Kamil MAZURCZAK[1]

Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach[2]

Instytut Nauk Społecznych i Bezpieczeństwa

k.mazurczak@vp.pl

ANONIMOWE PŁATNOŚCI INTERNETOWE WYKORZYSTYWANE W CYBERPRZESTĘPCZOŚCI. ISTOTA KRYPTOWALUTY BITCOIN

ABSTRAKT: Cyberprzestępcy korzystają z kryptowaluty Bitcoin od momentu jej powstania. To idealna, anonimowa platforma do globalnego przesyłania pieniędzy. Bitcoin nie ma zwierzchnictwa ani emitenta centralnego, przez co nie sposób go skraść jego posiadaczowi. Jest więc wykorzystywany przez ugrupowania przestępcze na całym świecie. Celem artykułu jest powiększenie wiedzy czytelnika na temat nowych technologii przesyłania pieniędzy. Wiedza ta pozwoli czytelnikowi na poprawienie jakości bezpieczeństwa personalnego w internecie. W efekcie zmniejszy potencjalne ryzyko wystąpienia różnego rodzaju fraudów i innych cyber-przestępstw.

SŁOWA KLUCZOWE: anonimowość, Bitcoin, BTC, cyberprzestępczość, kryptowaluty

AN ANONYMOUS WEB CYBERCRIME PAYMENTS. THE QUIDDITY OF BITCOIN CRYPTOCURRENCY

ABSTRACT: Cybercriminals use cryptocurrency Bitcoin since it come to existence. It is an ideal, anonymous platform for global money transfer. Bitcoin does not have authority or central issuer, so there is no way to steal it from its holder. It is therefore used by the criminal groups around the world. This article aims to increase the reader's knowledge on new technologies of money transfer. This knowledge will help the reader to improve the quality of personal security on the Internet. In effect it will reduce the potential risk of various types of frauds and other cybercrimes.

KEYWORDS: anonymity, Bitcoin, BTC, cybercrime, cryptocurrency

[1] Mgr Kamil Mazurczak – student pierwszego roku studiów stacjonarnych III stopnia na Uniwersytecie Przyrodniczo-Humanistycznym w Siedlcach, Wydział Humanistyczny, Instytut Nauk Społecznych i Bezpieczeństwa.

[2] Siedlce University of Natural Sciences and Humanities, Social Science and Security.

WPROWADZENIE

Niemal każdy cyberprzestępca trudzi się po to, żeby zarobić pieniądze. Pieniądze te musi przelewać, przyjmować, wpłacać, wypłacać, a także przechowywać. Skoro są to środki nielegalne, to nie może nimi dysponować w tradycyjny sposób.

Kiedy w latach trzydziestych XX w. w Stanach Zjednoczonych pojawiał się nowy wynalazek, jakim był odbiornik telewizyjny, prasa sceptycznie do niego podchodziła. Kilka lat później, każdy marzył aby mieć w swoim mieszkaniu telewizor, który już w latach sześćdziesiątych stał się obiektem pożądania na całym świecie.

Kiedy w latach dziewięćdziesiątych XX w., podłączano Polskę do internetu futurolodzy prognozowali, że poczta elektroniczna wyeliminuje fizyczne wysyłanie listów, zastąpi faktury ich elektronicznym odpowiednikiem, do tego w kilka sekund będzie można wysłać teksty, które dotychczas zamowałay całe tomy książek. Było to zbyt skomplikowane do zrozumienia. Dziś społeczeństwo wysoko rozwinięte nie wyobraża sobie podróży bez *Global Positioning System*, czyli popularnego GPS'u. Nie trzeba już znać się na kartografii, a kody kreskowe umieszczane na każdym produkcie usprawniają system szybkiej sprzedaży. To samo z sieciami społecznościowymi. Gdy powstawał Facebook, nie widziano dla niego przyszłości. Dzisiaj można prowadzić firmę używając jedynie Facebooka czy Twittera. Można korzystać z doskonałych cyfrowych zapisów audio oraz wideo. Można płacić za pomocą smartfonów nie wyjmując ich z kieszeni. Te i inne wynalazki zrewolucjonizowały systemy komunikacyjne, produkcyjne, społeczne oraz płatnicze.

Istnieje wiele opinii, traktujących o prymacie największej liczby odkryć oraz przełomowych wynalazków w XIX i XX w. Stwierdzenie to można uznać za prawdziwe jedynie w obrębie pewnej perspektywy czasowej. W gruncie rzeczy w przypadku postępu ma do czynienia z postępem geometrycznym.

Systemy płatnicze wykorzystywane w obrocie bezgotówkowym, a ściślej rzecz ujmując sposoby elektronicznych płatności są bardzo sprecyzowane i wolne od normatywnych odstępstw. Społeczeństwo dokonuje przelewów bezgotówkowych za pośrednictwem internetowych kont bankowych, a te są ściśle regulowane normami prawnymi. Dokonując przelewów korzystamy z systemu[3], który zapisuje historię transakcji wraz z wszystkimi danymi jakie posiada dwudziestosześciocyfrowe konto. Przelew trwa od kilkunastu minut, jeśli dokonujemy go w granicach tego samego banku, do kilku dni, gdy mamy do czynienia z transakcją międzynarodową lub/i z przewalutowaniem. Nierzadko za tę usługi banki pobierają opłatę. Kursy walut są regulowane na poziomie administracyjnym danego państwa, a każda waluta podlega inflacji. Oczywiście czynników wpływających na wysokość kursu jest wiele.

