ANONIMOWOŚĆ BITCOINA ZAGROŻENIEM BEZPIECZEŃSTWA

Leszek Lisiecki

Wojskowa Akademia Techniczna

Kamil Kucharski[1]

Streszczenie. Proces globalizacji i rewolucji informacyjnej to zjawiska, które definiują rzeczywistość społeczno-gospodarczą współczesnego świata. Znalazły one praktyczne odzwierciedlenie w funkcjonowaniu systemów pieniężnych w globalnej gospodarce światowej, przede wszystkim w nowej postaci cyberwaluty, jaką jest bitcoin. Przedmiotem artykułu są przesłanki powstania, istota, zasady i sposób działania bitcoina. Jego cechy oraz coraz szerszy zakres funkcjonowania tej cyberwaluty mogą w przyszłości zagrażać bezpieczeństwu w wymiarze społecznym, gospodarczym i międzynarodowym.
Słowa kluczowe: bitcoin, anonimowość, cyberbezpieczeństwo, przestępczość zorganizowana.

Rosyjski noblista Josif Brodski powiedział kiedyś, że oprócz powietrza, ziemi, wody i ognia to pieniądz jest piątą naturalną siłą, z którą najczęściej musi się liczyć człowiek. Warto zastanowić się nad tym, jaką rolę we współczesnym świecie odgrywa pieniądz. Przede wszystkim jest miarą wartości dóbr materialnych, ale również środkiem, dzięki któremu możemy realizować własne potrzeby (niższego oraz wyższego rzędu). Niewątpliwie – zapewniając stabilizację i możliwości nabywcze – determinuje poczucie bezpieczeństwa. Początków pieniądza należy szukać w czasach pierwotnych, kiedy narodził się handel, a różnica w posiadaniu dóbr doprowadziła do pierwszych transakcji wymiany (początkowo towaru za towar). Przez wieki pieniądz ewoluował od pieniądza towarowego, poprzez kruszcowy, papierowy aż do elektronicznego, którego najpopularniejszą formą jest bitcoin, wykorzystywany do obsługi transakcji w skali globalnej, w tym również, a może przede wszystkim, w nielegalnym handlu i finansowaniu przestępczości międzynarodowej.

Przesłanki powstania, istota i kurs bitcoina

Wszechogarniający postęp w dziedzinie informatyzacji i informatyki sprawił, że wiele aspektów życia uległo zmianie. Ten postęp oraz jego efekty w postaci dóbr i usług stały się impulsem powstania nowych rozwiązań nie tylko z dziedziny komunikacji czy bankowości, lecz także codziennej egzystencji. Współcześnie takie usprawnienia jak szybka transmisja danych, połączenia telekomunikacyjne z dowolnego miejsca na Ziemi, płatności zbliżeniowe czy ekspresowe przelewy pieniężne nie są niczym wyjątkowym. Należy stwierdzić, że zachodzące zmiany zdeterminowały

[1] Doktorant WCY WAT.

powstanie elektronicznej waluty. Internetowe płatności są znane społeczeństwu od wielu lat. Niemniej jednak e-waluta, a w szczególności bitcoin (BTC lub XBT), to dla wielu zjawisko nowe, wciąż nieodkryte.

Bitcoin nie jest pierwszą próbą stworzenia cyberpieniądza. Jednym ze swoistych prekursorów współczesnej e-waluty jest DigiCash (DC), którego początki sięgają 1990 roku. Mimo bardzo dobrego systemu zabezpieczeń transakcji, projekt zbankrutował ze względu na brak popularności.

Zainteresowanie walutą internetową wzrosło po popularyzacji portali społecznościowych, na których płacąc rzeczywistymi pieniędzmi, otrzymywało się odpowiednik elektroniczny. Wówczas pozwalał on na nabycie szeregu usprawnień i udogodnień na portalu. Przykładem profesjonalnej waluty internetowej opartej na portalu społecznościowym jest VEN działający w ramach serwisu Hub Culture. Historia cyberwalut zawiera również przykłady systemów opartych na złocie. Najstarszą tego typu walutą jest system e-gold utworzony w 1996 roku. Mimo początkowego sukcesu projekt upadł po 2003 roku, kiedy Departament Sprawiedliwości Stanów Zjednoczonych oskarżył jego twórców o pranie brudnych pieniędzy. Ostatecznie e-gold zamknięto w 2009 roku. Nie powstrzymało to zwolenników kryptowalut opartych na kruszcach, bo w tym samym okresie stworzono pecunix, gbullion oraz e-dinar[2].

Obecnie bitcoin jest zjawiskiem bezprecedensowym. Żadna waluta internetowa funkcjonująca przed BTC nie osiągnęła takiej popularności i rzeszy użytkowników. Nie oznacza to jednak, że jedynie BTC funkcjonuje na świecie. Wśród innych znanych cyberwalut można wymienić: *VEN*, *LiteCoin*, *PPCoin*, *FreiCoin*[3].

