DOI: 10.15199/13.2015.11.26

Postęp w technologii systemów kryptowalutowych

prof. dr. inż. WOJCIECH NOWAKOWSKI

Instytut Maszyn Matematycznych, Warszawa

Kryptowaluta (ang. *cryptocurrency*), czy inaczej waluta kryptograficzna to pieniądz wirtualny bazujący na prawach i procedurach kryptografii. Ujmując ściślej, to rozproszony system księgowy, wykorzystujący funkcje kryptograficzne, w którym zostają zapisane utajnione informacje o transakcjach i stanie posiadania umownych jednostek w taki sposób, aby nikt poza właścicielem nie miał do tych danych dostępu.

W istocie kryptowaluta to system informatyczny, który generuje wirtualne jednostki pieniężne i umożliwiają obrót tymi jednostkami kontrolowany metodami kryptograficznymi w sposób autonomiczny, niezależny od twórców systemu, administracji i otoczenia prawnego. Kryptografia wdziera się zresztą powszechnie do aplikacji internetowych, w których niezbędne są procedury uwiarygadniania [3, 11, 12].

Kryptowaluty na rynku

Kryptowaluty są już faktem rynkowym. W roku 2009 pojawiła się pierwsza koncepcja kryptograficznego pieniądza wirtualnego o nazwie Bitcoin [1]. Był to powszechnie dostępny w internecie zespół aplikacji informatycznych, stanowiący kombinację różnych procedur i algorytmów kryptograficznych, poprzednio ze sobą niewiązanych: Funkcji Skrótu, drzew Merkla, Dowodu Pracy (Proof-of-Work) oraz całego instrumentarium kryptografii klucza publicznego. Obecnie ta kryptowaluta jest najbardziej rozpowszechnioną kryptowalutą na świecie [2, 3, 4].

Kryptowalut może być nieskończenie wiele Każdy bowiem użytkownik internetu może stworzyć swoją kryptowalutę i „puścić" ją w obieg. Otwartą sprawą jest, czy nowo powołany kryptopieniądz znajdzie użytkowników, którzy zaangażują swoje tradycyjne środki lub pracę dla zdobycia nowych jednostek, a także czy znajdą się ci, którzy będą przyjmować te jednostki w zamian za towary czy usługi. Stale więc powstają w sieci klony Bitcoina, ale też i nowe, oryginalne systemy kryptowalutowe, wykorzystujące środowisko internetowe: otwarte oprogramowanie oraz sieć P2P.

Obecnie notuje się ponad 300 kryptowalut na 15 giełdach kryptowalut (tzw. kryptogiełdach, czyli serwisach internetowych, w których użytkownicy składają oferty kupna i sprzedaży kryptowalut). Istnieją poza tym setki innych, o niekiedy dziwnych nazwach i jeszcze bardziej dziwnych oznaczeniach np. Unobtanium (UNO), Cryptogenic Bullion (CGB), Philosopherstone (PHS), RadioactiveCoin (RAD), SherlockCoin (SHC), ThorCoin (THOR), ZeusCoin (ZEU), HomoCoin (HOMO), LoveCoin (LOVE), WikiCoin (WIKI), Revolution Coin (CHE), FourtyTwoCoin (42), OctoCoin (888), Megacoin (MΣC), H2Ocoin (H2O), Deutsche eMark (DEM), FuckCoin (FKC, FUCK), BabyCoin (BBC), NyanCoin (lub Nyan Cat, NYAN).

Poniżej przedstawiono szerzej znane obecnie kryptowaluty w kolejności chronologicznej według daty publikacji ich, posiadające przynajmniej jedną z poniższych cech:

- kapitalizacja minimum 1 milion USD
- innowacyjny protokół
- szersze uznanie w skali światowej
- brak doniesień o przestępczym wykorzystywaniu

Wśród wielu nowych kryptowalut, w styczniu 2014 roku pojawił się także polski klon Bitcoina – *Polcoin (PLC)* [5]. Jest to pierwsza polska wirtualna waluta, klon popularnego już Bitcoina. Istnieje zarówno w wersji na komputery stacjonarne jak i na urządzenia mobilne. Oto jej główne cechy:
Algorytm: SHA256d
Częstotliwość generowania bloku: 60 sekund
Wartość wygenerowanego bloku: 50 PLC
Zmniejszenie wartości generowanego bloku co: 2100000 bloków
Maksymalna liczba monet w obiegu: 210.000.000
Port sieci: 9338
Port RPC: 9337
Przeliczenie trudności przez sieć następuje co 360 bloków lub 6 godzin.