Jednak w XXI w. wyżej przedstawiony przelew bankowy jest już przestarzały, a jego koniec zdaniem autora jest nieunikniony. Istnieje waluta, której przesyłanie do każdego miej-

[3] A. Baranowska-Skimina, *Jak działa system ELIXIR,* 2014, http://www.finanse.egospodarka.pl/110971,Jak-dziala-system-ELIXIR,1,60,1.html, (26.01.2015).

sca na Ziemi, posiadającego dostęp do Internetu trwa kilka sekund, a opłata za każdy przelew, bez względu na wielkość transferowanych środków wynosi w przybliżeniu 0,04 PLN. Waluta ta nie podlega inflacji, nie posiada materialnej postaci, daje możliwość posiadania nieograniczonej liczby anonimowych kont, których założenie trwa nieco ponad minutę i jest darmowe, nie mając przy tym nad sobą żadnego rządowego zwierzchnika[4]. Waluta, której kurs w ciągu roku potrafi skoczyć o ponad 1.000 proc. nie może pozostać obojętna dla opinii publicznej. Takie są jej początki. Dzięki wyjątkowym możliwościom oferowanej przez funkcjonalność kryptowaluty Bitcoin (BTC) korzystają z niej już dziś gigantyczne firmy, takie jak Apple, Samsung, Volkswagen czy Microsoft. Już teraz można kupić Porsche, prosto z salonu za pośrednictwem BTC lub zapłacić za czesne na niektórych uczelniach wyższych. Jednakże można również anonimowo kupić narkotyki, broń albo wynająć płatnego zabójcę na czarnym rynku, korzystając z tzw. „jedwabnego szlaku" w sieci TOR (*Silk Road* oraz późniejsze odpowiedniki) Cyberprzestępcy korzystają z Bitcoina codziennie. Posiadając niezliczoną ilość kont mogą przelewać środki wielokrotnie.

Co ze sobą niesie Bitcoin i czym jest? Jak działa? Jakie są gwarancje bezpieczeństwa transakcji? Jakie są prognozy odnośnie rozwoju kryptowalut? Dlaczego to element niezbędny w anonimowości? Odpowiedzi na te pytania pomogą wyjaśnić dlaczego hakerzy najczęściej wybierają BTC do swoich transakcji pieniężnych.

CZYM JEST BITCOIN?

Bitcoin to pierwsza na świecie niezależna i zdecentralizowana cyfrowa waluta. Istnieje jedynie w systemach teleinformatycznych i nie posiada swojego materialnego odzwierciedlenia. Nie ma srebrnych i złotych monet, sztabek złota o określonej gramaturze z sinym oczkiem z rzadkiego kamienia. To algorytm składający się z kryptograficznego ciągu znaków posiadający określoną wartość[5]. W porównaniu z innymi walutami BTC ma dużo zalet:

- Bitcoin jest przesyłane bezpośrednio od nadawcy do odbiorcy przez Internet, co sprawia, że nie ma żadnych pośredników w transakcji. Nie ma potrzeby korzystania z banku czy kantoru. Oznacza to, że opłaty są dużo niższe od tradycyjnych, dotychczasowo wykorzystywanych przelewów bankowych.
- Kryptowaluty można używać wszędzie, gdzie tylko istnieje dostęp do sieci internetowej.
- Nikt nie zablokuje konta użytkownika.
- Nie ma żadnych dodatkowych wymagań i ograniczeń.

Zawarta jest w tym również możliwość posiadania anonimowego konta, a co za tym idzie dokonywanie niepersonalnych transakcji, co bezpośrednio łączy się z różnego rodzaju

[4] M. Węglewski, *Bitcoin. Kasa, czyli zera i jedynki,* 2014, http://biznes.newsweek.pl/bitcoin--kasa--czyli-zera-i-jedynki,104481,1,1.html, (26.01.2015).
[5] M. Szymankiewicz, *Bitcoin. Wirtualna waluta Internetu,* Warszawa 2014, s. 33.

niebezpieczeństwami, które mogą w znaczący sposób godzić w interesy państwa, zagrażając bezpieczeństwu narodowemu na płaszczyźnie gospodarczej, a także osłabiać bezpieczeństwo jednostki.

Bitcoin odmiennie niż w przypadku zdecydowanej większości walut nie opiera się na zaufaniu względem emitenta centralnego. Używa zdecentralizowanej, rozproszonej bazy danych, która rozprowadzana jest pomiędzy węzłami sieci *peer-to-peer* oraz przechowuje transakcję oraz jej historię.