Mimo możliwości wyboru, to właśnie bitcoin łączy transakcjami ludzi na całym świecie. Szczególnie przełomowy dla BTC był rok 2013, kiedy odnotował zarówno znaczny wzrost wolumenu transakcji w nim rozliczonych, jak i spadek jego ceny. Wówczas można było zauważyć wpływ sytuacji politycznej i gospodarczej świata na kurs kryptowaluty. Szczególnie istotne okazały się wydarzenia na Cyprze (blokada bankomatów oraz środków finansowych mieszkańców)[4]. 10 kwietnia 2013 r. kurs bitcoina spadł z 250 dolarów na 200. Kolejne dni przynosiły następne obniżki kursu. W krytycznych momentach 1 BTC był wart 75 dolarów. Aktywność Federalnego Biura Śledczego (FBI) zmierzająca do zatrzymania osób korzystających z tej waluty w działalności przestępczej odstraszyła kolejnych inwestorów. Mimo tego w październiku 2013 r. odnotowano wzrost kursu – do poziomu około 200 dolarów. Prawdziwa rewolucja nastąpiła w listopadzie 2013 r., kiedy za 1 BTC pod koniec miesiąca trzeba było zapłacić 1000 dolarów. Na taki jego poziom złożyło się kilka wydarzeń, m.in. uznanie przez zarząd Systemu Rezerwy Federalnej (FED) USA kryptowalut

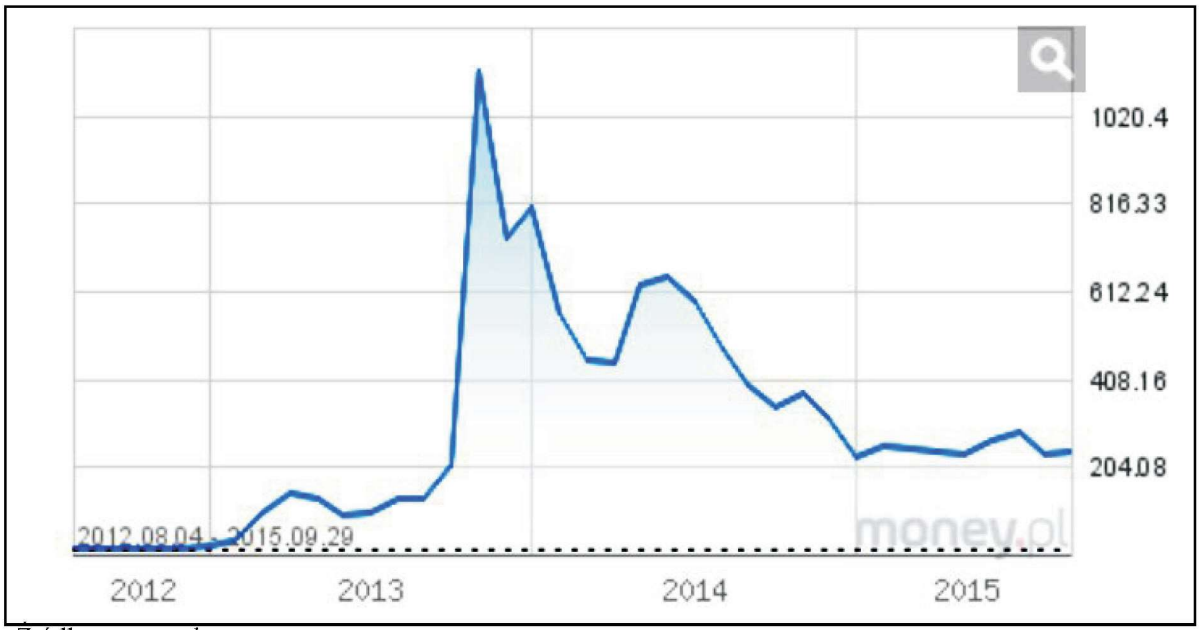
[2] R. Woś, *Waluta hakerów przyszłością gospodarki*, „Dziennik Gazeta Prawna", nr 112, 12-13 czerwca 2011, s. 4-5.

[3] http://gadzetomania.pl/3463,alternatywy-dla-bitcoin-czyli-przeglad-wirtualnych-walut.

[4] http://naszdziennik.pl/ekonomia-finanse/27946,cypr-w-panice.html.

za środek płatniczy taki jak inne waluty i formy płatności[5]. Kurs bitcoina od 2012 r. przedstawiono na wykresie 1.

Wykres 1. Kurs bitcoina w okresie od trzeciego kwartału 2012 r. do trzeciego kwartału 2015 r.



Źródło: money.pl

Zakładając, że bitcoin utrzyma swoją wysoką wartość oraz wciąż będzie rozszerzał się wolumen transakcji, które on obsługuje, można stwierdzić, że kwestią czasu jest akceptacja tej formy płatności przez kolejne podmioty gospodarcze, w tym również państwa.

Cechy, zasady i sposób użytkowania bitcoina

Ekonomiści, informatycy, naukowcy i cała społeczność międzynarodowa, która poznała bitcoina, zastanawia się nad fenomenem jego popularności. Należy zwrócić uwagę na cechy, które charakteryzują walutę internetową, odróżniając ją tym samym od tradycyjnej. To właśnie te różnice determinują popularność BTC. Pewne jest, że działanie oraz zasady użytkowania bitcoina nie są konwencjonalne i tożsame ze zwykłymi transakcjami elektronicznymi. Mimo funkcjonowania w tej samej przestrzeni informatycznej – najpopularniejsza na świecie cyberwaluta niesie ze sobą szereg udogodnień i usprawnień, które z dnia na dzień przyciągają kolejnych zwolenników.