Rys. 1. Symbol kryptowaluty Polcoin
Fig. 1. Cryptocurrency Polcoin

Efektywność obliczeń Dowodu Pracy (ang. proof-of-work)

Jedną z podstawowych procedur Bitcoina jest Dowód Pracy (ang. *proof of work*) [2]. Podstawowym jej celem jest zapewnienie w ściśle określony sposób kontrolowanej emisji jednostek pieniądza w sieci. Założeniem tej procedury jest to aby zadanie było trudne do obliczenia, ale łatwe do sprawdzenia. Pierwszym współczesnym przykładem zastosowania tego pomysłu to procedura „hashcash", oparta na funkcji skrótu SHA256 stworzona przez Adama Backa w 1996 w celu ograniczenia spamu. Przez wymaganie od każdego maila sporych

Tab. 1. Porównanie wybranych krypowalut. Tabl. 1. Comparison of selected cryptocurrencies

Waluta	Symbol	Data publikacji	Procedura	Metoda dystrybucji	Kapitalizacja rynkowa (USD)
Bitcoin	BTC	03.01.2009	SHA256d	Proof-of-work (fixed, halving)	6,34 mld
Ripple	XRP	01.03.2011	Ripple	centralna	139 mln
Litecoin	LTC	07.10.2011	SCrypt[1)]	Proof-of-work (fixed, halving)	154 mln
Bytecoin	BCN	04.07.2012	CryptoNight[2)]	Proof-of-work (random, smooth)	2,73 mln
Peercoin	PPC	19.08.2012	centralne	Proof-of- stake	15,5 mln
Freicoin	FRC	21.12.2012	SHA256d	Proof-of-work	84 tys.
Feathercoin	FTC	16.04.2013	SCrypt	Proof-of-work (fixed, halving)	1,15 mln
Primecoin	XPM	07.07.2013	Łańcuchy Cunninghama	Proof-of-work	1,2 mln
BitSharesX	BTSX	29.09.2013	Consensus through obscurity[3)]	?	66,5 mln
Nxt	NXT	29.09.2013	Consensus through obscurity	centralna	29 mln
Dogecoin	DOGE	06.12.2013	SCrypt	Proof-of-work (random)	12,7 mln
Darkcoin	DRK	19 Jan 2014	Combo11	Proof-of-work (fixed, curve)	12,5 mln
Monero	XMR	18 Apr 2014	CryptoNight	Proof-of-work (random, smooth)	6,27 mln
MaidSafeCoin	MAID	22 Apr 2014	Bitcoin	centralna	8,54 mln

[1)] *SCrypt* – funkcja skrótu kryptograficznego uważana za jedną z najbezpieczniejszych. Pozwala parametryzować nie tylko wymaganą do obliczeń moc obliczeniową, ale również wymaganą ilość używanej pamięci.

[2)] *CryptoNight* – jest jednym z algorytmów proof-of-work. CryptoNight został wdrożony w technologii CryptoNote (https://cryptonote.org)

[3)] *Consensus through obscurity* – uzgadnianie (słabo) zabezpieczone przez nieznajomość, które oparte jest na pogladzie, że nieznajomość luk w systemie uniemożliwia przeprowadzenie ataku

obliczeń, system czyni nieekonomicznym masowe wysyłanie maili, podczas gdy wymiana maili nie stanowi problemu. To samo rozwiązanie stosowane jest właśnie w celu „kopania monet" czyli kontrolowanej programowo emisji pieniądza Bitcoin.