W celu zapewnienia podstaw bezpieczeństwa, takich jak przykładowo udowodnienie, że dane Bitcoiny mogą być wydane tylko raz przez osobę, która je w danym momencie przetrzymuje używa się kryptografii klucza publicznego. Sieć implementuje rodzaj rozproszonego czasowego serwera, używając do tego matematycznych dowodów koncepcji łańcuchowych wykonanych działań, z ang. *Proof of Work*, stąd absolutnie cała historia transakcji musi być przechowywana w bazie oraz, co istotne upubliczniona. Za kolejne ogniwa zabezpieczeń uznać można również brak administracji centralnej oraz technologię *peer-to-peer* (p2p), które czynią manipulację wartości kryptowaluty, poprzez produkcję większej ich ilości całkowicie niemożliwą dla jakiejkolwiek jednostki i organizacji, zaliczając do nich liczając również organizacje rządowe[6]. Bitcoin nie podlega inflacji, nie jest na nią podatny. Wynika to z algorytmu, na którym BTC się opiera. Gdyby ktoś zechciał „dodrukować" pieniędzy, algorytm sieci nie przyjmie „dodrukowanych" Bitcoinów. Maksymalna ilość BTC, to 21.000.000. To również wynika z algorytmu tej kryptowaluty. Nie będzie więcej ani mniej. Oznacza to, że każdy nowy posiadacz Bitcoinów ma wpływ na kurs całej waluty. Im więcej będzie posiadaczy, tym na więcej osób system będzie musiał podzielić całość, podnosząc tym samym ich wartość oraz – a co idzie w parze – trudność sposobu wydobycia.

POCHODZENIE BITCOINA

Bitcoin został napisany w 2008 r., a wprowadzony do użytku rok później przez osobę, lub grupę osób o pseudonimie Satoshi Nakamoto. Jednak jest to jedna z kilku wersji dotyczących historii powstania tego przełomowego sposobu dokonywania transakcji pozagotówkowych. W spekulacjach pada również nazwisko Nick Szabo, który już w 1998 r. napisał koncept zwany „kryptowalutą"[7]. Padają też przypuszczenia, że twórcą może być również właściciel największego podziemnego czarnego marketu zwanego *Silk Road*, czyli Jedwabny Szlak, na którym właśnie za pośrednictwem Bitcoinów można było kupić od narkotyków, poprzez czołgi, samoloty, rakietnice, po terrorystów samobójców, zawodowych morderców, ludzkie organy do przeszczepu oraz ludzi – niewolników. Wszystkie z tych „dóbr wszelakich" mogły zostać dostarczone do wybranego miejsca na świecie po dokonaniu stosownej opłaty za pośrednictwem BTC. Market zarabiał miliony dolarów rocznie, a kryptowaluta sprawiła, że za-

[6] D. Homa, *Sekrety Bitcoina i Innych Kryptowalut*, Gliwice 2015, s. 19-21.
[7] R. Tomański, *Co powinniśmy wiedzieć o Bitcoin?*, 2013, http://technowinki.onet.pl/artykuly/co-powinnismy-wiedziec-o-bitcoin/b30nk (26.01.2015).

czął rozwijać się prężnie. Zagrażało to pośrednio bezpieczeństwu ludzi, ponieważ przestępcy zwiększali możliwości do nabywania towarów, których bez dostępu do anonimowych transakcji nie mogliby w ogóle zdobyć. Został zamknięty przez rutynowy błąd administratorów, który wykorzystało FBI. Jednak na jego miejsce utworzyło się wiele innych czarnych marketów, gdyż popyt „nie lubi próżni". Kto jest więc twórcą Bitcoina? Narzędzia, które zarówno ułatwia życie jak i je uprzykrza w zależności w jakich rękach jest używane. Przypuszczeń jest wiele, a prawda jeszcze nie wyszła na jaw. Właścicielowi widocznie nie zależy na splendorze i stawia anonimowość na wysokim szczeblu życiowej hierarchii.

WYDOBYWANIE BITCOINA

Co łączy wydarzenia mające miejsce nad kanadyjską rzeką Klondike na przełomie XIX i XX w. z jak najbardziej współczesnym internetem? W obu przypadkach padają słowa: „gorączką złota"[8]. Górnicy, skuszeni wielkimi marzeniami o bogactwie przybyli masowo w jedno miejsce aby w pocie czoła, poprzez żmudną aczkolwiek w ich mniemaniu intratną pracę oddać się czynności kopania. Obiektem pożądania ponad 100 lat temu był metaliczny kruszec, dzisiaj analogicznie to samo zaczęło dziać się z niewidzialnym dla oka, niemożliwym do organoleptycznego zbadania Bitcoinem. Kryptowaluta szturmem zdobyła rzesze internetowych zwolenników.

Jednak jak można zdobyć coś, czego „nie ma"? Bitcoin skądś musi się brać. Jest kopany. Tak samo jak kopie się złoto, kopie się Bitcoiny. Nie dosłownie tak samo, lecz proces wydobywczy z ang. nazywa się *mining*, czyli kopanie. Czynność ta, odbywa się za pomocą „koparek" czyli aplikacji, które pracują na bardzo wydajnych podzespołowo komputerach o ogromnej mocy obliczeniowej uzyskiwanej z potężnych kart graficznych. *Miner*, czyli górnik, mając do dyspozycji odpowiedniej klasy sprzęt może podjąć proces wydobywczy BTC. Uprzednio przystępując do specjalnej „kopalni", to jest grupy osób, które mają podobny sprzęt i chcą robić to samo. Grupa liczy od kilku do kilkuset osób – „koparek". Bitcoiny są w blokach, a każdy z nich liczy 25 BTC. Aby grupa mogła „wykopać" blok pieniędzy musi stworzyć zdalnie jeden superkomputer, który rozwiąże zagadkę, algorytm kryptograficzny. Czas *mining'u* jest uzależniony od mocy obliczeniowej maszyn. Po rozszyfrowaniu algorytmu „górnicy" dzielą się blokiem po równo i przystępują do wydobywania kolejnego. Proces ten jest w pełni zautomatyzowany. Wydobywanie kryptowalut stało się nowym, modnym i rentownym biznesem na całym świecie. Wiele firm inwestuje w drogi sprzęt hardware po to, aby w wydzielonym pomieszczeniu ustawić komputer z kilkudziesięcioma superwydajnymi kartami graficznymi, w celu stworzenia profesjonalnej, opłacającej się „kopalni" BTC, które poprzez pracę dwadzieścia cztery godziny na dobę, siedem dni w tygodniu będą napychać portfele inwestorów. Tylko jak długo? Gorączka złota nad Klondike w Kanadzie nie trwała przecież wiecznie.