Oficjalne Polskie Stowarzyszenie Bitcoin wyróżnia siedem cech, którymi można scharakteryzować najpopularniejszą kryptowalutę współczesnego świata. Są to:

[5] M. Szymankiewicz, *Bitcoin – wirtualna waluta Internetu*, Helion, Gliwice 2014, s. 26-27.

„anonimowość, decentralizacja, prostota, brak opłat za transakcje, szybkość, brak obciążeń zwrotnych, przejrzystość”[6].

Zjawisko braku anonimowości w sieci jest narastającym problemem. Z jednej strony dzielimy się informacjami o miejscu zamieszkania, skończonych szkołach, odwiedzonych krajach i aktualnych wydarzeniach z naszego życia na portalach społecznościowych. Z drugiej strony dokonując wielu czynności, jesteśmy monitorowani przez banki, pracodawców oraz służby. Można zatem stwierdzić, że zachowanie anonimowości w Internecie oraz życiu jest praktycznie niemożliwe. Każda transakcja wykonywana przy użyciu karty płatniczej jest udokumentowana oraz archiwizowana w zasobach banku. Co więcej, bank analizuje nasze wydatki tak, by zaproponować nam przygotowany przez siebie produkt, np. kredyt na remont mieszkania. Odpowiedzią na te problemy jest bitcoin, ponieważ portfel użytkownika tej waluty nie jest przywiązany do żadnego imienia i nazwiska. W praktyce oznacza to, że wykonywane przez nas transakcje są anonimowe. Nie można zidentyfikować, kto złożył zlecenie na dany zakup oraz na czyje konto trafiają kryptopieniądze.

BTC jest całkowicie zdecentralizowany. W praktyce oznacza to, że żadna instytucja, organizacja, rząd lub inny podmiot nie kontroluje tej kryptowaluty. Ponadto, każde urządzenie, które obsługuje bitcoiny, ma takie same prawa. Jest wiele zalet, ale również wad takiego układu. Przede wszystkim użytkownicy są pewni, że żaden podmiot nie jest w stanie przejąć ich pieniędzy, zamrozić konta lub w jakikolwiek inny sposób utrudnić dostępu do waluty. W ten sposób można uniknąć wydarzeń takich jak np. na Cyprze w 2013 roku. Z drugiej strony, brak regulacji kursu waluty doprowadza do wielu wahań, tak więc spekulowanie na rynku bitcoina jest ryzykowne. Notowania bitcoina reagują w ograniczonym stopniu na wydarzenia geopolityczne, ale są inne czynniki, które sprawiają, że nie jest on do końca tak stabilny jak waluty narodowe.

Wielu użytkowników uważa również, że samo założenie konta oraz użytkowanie bitcoina jest nieporównywalnie prostsze w porównaniu z tradycyjnymi walutami. Na przykładzie Polski należy zauważyć, że posiadanie rachunku bankowego (bez współwłaścicielstwa) wymaga ukończenia osiemnastego roku życia. W innym przypadku należy uzyskać upoważnienie i zgodę opiekuna prawnego. Ponadto konta i portfele bankowe zwykle są płatne, a ich obsługa nie zawsze jest intuicyjna. Znaczna poprawa w tym zakresie nastąpiła po uruchomieniu bankowości elektronicznej. Mimo wszystko BTC swoją prostotą i zasadami użytkowania wyróżnia się oraz jest alternatywą dla płatności tradycyjnych i elektronicznych. Każdy, bez względu na wiek, płeć i pochodzenie, może założyć portfel Bitcoin. Jedyny warunek, jaki musi spełniać, to posiadanie komputera lub smartfona z dostępem do Internetu.

[6] http://www.bitcoin.org.pl/czym-jest-bitcoin/.

Różnica dotyczy również opłat za użytkowanie konta. Tradycyjne banki w Polsce i na świecie naliczają prowizje za np. prowadzenie rachunku, przelew internetowy zewnętrzny, zlecenia stałe, realizację poleceń zapłaty, wydanie karty, użytkowanie karty, wypłaty z bankomatów krajowych oraz wypłaty z bankomatów za granicą. Odnosząc się do BTC, należy stwierdzić, że założenie rachunku nie wymaga żadnych dokumentów, jest bardzo intuicyjne i całkowicie darmowe.

