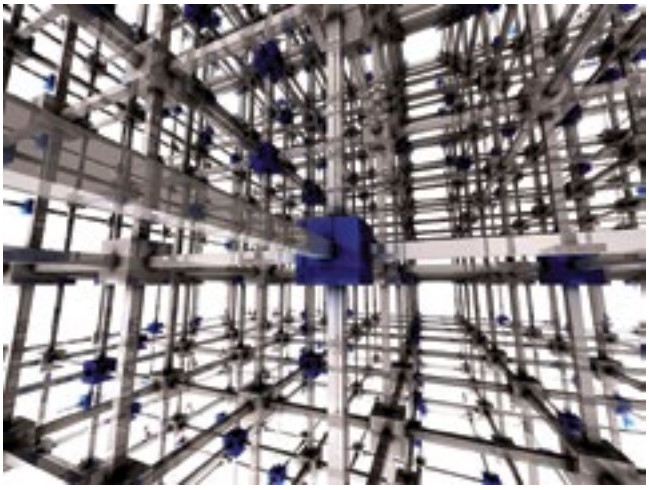
Technologia łańcucha bloków została został zastosowana przez twórcę (twórców) kryptowaluty Bitcoin jako rejestr wszelkich transakcji w tym systemie. Transakcje te są grupowane w blokach w celu ich weryfikacji, po czym bloki te są po kolei dołączane do łańcucha poprzednio zweryfikowanych bloków tworząc kompletny zapis wszystkich transakcji dokonanych w systemie od początku jego istnienia. Ten właśnie rejestr bloków to *blockchain*.

Technologia łańcucha bloków jest dość szeroko wykorzystywana. Inne znane, choć mniej rozpowszechnione kryptowaluty jak np. Litecoin czy Dogecoin również tworzą łańcuchy bloków. Wiele różnych innych projektów wykorzystuje własne łańcuchy bloków do przechowywania danych innych niż zapisy transferów finansowych. Projekt Namecoin (fork Bitcoina) wykorzystuje łańcuch bloków do rejestracji obrotów domenami internetowymi. Technologia ta jest również wykorzystywana np. do rejestracji prostych programów, które automatycznie przenoszą fundusze, gdy spełnione są określone warunki.

Wejście Big Blue

Ostatnio wielkim zainteresowanym implementacją technologii łańcucha bloków w bardziej tradycyjnych zastosowaniach niż kryptowaluty okazał się Big Blue, czyli jeden z najstarszych koncernów informatycznych – IBM.

IBM rozwija swoją własną wersję tej technologii *blockchain*. Jest to spektakularna wiadomość i zarazem najnowszy znak, że tą technologią zainteresował się świat wielkich korporacji. IBM „odkrył", że łańcuch bloków, swoisty system księgowy systemu Bitcoin, może być zastosowany w wielu dziedzinach bankowości, ale też i Internetu Rzeczy (IoT). Pozwoli też na tworzenie umów cyfrowych, które – jak w transakcjach bitcoinowych będą rejestrowane publicznie i zatwierdzane w światowej sieci komputerowej.



Rys. 2. Wizja graficzna rozproszona sieci urządzeń, czyli zdecentralizowanego Internetu Rzeczy (www.coindesk.com)
Fig. 2. Graphic vision of distributed network of devices – a decentralized Internet of Things (www.coindesk.com)

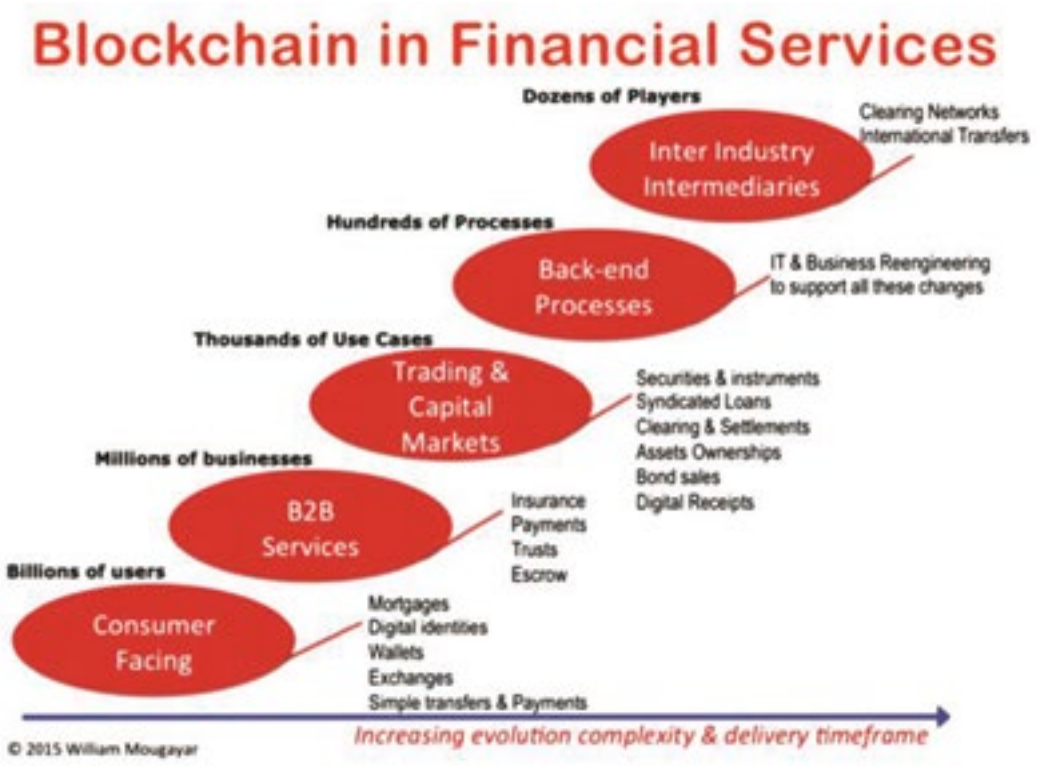
Koncepcja systemu ADEPT (ang. *Autonomous Decentralized Peer-to-Peer Telemetry*) została formalnie zaprezentowana przez IBM wspólnie z firmą Samsung na targach CES 2015 w Las Vegas. ADEPT jest projektem badawczym dotyczącym zastosowania sieci peer-to-peer i technologii łańcucha bloków do zdecentralizowanej wersji Internetu Rzeczy (IoT). Podstawę systemu jest wykorzystanie narzędzia matematycznych dowodów wykonanych operacji tzw. dowodów wykonanej pracy (ang. *Proof of Work, PoW*).