[8] Focus.pl, *Bitcoin: Waluta przyszłości?,* 2014, http://www.focus.pl/technika/bitcoin-waluta-przyszlosci-10879, (26.01.2015).

ALGORYTM BTC

Algorytm kryptowaluty Bitcoin został wydany na licencji *opensource,* co sprawia, że każdy ma prawo do wglądu jak i edycji programu. Nie można pominąć faktu, że wprowadzenie każdej zmiany potrzebuje mocy ponad połowy sieci. Moc sieci tworzą jej „kopacze”[9]. Im wyższa staje się moc, tym trudniej „wykopać” jest blok BTC. Stopień trudności wiąże się bezpośrednio z czasem wydobywania, a ten z opłacalnością. Na dzień dzisiejszy pojedynczy użytkownik jest w stanie zarobić posiadając jedną wydajną maszynę, jednak za kilka lat to najprawdopodobniej przestanie być rentowne, gdyż zarabiać będą już tylko firmy mające do dyspozycji tysiące superkomputerów. Skoro liczba bitcoinów jest policzalna, to znaczy, że kiedyś, w nieokreślonym jeszcze czasie, wszystkie zostaną wydobyte. Statystycznie, wszystkie Bitcoiny zostaną wydobyte w 2140 r., a zostało ich ponad 8.000.000. Czyli już zostało wydobytych 13.000.000, a skoro BTC jest od 2008 r., to oznacza, że te 13.000.000 Bitcoinów zostało wydobyte przez 7 lat. Wniosek jest prosty. Kopanie niniejszej kryptowaluty będzie coraz trudniejsze.

PRAKTYCZNE DZIAŁANIE BITCOINA

Jak zwykły człowiek może zdobyć Bitcoiny nie posiadając wyspecjalizowanego sprzętu? Można je zwyczajnie i w pełni legalnie kupić na giełdach BTC. W Polsce funkcjonuje kilka giełd wymieniających złotówki na walutę wirtualną. Najpopularniejszą z nich jest Bitcurex.com – jedna z dziesięciu największych giełd bitcoinowych na świecie. Aby móc cieszyć się w pełni z transakcji należy na początek założyć konto – „portfel”. Portfel można zapisać na swoim komputerze – dysku, bądź pamięci zewnętrznej, można też założyć portfel wirtualny online na jednym z oferowanych przez system portali. Bez względu jaki proces zostanie wybrany, wygeneruje się jedyny i niepowtarzalny adres portfela Bitcoin. Nic nie stoi na przeszkodzie aby wygenerować kolejny, a nawet milion następnych, jeśli tylko wyrazi się taką chęć. Czynność ta jest całkowicie darmowa, łatwa, szybka i anonimowa.

Adresy nie zawierają żadnych danych o właścicielu. Są też zapisywane w łatwej dla odczytania przez człowieka formie jako ciągi tekstowe o składni zarówno literowej jak i cyfrowej w przybliżonej długości 34 znaków. Taka prostota korzystania z anonimowego narzędzia przesyłania pieniądza była dla cyberprzestępców marzeniem, które się spełniło.

Adres zaczyna się zawsze od cyfry 3 albo 1, występują w nim wielkie i małe litery z wyjątkiem wielkiej litery „O” oraz cyfry rzymskie, bez „0”. Nie istnieją znane nam z przelewów bankowych tytuły wpłat. Użytkownicy zastępują sobie ten brak nieograniczoną

[9] A. Golański, *Bitcoin bez płaczu. Jak działa kryptograficzna e-waluta?*, 2012, http://webhosting.pl/Bitcoin.bez.placzu.czesc.1.Jak.dziala.kryptograficzna.e_waluta?page=1, (26.01.2015).

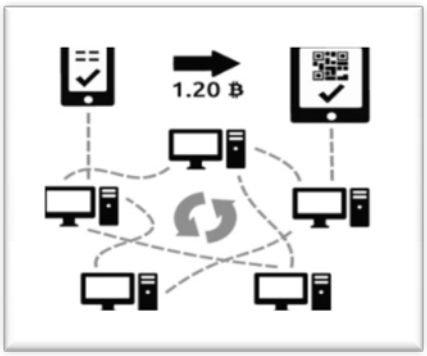
możliwością tworzenia nowych adresów, co również przyczynia się do zwiększenia anonimowości transakcji przy używaniu jednego adresu do pojedynczej operacji[10].