Niewątpliwą zaletą transakcji bezgotówkowych jest szybkość. Funkcjonuje to zarówno w przypadku tradycyjnej bankowości internetowej, jak i przelewów bitcoin. Należy jednak zaznaczyć, że banki stosują w praktyce szereg ograniczeń. Najczęściej używane rozwiązania to błyskawiczne przelewy z rachunku na rachunek, ale tylko w tym samym banku, lub limity wolumenu transakcji. Za inne formy rozliczeń dostawca usług bankowych pobiera określone prowizje lub opłaty stałe. Alternatywą dla tego są serwisy typu PayU. „PayU jest częścią grupy działającej na czterech kontynentach, obsługującej płatności internetowe w siedmiu krajach Europy Środkowo-Wschodniej”[7]. Dzięki tej usłudze jesteśmy w stanie bardzo szybko zapłacić za produkty w sklepach internetowych i serwisach aukcyjnych. Mimo wszystko należy pamiętać, że jest to firma zewnętrzna (pozabankowa). Zupełnie inaczej sprawa wygląda w przypadku transakcji bitcoinowych, gdzie środki finansowe są przekazywane z portfela na portfel w czasie rzeczywistym, tzn. wystarczy odpowiednie podanie danych oraz nasza akceptacja, aby BTC znalazł się na koncie innego użytkownika, niezależnie od tego, jakiego programu Bitcoin używa.

Bardzo istotną cechą transakcji bitcoinowych jest brak obciążeń zwrotnych. Definicji tej operacji jest bardzo wiele, ale na potrzeby tej pracy przyjęto wytłumaczenie najbardziej znanego serwisu internetowego na świecie do płatności elektronicznych w walutach tradycyjnych – PayPal. „Obciążenie zwrotne, nazywane również cofnięciem transakcji, ma miejsce, kiedy kupujący składa u wystawcy karty kredytowej wniosek o cofnięcie transakcji, która już została rozliczona. Kupujący może wystąpić do wystawcy swojej karty kredytowej o obciążenie zwrotne zgodnie z regulaminem i terminami ustalonymi przez stowarzyszenie wystawców kart kredytowych”[8]. Jest to bardzo wygodne rozwiązanie, które chroni nas przed atakami hakerskimi, np. DNS-spoofing.

DNS-spoofing to atak sieciowy polegający na podmienieniu adresu domeny w taki sposób, aby osoba korzystająca z niej nie zorientowała się, że nie znajduje się na prawdziwym serwisie. Ostatecznie korzystając np. z usług bankowych, logujemy się na stronie banku, która jest spreparowana, a co za tym idzie, przekazujemy swoje dane hakerowi. W ten sposób autor ataku zyskuje pełny dostęp do naszego konta i jeśli nie jesteśmy zabezpieczeni dodatkowymi krokami autoryzacji (np. potwierdzenie

[7] http://www.payu.pl/o-nas.

[8] https://www.paypal.com/pl/webapps/mpp/security/sell-chargebackfaq#goto1.

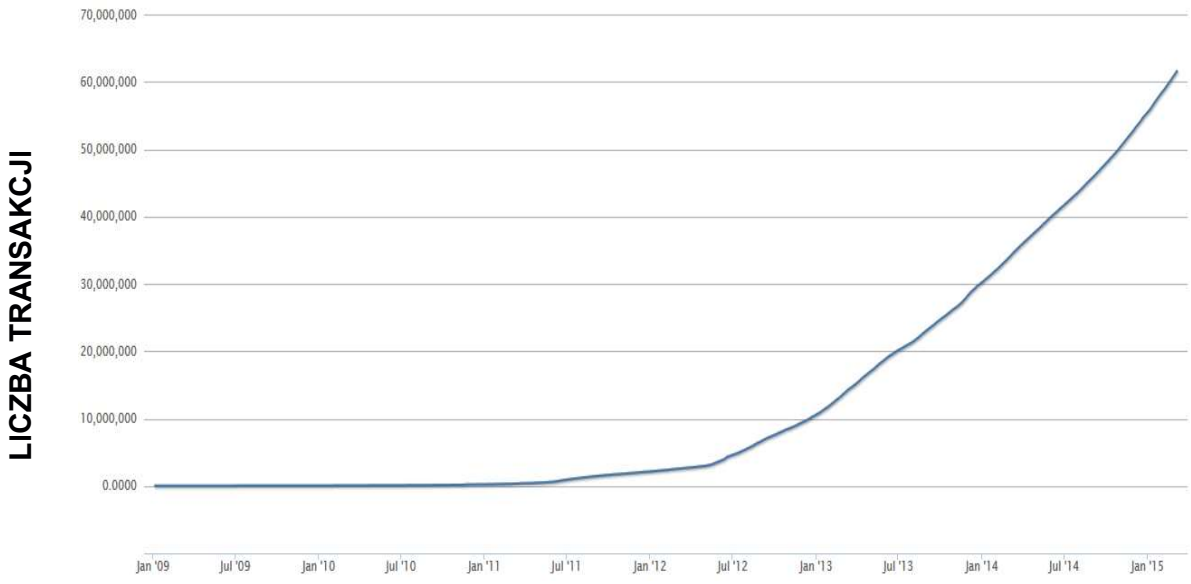
przelewu SMS-em albo kodem jednorazowym), to bardzo prawdopodobne, że środki z naszego konta zostaną utracone[9].

W odpowiedzi na to użytkownik tradycyjnych usług bankowości elektronicznej dysponuje wspomnianym obciążeniem zwrotnym. Brak takiej cechy w transakcjach BTC jest dla jednych wadą, a dla drugich zaletą. Przede wszystkim po wykonanej transakcji nie jesteśmy w stanie odzyskać środków finansowych, jeśli nie posiadamy dostępu do portfela adresata, a co za tym idzie – jeśli popełniliśmy błąd, bitcoiny tracimy bezpowrotnie. Z drugiej strony brak powiązania pomiędzy kontami eliminuje możliwość zidentyfikowania nas. Jest to cecha szczególnie pożądana przez osoby zajmujące się przestępczością zorganizowaną.