Mamy przy tym jednak problem ogólnej nieefektywności: obliczenia proof-of-work w sieci Bitcoin to obecnie 72073 trylionów operacji na SHA256 wykonywanych co sekundę, podczas gdy same te obliczenia nie są do niczego przydatne, ani w praktyce ani w nauce. Obliczenia te są bowiem specjalnie utrudniane, by rosła trudność „wydobycia" jednostek waluty w miarę jej emisji. To marnotrawstwo nie jest jednak bezsensowne. Wobec braku alternatywy, jest ono konieczną ceną za zdecentralizowanie i prawie autonomiczne działanie globalnej waluty. W 2009 roku, roku publikacji artykułu Satoshi Nakamoto [1], proof-of-work rzeczywiście był jedyną dostępną automatyczną procedurą emisyjną. Wkrótce pojawiło kilka nowych pomysłów.

Rys. 2. Symbol kryptowaluty Primecoin
Fig. 2. Cryptocurrency Primecoin

Potencjalnie najbardziej obiecującą, choć niepozorną alternatywą dla proof-of-work Satoshiego jest propozycja Sunny'ego Kinga w opracowanej przez niego kryptowalucie *Primecoin* [6]. Zamiast porzucać całkowicie *dowód pracy*, autor stara się uczynić to narzędzie potencjalnie użytecznym. Primecoin wymaga od górników wyszukiwania długich łańcuchów Cunninghama liczb pierwszych – łańcuchów wartości n-1, 2n-1, 4n-1 i tak dalej aż do momentu, gdy wszystkie wartości w łańcuchu są liczbami pierwszymi. Nie jest przy tym oczywiste, w jaki sposób łańcuchy te mogą być użyteczne. Autor zwraca tylko uwagę na to, że większość kosztów produkcji urządzeń wyspecjalizowanych do tradycyjnych obliczeń proof-of-work (np. ASIC) wynika z poszukiwania nowych metod obliczeniowych w nich stosowanych, a nie produkcji samych urządzeń. Propozycja Primecoin mogłaby być więc owocować znalezieniem bardziej wydajnych metod wyliczeń ogólnie arytmetycznych Nie jest to jednak przekonujące.

Dowód Stawki

Nowością w nowo publikowanych systemach kryptowalutowych jest procedura Dowód Stawki (ang. *Proof of Stake*) [7, 8]. To alternatywa dla procedury SHA256 z Bitcoina i podobnych, dzięki której możliwe jest całkowite wyeliminowanie marnowania mocy obliczeniowej właściwej Dowodowi Pracy. Zamiast wymagać od udowadniającego, aby wykonał określoną ilość wyliczeń, proof-of-stake wymaga jedynie okazania określonej ilości posiadanych środków. Satoshi nie mógł tego zrobić sam, gdyż przed rokiem 2009 nie było żadnych „dóbr cyfrowych", które mogłyby bezpiecznie działać w połączeniu z protokołami kryptograficznymi. PayPal oraz inne internetowe serwisy obsługujące karty kredytowe mamy co prawda od ponad 10 lat, ale są to systemy scentralizowane, więc utworzenie w ich ramach systemu Dowodu Stawki umożliwiłoby samemu PayPalowi i innym podobnym mu serwisom np. na fałszywych transakcji. Adresy IP oraz nazwy domen są częściowo zdecentralizowane, ale nie jest możliwe stworzenia takiego dowodu posiadania tych dóbr cyfrowych, który mógłby być sprawdzony w przyszłym czasie. W istocie jedynym wirtualnym dobrem, które może działać jako wirtualny Dowódem Stawki jest Bitcoin lub inne działające kryptowaluty.