1rYK1YzEGa59pI314159KUF2Za4jAYYTd

Nazwa: *Przykładowy adres portfela BTC*
Źródło: Opracowanie własne

Po wygenerowaniu portfela można już dokonywać przelewów internetowych. Wszystkie potwierdzone transakcje zapisywane są bez żadnych wyjątków w łańcuchu bloków, który jest współdzielonym zapisem transakcji. Właśnie na tym polega cała sieć Bitcoin. W taki sposób przelewy mogą zostać zweryfikowane pod kątem posiadania odpowiedniej ilości BTC na koncie wydającego. Kryptografia wymusza integralność oraz porządek chronologiczny łańcucha bloków.

Za transakcję rozumie się przesłanie pewnej wartości pomiędzy dwoma adresami – portfelami, które zawierają część danych tajnych, zwanych kluczem prywatnym. Klucze prywatne niosą ze sobą matematyczne dane potwierdzające pochodzenie od właściciela danego adresu, dlatego są używane jako swoisty elektroniczny podpis, będący nie do podrobienia. Podpis zapobiega także modyfikacjom przez osoby trzecie na każdym etapie od momentu wydania.



Rysunek 1. *Transakcja BTC*
Źródło: bitcoin.org.

Wygląda na to, że przelewy dokonywane za pośrednictwem kryptowaluty są bezpieczne zarówno dla nadawcy jak i odbiorcy. Równocześnie, przy zachowaniu odpowiedniej dawki ostrożności zachowują anonimowość, co zostało od razu dostrzeżone przez ludzi operującymi nielegalnym środkami, wszelakiego pochodzenia.

FUNKCJONALNOŚĆ BITCOINA

Bitcoin zmienia świat finansów, tak jak internet zmienił wydawnictwa prasowe. Gdy każdy ma jednakowy dostęp do globalnego rynku, powstaje wiele ciekawych pomysłów. Zatem jak w praktyce używany jest dziś BTC? Można płacić nim za gry i akcesoria do gier, pre-

[10] Obserwacja autorska.

zenty, kawę, ubrania, książki, serwery, strony internetowe, komputery, zapłacić za czesne na niektórych wyższych uczelniach państwowych, kupić samochód prosto z salonu. W kwietniu 2013 r., nowe Porsche Cayman S zostało sprzedane za 300 BTC[11]. Oprócz tego, można zapłacić za kolację, hotel, wycieczkę, apartament i wiele innych, wymieniając przy tym swoją rodzimą walutę na Bitcoiny za pośrednictwem internetowych kantorów

Kryptowaluta, to świetna możliwość zarówno dla małych, jak i dużych firm. Sama w sobie pełni dodatkową funkcję promującą, bowiem można odnieść wówczas wrażenie, że podmiot akceptujący płatności cyberwalutami, idzie z duchem czasu uznając ekosystem wirtualnej waluty, będącej odbiciem realnego pieniądza. Akceptowanie ich nic nie kosztuje, nie ma żadnych opłat ani zwrotów czy prowizji. Istnieją również specjalne bankomaty, dzięki którym możemy klasycznie wymienić fizyczne waluty na te wirtualne, bez logowania się w internetowych kantorach. Dla cyberprzestępców dostępny jest więc wachlarz możliwości, który skrzętnie i z premedytacją wykorzystują.

KURS BITCOINA NA PRZESTRZENI KILKU LAT

Siedem lat temu, gdy na świat przychodził Bitcoin, jego wartość wynosiła 40 groszy za 1 BTC. W 2012 r. kurs oscylował w wysokości 30 PLN. Na początku 2013 r. kurs poszedł do góry i w szczytowym momencie uplasował się na wysokości 3.500 PLN za 1 BTC[12]. Żadna waluta świata nigdy nawet nie zbliżyła się w połowie do tej wartości. To zadziałało na ludzką wyobraźnie, gdyż wystarczyło zainwestować średnią krajową, aby w krótkim czasie kupić mieszkanie o wysokim standardzie. Ponieważ wartość Bitcoina kontrolowana jest tylko i wyłącznie przez prawa jakimi rządzą popyt i podaż wśród użytkowników, kurs potrafi ulec znaczącej zmianie nawet podczas kilku godzin. Niektórzy analitycy twierdzą, że to czysty hazard. Na pewno jest, a bynajmniej była w tym część racji. Cyberwaluta osiągnęła swój maksymalny kurs po przystąpieniu Chin do akceptacji płatności w BTC. Chińskie Google – Baidu po jakimś czasie zawiesił przyjmowanie płatności w bitcoinach. Wówczas kryptowalutę dotknął krach. Nagłe spadki kursu doprowadziły do masowego wyciągania pieniądza z elektronicznych portfelów, co jeszcze go obniżyło. Spekulanci prognozowali, że to już koniec eksperymentu pod tytułem Bitcoin. Jednak mylili się i to znacząco, aczkolwiek do dzisiaj nie można przewidzieć zachowania się elektronicznej waluty na światowych giełdach. Zmiany są zależne od samych uczestników gry, którzy niejednokrotnie przejawiają zachowania konformistyczne.

Dzisiaj kurs Bitcoina jest stosunkowo stabilny, lecz stabilność ta bywa liczona w miesiącach. Czy to wystarczy by w ogóle można było mówić o jakiejkolwiek stabilności?