Ostatnią cechą, na którą zwraca uwagę Polskie Stowarzyszenie Bitcoin, jest przejrzystość. Oznacza to, że wszelkie zawierane przez nas transakcje są zbierane w portfelu i archiwizowane. W ten sposób wszystkie operacje na koncie są przez nas w pełni kontrolowane. Nie ma również niezrozumiałych przepisów, zmian stawek oprocentowania oraz innych regulacji, które towarzyszą bankowości tradycyjnej.

Wszystkie powyższe cechy określają istotę waluty bitcoin oraz determinują jej niewątpliwy sukces, który osiągnęła w ostatnich latach. Sytuację tę doskonale obrazuje wykres 2, który prezentuje liczbę transakcji wykonywanych w BTC w latach 2009-2015.

Wykres 2. Liczba transakcji w BTC w latach 2009-2015



Źródło: opracowanie własne na podstawie portalu BlockChain.info

[9] M. Szmit, M. Tomaszewski, D. Lisiak, I. Politowska, *13 najpopularniejszych ataków sieciowych na twój komputer. Wykrywanie, usuwanie skutków i zapobieganie*, Helion, Gliwice 2008, s. 68.

Warto zastanowić się, jak w praktyce funkcjonuje najbardziej znany na świecie kryptologiczny pieniądz – bitcoin. Twórcą zarówno protokołu, jak i samej waluty jest Satoshi Nakamoto. Przy czym nie jest to imię i nazwisko, a pseudonim internetowy (tzw. nick). Nikt *de facto* nie zna prawdziwych danych osoby odpowiedzialnej za funkcjonowanie BTC. Wspomniany człowiek (lub grupa ludzi posługująca się tym pseudonimem) opublikował w 2008 roku manifest – tłumacząc tym samym zasady i sposoby użytkowania kryptowaluty.

Satoshi Nakamoto, tworząc protokół, uwzględnił trzy podstawowe zasady, które muszą być spełnione, aby mówić o walucie jako takiej:

- „dana kwota musi być powiązana z konkretnym użytkownikiem,
- daną kwotę można przekazać innemu użytkownikowi,
- przekazana kwota nie może zostać ponownie przekazana przez pierwotnego właściciela”[10].

Twórca, chcąc zrealizować powyższe założenia, użył dwóch mechanizmów kryptograficznych, tj. podpisu cyfrowego oraz funkcji skrótu.

Funkcja skrótu (inaczej funkcja haszująca) to algorytm komputerowy, który zmienia dane wejściowe w określony ciąg znaków alfanumerycznych. W konsekwencji powstaje skrót (tzw. *hash*), który ma stałą długość. Jedną z najbardziej znanych funkcji skrótu jest md5. Wynikiem działania tego algorytmu jest 32-znakowy ciąg zawierający cyfry od 0-9 oraz litery a-f[11]. Funkcja ta jest bardzo często wykorzystywana przy sprawdzaniu poprawności pobranych plików. Wówczas weryfikuje hash pliku pobranego przez nas z hashem pliku znajdującego się na serwerze. Ponieważ sam algorytm wykonywany jest bardzo szybko, jest to jedna z najbardziej popularnych funkcji skrótu wykorzystywanych do obliczania sumy kontrolnej. Rysunek 1 przedstawia wynik funkcji haszującej md5, kiedy danymi wejściowymi jest słowo „Bitcoin”.

Warto zauważyć, że funkcji skrótu nie można odwrócić, tzn. mając jej wynik, nie jesteśmy w stanie sprawdzić, jakie były dane wejściowe. Ponieważ algorytm md5 nie jest w stanie zapewnić odpowiedniego poziomu bezpieczeństwa w transakcjach BTC, autorzy wykorzystali funkcję SHA-256. Jest to funkcja haszująca zaprojektowana przez National Security Agency (NSA) jako federalny standard przetwarzania informacji w USA[12].

Drugim elementem zapewniającym bezpieczeństwo i poprawność transakcji BTC jest podpis cyfrowy. Można stwierdzić, że jest to namiastka własnoręcznego podpisu, która ma potwierdzić naszą wolę lub zapoznanie się z dokumentem. W rozumieniu polskiego prawa podpis elektroniczny zawiera „dane elektroniczne

[10] M. Węgrzyn, J. Jabłoński, M. Nowakowski, *Transakcje i monety internetowe. Kryptologia a biznes – bezpieczeństwo stosowane*, Wydawnictwo BTC, Legionowo 2014, s. 81.

[11] M. Szymankiewicz, *Bitcoin – wirtualna waluta Internetu*, op. cit., s. 34.