Rys. 3. Symbol kryptowaluty Peercoin
Fig. 3. Cryptocurrency Peercoin

Pojawiło się już kilka propozycji odnośnie tego, jak można by wprowadzić Dowód Stawki do użytku; jedynym, który w obecnym momencie działa w praktyce jest Peercoin (też PPCoin lub PPC) [9], również stworzony przez Sunny'ego Kinga. Algorytm sprawdzania bloku Dowodem Stawki w PPCoin polega na wymaganiu od górnika utworzenia transakcji „stawki monetowej" (ang. *coinstake*), czyli wysłania określonej liczby jednostek kryptowaluty posiadanych przez „górnika" do siebie samego. Określona jest przy tym wysokość nagrody (podobnie jak działające w Bitcoinie wynagrodzenie, obecnie 25 BTC jeden blok). Hash w ramach SHA256 wyliczany jest jedynie na podstawie danych transakcji, pewnych dodatkowych niezmiennych informacji oraz aktualnej godziny (podawanej w postaci całkowitej liczby sekund, jakie upłynęły od dnia 1 stycznia 1970). Hash ten jest następnie sprawdzany podobnie jak w Bitcoinie – trudność jest tu jednak odwrotnie proporcjonalna do „wieku monetowego" danych wyjściowych transakcji. Wiek ten określany jest jako wielkość danych wyjściowych transakcji liczony w PPCoinach pomnożonych przez czas przez który wspomniane dane wyjściowe istniały. W zasadzie każdy blok PPCoin odgrywa rolę „symulowanej instalacji górniczej" (ang. *simulated mining rig*) o ciekawej właściwości: jej moc kopiąca rośnie liniowo, a spada do zera za każdym razem, gdy pojawi się nowy blok.

Nie wiadomo, czy używanie wieku monety zamiast wielkości wyniku jest konieczne. Pierwotnym założeniem tego rozwiązania było zapobieganie ponownemu użyciu tych samych monet, ale obecne działanie PPCoin nie pozwala górnikom na świadome próby wygenerowania bloku z określonym wynikiem transakcji (ang. *transaction output*). Zamiast tego, system wykonuje odpowiednik wybierania losowego co sekundę i być może nadawania użytkownikowi prawa stworzenia bloku. Nawet bez użycia wieku jako aspektu losowego system ten jest zbliżony do emisji Bitcoinów, jednak bez marnotrawienia mocy obliczeniowych. Korzyść z uwzględniania wieku monety wynika ze wzrostu szansy na powodzenie rośnie z czasem. Górnicy mogą spodziewać się tworzenia bloków bardziej regularnie, co obniża ryzyko tworzenie klonów zcentralizowanych ośrodków kopiących (ang. *mining pools*).

Qora 2.0

Qora [10] to kryptowaluta drugiej generacji, która po udanym i pełnym obietnic debiucie w roku 2014, w zasadzie upadła. Opóźnienia w upublicznieniu kodu źródłowego spowodowały utratę zaufania i zapoczątkowały nieprzyjemną kampanię dezinformacyjną sugerującą, że Qora nie ma w sobie nic oryginalnego. Społeczność Qory mocno uszczuplała, rozwój kodu stanął w miejscu i ostatecznie twórca sam porzucił swoje dzieło. Ci informatycy, którzy pozostali w społeczności Qory okazali się bardzo lojalni i utalentowani. Po okresie dużej niepewności co do przyszłości, Qora ruszyła na nowo z nowym zespołem. W przeciwieństwie do pierwotnego założyciela, który ograniczał się jedynie do pisania kodu, nowy zespół programistów postanowił równo rozłożyć akcenty i zadbać także o integrację systemu z giełdami oraz marketing, który jest niezwykle istotnym elementem każdego projektu w świecie kryptowalut.

Rys. 4. Symbol kryptowaluty Qora ver. 2
Fig. 4. Cryptocurrency Qora2 symbol

Qora oparta jest na procedurze proof-of-stake, a więc jest wolna od kosztów wydobywania. To powoduje, że interesy ekonomiczne posiadaczy waluty i tych, którzy zapewniaja jej bezpieczeństwo stają się zgodne. W planie rozwoju waluty jest wewnętrzna giełda wymiany aktywów, pseudonimy (tj. połączenie dowolnej informacji z dowolną nazwą, co otwiera możliwość utworzenia zdecentralizowanego rejestru DNS), zdecentralizowany system głosowania, opcja przesyłania wiadomości tekstowych do innych użytkowników i wiele innych funkcji. Np. nowe wcielenie Qory zawiera, poza wbudowanym systemem głosowania i wewnętrzną giełdą wymiany aktywów, nowy portfel z dostępem do zdecentralizowanej sieci społecznościowej, a także daje możliwość tworzenia zdecentralizowanych stron webowych. Zautomatyzowane transakcje, także znane jako *smart contracts* z Ethereum (któremu zostanie poświęcony kolejny artykuł), zostały uruchomione już klika miesięcy temu, równocześnie z niewymagającą zaufania giełdą krypto-do-krypto oraz *Atomic Cross-Chain Transfers*, czyli transakcjom między dwoma niezależnymi łańcuchami bloków (ang. *blockchain*). Uniwersalny portfel działa na wszystkich platformach obsługujących Javę, czyli praktycznie wszędzie.