[11] P. Rochowicz, *Wirtualna waluta pod lupą fiskusa,* 2013, http://prawo.rp.pl/artykul/1042170.html, (26.01.2015).
[12] J. Korus, *Wirtualna waluta Bitcoin warta ponad 1000 dolarów,* 2013, http://biznes.newsweek.pl/bitcoin-przekroczyl-wartosc-1000-dolarow-na-newsweek-pl,artykuly,275833,1.html, (17.11.2015).

Tabela nr 1 pokazuje, że kurs Bitcoina wahał się na przestrzeni około 2 lat dość znacznie. Zatem nie jest to waluta o stabilnym charakterze. Specjaliści stale ostrzegają o niebezpieczeństwach związanych z inwestowaniu w ulegającą stałym wahaniom kryptowalutę.

Data	Kurs w PLN	Źródło danych
20.12.2013	2107zł	bitcoiny.org
17.01.2014	2753zł	bitcoiny.org
24.03.2014	1733zł	bitcoin.pl
17.11.2015	1337zł	bitcoin.org

Tabela 1. *Kurs BTC na przestrzeni około 2 lat*

„CIEMNA STRONA" BITCOINA

Julius Robert Oppenheimer, amerykański fizyk, twórca bomby atomowej, po jej skonstruowaniu rzekł: „Mam krew na rękach." Po wybuchu w Los Alamos słowa jego komentarza brzmiały: „Stałem się śmiercią; niszczycielem światów"[13]. Zdawał sobie sprawę, że jego wynalazek uśmierci wiele istnień i zamieni w nicość każde miejsce, w którym dojdzie do wybuchu. Nie mylił się, jednak trzeba też przyznać, że nawet coś siejącego takie zniszczenie jak broń atomowa może być wykorzystywana do dobrych celów, takich jak chociażby funkcja odstraszania czy potencjalna możliwość zmiany trajektorii lotu asteroid zagrażających bezpieczeństwu całego społeczeństwa i środowiska naturalnego.

Bitcoin oferując tak wiele możliwości związanych z anonimowością, nazywany jest czasem „walutą wolnych ludzi". Brzmi to bardzo wzniośle, jeśli weźmie się pod uwagę dobę kryzysu ekonomicznego oraz niepewności bankowych transakcji. Kryptowaluta nie mając zwierzchnictwa emitenta centralnego i nie posiadając systemu skutecznej kontroli przepływu pieniądza stała się podstawowym pieniądzem używanym przez przestępców na całym świecie.

Istnieje bowiem takie miejsce, jak „ciemna strona" internetu[14]. Właściwie nie stanowi go właściwym tego słowa znaczeniu, lecz sieć, która działa podobnie jak wszystkim dobrze znany internet. To *darknet*: sieć TOR, Freenet i I2P, z czego ten pierwszy jest największy i najbardziej popularny. Nie można się tam dostać ze zwykłej przeglądarki typu Google Chrome, Internet Explorer czy Opera. Trzeba mieć poprawnie skonfigurowany komputer, specjalistyczne oprogramowanie wraz z przystosowaną przeglądarką. To wszystko gwarantuje anonimowość na bardzo wysokim poziomie. TOR przypomina internet sprzed 20 lat. Nie ma tam wyskakujących reklam ani kolorowych stron, nie istnieje też żaden odpowiednik Google. Poruszanie się jest więc dość prymitywne, a strony ładują się wolno, ponieważ nasza

[13] A. Kimball Smith, C. Weiner, *Robert Oppenheimer: Letters and recollections*, Cambridge 1980, s. 1.
[14] J. Grabowski, *Darknet – Internet do którego lepiej nie wchodzić,* 2012, http://www.komputerswiat.pl/artykuly/redakcyjne/2012/05/darknet---internet-do-ktorego-lepiej-nie-wchodzic.aspx, (26.01.2015).

obecność jest szyfrowana w bardzo skomplikowany sposób. Na tyle skomplikowany, że FBI, NSA i CIA nie są w stanie dotrzeć do faktycznych właścicieli stron, portali i marketów w sieci TOR, o ile właściciele poprawnie wszystko skonfigurują. Nie istnieje tam cenzura. Z *darknetu* korzystają przestępcy, organy ścigania, szpiedzy, agenci specjalni, dziennikarze, handlarze bronią i żywym towarem, zawodowi płatni mordercy, pedofile, dewianci, oszuści internetowi, faszyści, naziści i kobiety chcące usunąć ciążę, itd. Nie sposób wymienić wszystkich, ale jedno jest pewne. Wszyscy, w wyżej wymienionym gronie, korzystają z usługi przelewu bezgotówkowego, jaki oferuje Bitcoin. W zestawieniu z anonimizującym połączenie sieciowe TOR-em i gwarantującym anonimową transakcję BTC, przestępcy mają gotową platformę do robienia interesów opartych na handlu nielegalnym towarem, fraudów, a także do prania nielegalnych Bitcoinów. W podziemnym Internecie znajdują się pralnie kryptowalut[15]. Przestępca wchodząc w posiadanie „brudnych" BTC przelewa je do „pralni", która mieszając wszystkie wysyła na oddzielny adres, po pobraniu prowizji „czyste" Bitcoiny, które „wyprane" kilka razy z powodzeniem przesyłane są do jeszcze innego portfela, skąd zamieniane są w kantorach na waluty, które przestępca może bezpiecznie wypłacić z bankomatu nieopodal miejsca swojego zamieszkania.