[12] M. Węgrzyn, J. Jabłoński, M. Nowakowski, *Transakcje i monety internetowe. Kryptologia a biznes – bezpieczeństwo stosowane*, op. cit., s. 80-81.

dołączone do innych danych elektronicznych lub logicznie z nimi powiązane w celu potwierdzenia tożsamości podmiotu podpisującego, który się nim posługuje"[13]. Przez wykorzystanie takiej metody kryptograficznej możliwe jest zidentyfikowanie konkretnego użytkownika, który posługuje się danym podpisem. Co więcej, nie można dokonywać zmian w dokumentach, które już zostały podpisane, bo każda taka próba pozostawia po sobie ślad. Na samym początku podpisu cyfrowego wykorzystuje się omawianą wcześniej funkcję skrótu. Całość tworzy kod, który w obecnych warunkach jest niemożliwy do złamania.

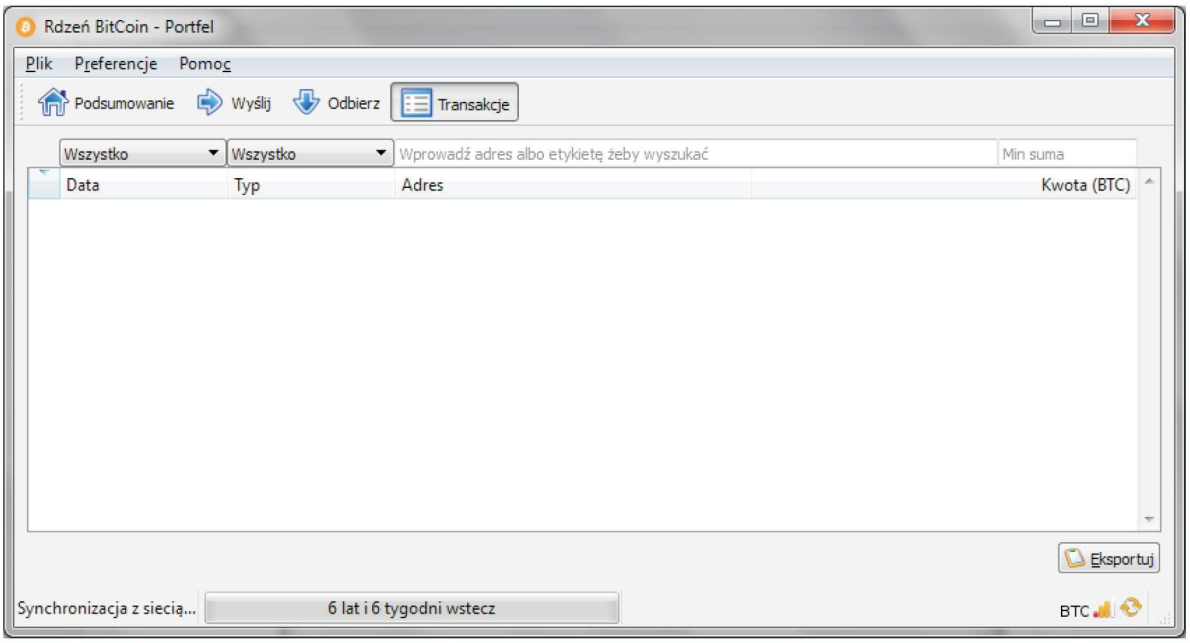
Rys. 1. Wynik algorytmu md5 przy danych wejściowych „Bitcoin"
Źródło: opracowanie własne przy wykorzystaniu *MD5 Online Generator*, www.md5.cz

Transakcja bitcoin przebiega przy wykorzystaniu klucza prywatnego oraz publicznego. Każdy użytkownik tej waluty takie posiada. W celu przesłania BTC do innej osoby wykorzystujemy program Bitcoin (wygląd jednego z najbardziej popularnych programów obsługujących BTC zaprezentowano na rysunku 2).

Program ten tworzy transakcję, w której uzupełniamy wybraną przez nas sumę BTC do przelewu oraz klucz publiczny adresata. Na koniec całość jest podpisywana kluczem publicznym właściciela portfela. Wszystkie wykonywane przez nas transakcje są zapisywane w swoistym archiwum, które określono jako *block chain*. Ponadto po wykonaniu przelewu kryptowaluty informacja ta jest rozsyłana do innych komputerów w sieci[14].

Komputery, które są w sieci, czuwają również nad poprawnością transakcji, tzn. weryfikują, czy osoba przesyłająca BTC rzeczywiście jest w ich posiadaniu oraz czy nie próbuje ponownie ich wykorzystać. Po zaakceptowaniu takiego przelewu, jego dane identyfikujące są dopisywane do bloku (*block)* oraz do łańcucha (*chain*), który archiwizuje całość transakcji wykonanych w BTC od początku istnienia tej kryptowaluty[15].

[13] Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym, Dz.U. z 2001 Nr 130, poz. 1450.
[14] K. Kopańko, M. Kozłowski, *Bitcoin – złoto XXI wieku*, Helion, Gliwice 2015, s. 44-45.
[15] https://blockchain.info/pl/.