Duńska giełda CCEDK dodała Qorę do swojej listy kryptowalut, co oznacza, że Qora ma teraz swój nowy dom i nowe źródło płynności. Obsługiwana jest wymiana w relacji do BTC a także trzech tradycyjnych walut: USD, EUR i CNY.

Dowód Stawki w zastosowaniach pozawalutowych

Interesujące są możliwości zastosowania Dowodu Stawki w pozawalutowych aplikacjach. Do tej pory systemy antyspamowe na przykład były zaliczane do trzech kategorii: Dowód Pracy, captcha oraz systemy tożsamościowe.

Dowód Stawki może tworzyć czwartą kategorię działań antyspamowych. Zamiast przepisywać captcha, aby założyć konto na forum, użytkownik może przecież wykorzystać wiek monetowy poprzez wysłanie sobie Bitcoina lub PPCoina. Aby upewnić się, że każde wyliczenie w ramach Dowodu Stawki jest wykonywane przez użytkownika, a nie losowo wyciągnięte z łańcucha bloków, system może wymagać od użytkownika również wysłania podpisanej wiadomości ze zgadzającym się adresem, lub przesłania pieniędzy sobie samemu w losowo określonej kwocie. Zwróćmy uwagę, że wiek monetowy jest tu kluczowy; chcemy bowiem, by użytkownicy mogli tworzyć Dowody Stawki na żądanie, więc jakaś wartość musi zostać skonsumowana, by zapobiec powtórnemu użyciu. W pewnym sensie Dowód Stawki funkcjonuje podobnie, jak potwierdzanie smsem.

Prawdziwy potencjał Dowodu Stawki widać jednak w kontekście zdecentralizowanych systemów typu Bitmessage. Bitmessage silnie szyfruje wiadomości w skrzynce odbiorczej każdego użytkownika i replikuje go wewnątrz swojej sieci P2P w skrzynkach pocztowych innych użytkowników, w celu ukrycia tożsamości użytkownika. Zapobiega to podsłuchiwaniu i chroni sieć przed wszelką kontrolą.

Aktualnie Bitmessage z b raku wyboru korzysta z Dowodu Pracy. Nie ma żadnego „zdecentralizowanego systemu captcha" – nie prowadzono też prac nad jego stworzeniem. Jednakże, Dowód Pracy jest marnotrawny i czyni Bitmessage systemem w pewien sposób niewygodnym i mocożernym. Działa dobrze z emailami, ale nie sprawdza się jako komunikator. Jeśli jednak Bitmessage mógłby zostać zintegrowany z Bitcoinem (lub Primecoinem czy PPCoinem) i używać go jako Dowód Stawki, spora część trudności oraz problemów z marnotrawieniem mogłaby zostać rozwiązana.

Dowód Stawki może być użyty aby zabezpieczać kryptowaluty, ale też w zdecentralizowanych systemach antyspamowych, a także w wielu innych protokołach, których jeszcze nie ma. Podobnie jak nikt nie znał kategorii „kryptowaluta" do czasu publikacji Wei Dai'a [14].

Literatura

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. http://bitcoin.org/bitcoin.pdf

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

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

[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] Polcoin, pierwsza polska kryptowaluta. http://www.polcoin.pl/index.php/pl/

[6] http://primecoin.io

[7] Vitalik Buterin. What Proof of Stake Is And Why It Matters. 2013. https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463

[8] Mateusz Kocot. Czym jest dowód stawki i dlaczego ma on znaczenie. http://bitcoinet.pl/2014/05/20/czym-jest-dowod-stawki-i-dlaczego-ma-on-znaczenie

[9] http://peercoin.net

[10] 2nd Generation Cryptocurrency, http://www.qora.org

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

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

[14] Wei Dai, b-money. 1998. http://www.weidai.com/bmoney.txt