Istnieją też markety, w których można kupić wszystko, co nielegalne, płacąc oczywiście Bitcoinami. Wyglądem i strukturą przypominają dobrze nam znane z polskiej sceny handlowości internetowej – Allegro. Sprzedający mają mierzalne zaufanie na podstawie pozytywnych i negatywnych komentarzy. Za Bitcoiny można zatem kupić karabin, który zostanie wysłany do kupującego na wskazany adres, paczkomat, lub placówkę poczty w przypadku opcji *poste restante*. Anonimowość kryptowaluty zwiększa dostęp nielegalnych towarów dla zwykłych ludzi, którzy często skuszeni prostotą uzyskania czegoś zakazanego stają się w świetle prawa przestępcami. Nie wspominając już o grupach przestępczych, które mając możliwość anonimowej sprzedaży narkotyków, broni czy ludzi stale poszerzają swoje nielegalne rynki zbytu. Wyjątkowo ciężko jest z tym walczyć organom ścigania. Aby doszło do schwytania sprzedawcy, musi on sam popełnić błąd, inaczej nakład pracy i środków, które agendy bezpieczeństwa musiały by przeznaczyć na pojmanie takiego cyberprzestępcy byłby niewspółmiernie wysoki do ryzyka jakie niesie ze sobą jego funkcjonowanie w przestępczym środowisku. Mowa tu zarówno o sprzedawcach dóbr wszelakich, jak i o usługodawcach czy pedofilach wymieniających się dziecięcą pornografią, którzy także używają Bitcoinów do swych zakupów i wymiany wiedzy.

Wszystko zależy od tego w jakiej ręce danemu narzędziu (w tym przypadku kryptowalucie) przyjdzie pracować. Może ono ułatwiać życie poprzez błyskawiczne przelewy, ale i powiększać szarą strefę wydatków, transakcji nielegalnymi towarami i rozwoju cyberprzestępczości w szerokim tego problemu rozumieniu.

[15] *How Bitcoin Laundering Works*, Bitlaunder.com, https://bitlaunder.com/launder-bitcoin, (26.01.2015).

PROGNOZY DLA BITCOINA

Czy możemy uznać Bitcoina za walutę przyszłości? Czy jedynie eksperyment na miarę międzynarodowego języka esperanto, którego podstawy opublikował pod koniec XIX w. Ludwik Zamenhof? Jak pokazuje historia – esperanto, który był bardzo łatwy w nauce, logiczny i stosunkowo precyzyjny, nigdy nie wszedł w praktyce do międzynarodowego użytku[16]. Z Bitcoinem jest trochę inaczej, bowiem jego użytkowników przybywa z dnia na dzień, a od czasu wielkiego wzrostu kursu na początku 2013 r. daje o sobie słyszeć nawet w popularnych mediach, które nie są *stricte* związane z branżami IT. Firmy o globalnym zasięgu dostrzegają w nim finansowe możliwości i akceptując płatności BTC przyłączają się do wspierania projektu.

Świat bezsprzecznie cały czas zmierza ku rozwojowi technologicznemu i każdy wynalazek, który będzie niósł ze sobą prostotę obsługi, zwiększone możliwości, a przede wszystkim ułatwienia w życiu codziennym, ma ogromne szanse na akceptację społeczeństwa. Przypuszczalnie rewolucja związana z bitcoinem nastąpi wówczas, kiedy będzie można wysyłać go za pośrednictwem wiadomości tekstowych. Dotychczas pomimo prostoty, z jaką można posługiwać się Bitcoinem korzystają z niego w dużej ludzie związani z informatyką. Nie trzeba dodawać, że dla ekspertów od informatycznego bezpieczeństwa jest to niezwykle proste. Jeśli do tego otrzymują jeszcze anonimowość, to jest to narzędzie jak na razie najodpowiedniejsze do pracy wszystkich cyberprzestępców, którzy wykorzystują swoją wiedzę do celów zarobkowych.

Istnieje również prawdopodobieństwo, którego nie sposób przeoczyć. A co, jeśli Bitcoin, to największe w historii finansowe oszustwo na Ziemi? Mowa tu o bańce spekulacyjnej na zasadzie piramidy finansowej[17]. Nouriel Raubini, ekonomista, który precyzyjnie przewidział kryzys finansowy w 2008 r. opisuje Bitcoina jako: „Narzędzie w rękach przestępców, kiepski środek przechowywania bogactwa i jeden wielki przekręt finansowy". Jego zdaniem BTC nie jest walutą, nie jest nawet jednostką rozliczeniową, ani środkiem płatności czy przechowywania środków. „Jest grą w piramidę finansową, która prowadzi do nielegalnych działań"[18]. Nie przeszkodziło to jednak Richardowi Bransonowi, zamożnemu przedsiębiorcy, ogłosić, że opłaty za komercyjne loty w kosmos będą przyjmowane w Bitcoinie[19]. Płatności w tej kryptowalucie przyjmują na Cyprze warsztaty, bary, sklepy, a nawet uniwersytety.