Rys. 2. Program Bitcoin Core

Źródło: opracowanie własne przy wykorzystaniu oprogramowania Bitcoin Core, *bitcoin.org*

Ponieważ bitcoin jest walutą zdecentralizowaną, nie ma żadnego podmiotu, który zajmowałby się jego emisją. Stąd też tej cyberwaluty nie można drukować lub wybijać. Jedyną metodą pozyskiwania BTC jest tzw. wydobywanie/kopanie, tłumacząc angielskie słowo *mining*. Istotny jednak jest fakt, że ilość waluty została ograniczona przez jej twórców do 21 milionów. Ostatecznie nigdy na świecie w internetowym obiegu nie pojawi się więcej niż 21 milionów BTC. Każdy z nich jest nagrodą za udostępnioną przez użytkowników moc obliczeniową komputerów (proces miningu/wydobywania). Kopanie bitcoina można porównać do złamania zagadki matematycznej niezbędnej do rozwiązania bloku (sam blok składa się z transakcji). Należy podkreślić, że rozwiązanie bloku rozumie się jako jego zweryfikowanie i udostępnienie go publicznie. Pierwszy taki blok został rozwiązany przez twórcę BTC – Satoshiego Nakamoto, a za jego upublicznienie autor otrzymał nagrodę w wysokości 50 BTC. Od tej chwili wydobywaniem BTC zajęła się społeczność całego świata[16].

Najprostszym jednak sposobem pozyskania bitcoina jest zakup tej kryptowaluty w Internecie, np. na portalach aukcyjnych typu Ebay czy Allegro lub w kantorach online. Kupno BTC na serwisach aukcyjnych ma jedną zasadniczą wadę, tj. nieporównywalnie wyższą cenę (czasami nawet dwukrotnie wyższą od rynkowej). Dzieje się tak, ponieważ wówczas cena ustalana jest przez osobę prywatną dysponującą elektronicznym pieniądzem. Stąd też bardziej popularnym rozwiązaniem są kantory online (takie jak *cryptocoins.com*).

[16] M. Szymankiewicz, *Bitcoin – wirtualna waluta Internetu*, op. cit., s. 40-41.

Cyberwaluta bitcoin obecnie osiąga znaczną wartość w przeliczeniu np. na dolary lub złotówki. Z tego powodu został utworzony system podziału BTC. Przede wszystkim wyróżnia się 0,01 część BTC, czyli 1 centbitcoin lub bitcent (cBTC). Kolejno mamy 0,001 BTC, tj. 1 milibitcoin lub mbit (mBTC). Wartością jeszcze mniejszą jest ubit (mikrobitcoin), który stanowi 0,000001 BTC. Najmniejszym „nominałem" jest 1 satoshi (nazwany na cześć twórcy waluty), który jest wart 0,00000001 BTC. Używanie niektórych z powyższych wartości jest bezzasadne, ale ponieważ kurs cyberwaluty jest mocno nieprzewidywalny – jej twórcy musieli zabezpieczyć się na wypadek ewentualnych znacznych wzrostów wartości[17].

W kontekście powyższych informacji należy stwierdzić, że Polska, tak jak cały świat, podąża nurtem bitcoina. Mimo braku regulacji prawnych, w naszym kraju powstały już pierwsze bankomaty, w których można zakupić kryptowalutę. „Należy tylko wybrać język (dostępne są polski, angielski i niemiecki), zeskanować adres swojego portfela z telefonu, tabletu lub laptopa, włożyć do maszyny pożądaną ilość gotówki, aby dosłownie w sekundę zasilić portfel BTC"[18]. Pierwsze bankomaty bitcoinowe pojawiły się w Warszawie, jednak jak wynika z doniesień medialnych – podobne urządzenia znajdują się już np. we Wrocławiu czy Katowicach. Rośnie również liczba placówek akceptujących BTC jako formę zapłaty. W Warszawie na dzień 1 marca 2015 roku jest ich osiemnaście[19].

Ogólne zasady i sposoby użytkowania bitcoina są proste. Ważne jest to, że użytkownik nie musi posiadać zaawansowanej wiedzy informatycznej, by założyć portfel i obracać kryptowalutą. System i interfejs aplikacji został tak dostosowany, że jego obsługa jest intuicyjna. Do pierwszych transakcji wystarczy poznać podstawowe reguły, które rządzą światem bitcoina. Istotą jego sukcesu jest prostota, anonimowość i szybkość. Kurs regulowany głównie popytem i podażą sprawia, że inwestycja w bitcoiny może okazać się bardzo opłacalna, ale również bardzo ryzykowna. Praktycznie w każdym aspekcie funkcjonowania bitcoina widać wpływ globalizacji i postępu informacyjnego, zatem zasadne jest stwierdzenie, że jest to waluta ery globalizacji. Reasumując, należy stwierdzić, że jest to pierwsza krytpowaluta, która odniosła tak duży realny sukces. Niestety, jej cechy umożliwiają nie tylko realizację legalnych transakcji, lecz także służą do obsługi nielegalnego handlu międzynarodowego oraz prowadzenia i finansowania działalności przestępczej w skali globalnej.

Tak jak bitcoin jest swoistą alternatywą dla tradycyjnych środków płatniczych, tak również Dark Web funkcjonujący w sieci TOR stanowi alternatywę dla tradycyjnego Internetu. Jest to zbiór powiązanych ze sobą serwerów, pomiędzy którymi połączenie jest odpowiednio zabezpieczone (szyfrowane i wybierane losowo). Użytkownik

[17] https://en.bitcoin.it/wiki/Units.