Arvind Krishna, wiceprezes i dyrektor IBM Research, który prowadzi ogólną strategię techniczną firmy IBM, a wcześniej był dyrektorem generalnym IBM Systems ds. rozwoju najnowszych technologii nadzorującym pracę ponad 3000 naukowców i technologów w 12 laboratoriach IBM na świecie napisał na blogu:

„To zupełnie nowa architektura dla biznesu. To fundament nowej generacji aplikacji transakcyjnych, które tworzą zaufanie i przejrzystość a jednocześnie usprawniają procesy biznesowych... ...Jest ona niezbędna by znacznie zmniejszyć koszty i móc efektywnie się rozwijać".

IBM uważa technologię łańcucha bloków za przebój w dziedzinie wymiany danych, a w szczególności skok jakościowy w udostępnianiu dokumentację i przeprowadzaniu wszystkich rodzajów transakcji, również w bardziej tradycyjnych walutach. Firmy mogłyby bowiem „księgować" transakcje z dostawcami na całym świecie w udostępnionym łańcuchu bloków, a nie w postaci zwykłej wymiany danych pomiędzy odrębnymi bazami. Wypożyczalnie samochodów na przykład, mogłyby używać inteligentnych umów, które automatycznie realizowałyby usługę po otrzymaniu informacji o płatności i ubezpieczeniu wprost z łańcucha bloków.

Inteligentne urządzenia mogłyby nawet z łańcucha bloków zamiast połączenia z tradycyjnym serwerem w chmurze. Na przykład lodówka wyposażona w czujniki i podłączona do Internetu mogłaby że korzystać z danych zawartych w łańcuchu bloków i automatycznie zarządzać interakcją ze światem ze-



Rys. 3. Prognozowane obszary zastosowań łańcucha bloków w usługach finansowych (www.coindesk.com)
Fig. 3. BlockChain in Financial Services (www.coindesk.com)

wnętrznym, od zamówienia i zapłaty za artykuły spożywcze po aktualizacje oprogramowania. Warto przy tym zauważyć, że projekty tego rodzaju, w odróżnieniu od systemu Bitcoin mogą wykorzystywać łańcuchy niepubliczne dostępne tylko dla zaproszonych użytkowników sieci, z różnymi uprawnieniami dla różnych użytkowników.

Prace dotyczące zastosowania technologii łańcucha bloków w branży finansowej są także prowadzone w dziewięciu największych bankach, w tym Goldman Sachs, JP Morgan, Credit Suisse i Barclays. Sklep internetowy Overstock.com, który rozpoczął niedawno przyjmowanie bitcoinów, również rozwija swoją własną technologię łańcucha bloków na platformie obrotu papierami wartościowymi. Platforma ta ma rozliczać transakcje znacznie szybciej niż tradycyjne giełdy.

Technologia łańcucha bloków, która została rozpowszechniona przez popularny już system transakcyjny Bitcoin może więc doprowadzić do wielu w zupełnie nowych obszarów gospodarki. To kolejny znak, jak wielkie możliwości innowacyjne może przynieść zastosowanie kryptografii w świecie współczesnej informatyki.

Literatura

[1] Wojciech Nowakowski, Kryptografia współczesna. Monografia. ISBN 978-83-927542-4-4. Stron 121. IMM 2014

[2] Wojciech Nowakowski, Kryptograficzne aspekty technologii wirtualnej waluty BitCoin. Elektronika – konstrukcje, technologie, zastosowania, nr 5/2013, str. 58–62.

[3] Wojciech Nowakowski, Silent Circle – zaklęty krąg nowoczesnej kryptografii dla wszystkich. Elektronika – konstrukcje, technologie, zastosowania, nr 12/2014, str. 38–40.

[4] Wojciech Nowakowski, Nowe problemy kryptowaluty Bitcoin: błąd w Android i zablokowanie procesu „kopania" monet. Elektronika – konstrukcje, technologie, zastosowania, nr 12/2013, str. 52–53.

[5] Wojciech Nowakowski, Bliższa chmura, czyli usługi obliczeniowe we mgle. Elektronika – konstrukcje, technologie, zastosowania, nr 5/2015, str. 34–37.