[18] http://bitcoin.pl/wiadomosci/startupy/633-nowy-bankomat-bitcoin-w-popularnym-warszawskim-lokalu.

[19] http://bitcoin.pl/placowki.

korzystający z sieci TOR (przy zachowaniu odpowiednich zasad) może być pewien swojej prywatności.

Prowadzenie nielegalnej działalności w sieci TOR jest możliwe dzięki założonym tam forom internetowym działającym na zasadach e-sklepów. Serwery TOR, na których funkcjonują takie usługi, są również anonimowe, dlatego służby, które starają się przeciwdziałać temu zjawisku, mają bardzo utrudnione zadanie. W sklepach sieci TOR, płacąc bitcoinem, można w szybki, prosty i anonimowy sposób nabyć narkotyki, pornografię dziecięcą, broń, materiały wybuchowe, nielegalne dokumenty czy fałszywe banknoty. Co więcej, posiadając odpowiednie fundusze, można wynająć płatnego mordercę. Najpopularniejszym do 2011 r. sklepem TOR był Silk Road. Obecnie serwisy, które oferują wymieniane usługi, to m.in. Agora Forum, BlackBank, Dream Market, Havana Marketplace czy polskojęzyczny serwis Victoria. Integracja bitcoina w system nielegalnych sklepów jest coraz bardziej zaawansowana. Właściciele tych serwisów dbają nie tylko o prostotę i szybkość wykorzystania cyberwaluty, lecz także bezpieczeństwo stron nielegalnych transakcji. Rozwój zjawiska i wzrost popularności Deep Webu wśród społeczności świata sprawia, że kwestia ta może stać się istotnym zagrożeniem bezpieczeństwa współczesnego świata. TOR i bitcoin stały się doskonałym narzędziem integrującym środowiska przestępcze w wymiarze ponadnarodowym.

Zasady funkcjonowania sieci TOR oraz bitcoina są podobne (o sieci TOR napiszemy w kolejnym artykule). Determinuje to wzajemną współpracę i przenikanie się tych narzędzi. Należy stwierdzić, że gdyby nie istnienie bitcoina – sieć TOR byłaby niekompletna. Kryptologiczna waluta wprowadziła Dark Web na nowy poziom rozwoju, bo użytkownicy sieci mogą nie tylko przeglądać zawartość udostępnioną w ramach anonimowych serwisów, lecz także dokonywać płatności i nabywać różne dobra materialne i niematerialne.

LITERATURA:

1. W. Dębski, *Rynek finansowy i jego mechanizmy. Podstawy teorii i praktyki*, PWN, Warszawa 2007.
2. K. Kopańko, M. Kozłowski, *Bitcoin – złoto XXI wieku*, Helion, Gliwice 2015.
3. A. Sławiński, *Rynki finansowe*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2006.
4. M. Szmit, M. Tomaszewski, D. Lisiak, I. Politowska, *13 najpopularniejszych ataków sieciowych na twój komputer. Wykrywanie, usuwanie skutków i zapobieganie*, Helion, Gliwice 2008.
5. M. Szymankiewicz, *Bitcoin – wirtualna waluta Internetu*, Helion, Gliwice 2014.
6. M. Węgrzyn, J. Jabłoński, M. Nowakowski, *Transakcje i monety internetowe. Kryptologia a biznes – bezpieczeństwo stosowane*, Wydawnictwo BTC, Legionowo 2014.
7. R. Woś, *Waluta hakerów przyszłością gospodarki*, „Dziennik Gazeta Prawna", nr 112, 12-13 czerwca 2011.

8. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym, Dz.U. z 2001 Nr 130, poz. 1450.
9. http://bitcoin.pl/placowki.
10. http://bitcoin.pl/wiadomosci/startupy/633-nowy-bankomat-bitcoin-w-popularnym-warszawskim-lokalu.
11. http://gadzetomania.pl/3463,alternatywy-dla-bitcoin-czyli-przeglad-wirtualnych-walut.
12. http://naszdziennik.pl/ekonomia-finanse/27946,cypr-w-panice.html.
13. http://www.bitcoin.org.pl/czym-jest-bitcoin/.
14. http://www.money.pl/banki/konta-internetowe/porownanie-kont-internetowych/oplaty/.
15. http://www.payu.pl/o-nas.
16. https://blockchain.info/pl/.
17. https://en.bitcoin.it/wiki/Units.
18. https://www.paypal.com/pl/webapps/mpp/security/sell-chargebackfaq#goto1.

ANONYMITY OF BITCOIN AS A SECURITY THREAT

Abstract: The process of globalization and the resolution of information are a phenomenon that define the socio-economic reality of today world. These phenomenon were reflected in the practical functioning of monetary systems in the global world economy, especially in a new form of cybercurrency which is Bitcoin. Article is focused on determinants of functioning, the essence, principles and methods of using Bitcon. Activity of Bitcoin users shows that in future it can be one of security threat in social, economical and international dimensions.
Keywords: Bitcoin, anonymity, cybersecurity, organized crime.