Wszystko wskazuje na to, że pomimo obaw pod względem sprawności działania systemu oraz funkcjonalności i prostoty w użytkowaniu, Bitcoin rozwija się z dnia na dzień,

[16] M. Byram, *Routledge Encyclopedia of Language Teaching and Learning, Routledge*, London 2001, s. 464.
[17] Ł. Michalik, *Bitcoin – waluta wolnych ludzi czy pomysłowa piramida finansowa?,* http://gadzetomania.pl/4279,bitcoin-waluta-wolnych-ludzi-czy-pomyslowa-piramida-finansowa, (26.01.2015).
[18] *„Dr. Zagłada" atakuje Bitcoina. „To piramida finansowa"*, TVN24bis, 2014, http://tvn24bis.pl/wiadomosci-gospodarcze,71/dr-zaglada-atakuje-bitcoina-to-piramida-finansowa,406152.html, (17.11.2015).
[19] J. Bereziński, *Potężna pomoc dla Bitcoina – do gry wchodzi kosmiczny Richard* Branson, 2014, http://www.biztok.pl/waluty/potezna-pomoc-dla-bitcoina-do-gry-wchodzi-kosmiczny-richard-branson_a16182, (17.11.2015).

a płatności kryptowalutą stają się coraz popularniejsze na całym świecie, nie tylko w kręgach przestępczych.

PODSUMOWANIE WYKORZYSTANIA BITCOINA

Bitcoin szybko zmienia świat finansów, tak jak email zmienił świat poczty. Dziś nikt nie wyobraża sobie powrócenia do tradycyjnych metod komunikacji, jakie towarzyszyły człowiekowi przez wieki. Nie pisze się już tak wiele listów, zastąpiły je smsy, emaile, bądź wykorzystywane są wbudowane w portale społecznościowe komunikatory online. Nic nie stoi na przeszkodzie dla programistów aby wbudować np. w Facebooka system płatności za pośrednictwem BTC. Niebawem to może stać się realne, z racji na swoją funkcjonalność. Kryptowaluty otwierają przed ludzkością szerokie perspektywy, lecz nigdy nie będą reklamowane przez żaden rząd, z racji tego, że są poza kontrolą – nie posiadają emitenta centralnego. Nad systemem czuwają matematycznie potwierdzone zabezpieczenia kryptograficzne. Bitcoinów nie da się ukraść z czyjegoś konta bez dostępu do niego. W przeciwieństwie do tradycyjnych kont, z których pieniądze stale wyciekają za sprawą hakerów.

W zależności od punktu widzenia, jaki przyjmiemy, wyjątkowe właściwości Bitcoina posiadają zarówno plusy, jak i minusy. System płatniczy opierający się o anonimowość, a także brak nadzoru oraz pośrednictwa pozwala z jednej strony na błyskawiczne i niezwykle tanie operacje finansowe, których dokonywać można na całym świecie, wszędzie tam, gdzie tylko jest dostęp do Internetu, a z drugiej zniechęca inwestorów chwiejnym kursem, ułatwiając jednocześnie życie w szarej strefie. Jednak tradycyjny pieniądz również nie jest wolny od zbliżonych podobieństwem problemów.

Na razie Bitcoin stanowi wyjątkową alternatywę dla płatności internetowych. Równocześnie dla sprzedawcy, jak i klienta. Kiedy detalista zarabiając 5-7 proc. na towarze, oddaje bankowi 2 proc. za obsługę karty bankowej, BTC zaczyna coraz bardziej interesować. Światowy przepływ finansów bez udziału rządów, instytucji bankowych, emitenta centralnego oraz pośredników brzmi niemal nierealnie. Dużą siłą Bitcoina jest fakt, że interesuje się nim coraz więcej osób lubiących nowe technologie. Ludzkość cały czas żyć będzie w postępowych i innowacyjnych czasach, a stare technologie będą zawsze wypierane przez nowe rozwiązania. Bitcoin jest właśnie takim rozwiązaniem technologicznym, które odpowiada mierze naszych czasów, a jako konkurent tradycyjnych przelewów bankowych sprawdzi się nie gorzej, zwłaszcza, kiedy wciąż spada zaufanie do bankowych systemów w dobie kryzysu finansowego. Jeśli chodzi o bezpieczeństwo, to kryptowaluty posiadają lepiej rozwinięty od standardowych środków płatniczych system. Zdecentralizowana sieć zapewnia komfort użytkowania i anonimowość, która niestety bywa różnie wykorzystywana.

Cyberprzestępcy od 2008 r., kiedy powstał Bitcoin mają platformę do przelewania i przetrzymywania nielegalnie pozyskanych środków. Sprzedawcy oferujący nielegalne towary w *darknecie* mogą stworzyć serwisy aukcyjne podobne do znanego w Polsce Allegro. Istnieją specjalne „pralnie" nielegalnych Bitcoinów, dzięki którym haker może bezpiecznie wy-

płacać pieniądze bankomacie. Tak robią profesjonaliści. Eksperci od bezpieczeństwa IT wykorzystujący swą wiedzę do kradzieży, wyłudzeń, szantaży i innych zabiegów mających na celu pozyskanie pieniądza.

BIBLIOGRAFIA

Byram Michael. 2001. The Routledge Encyclopedia of Language Teaching and Learning. London: Routledge.

Homa Dominik. 2015. Sekrety Bitcoina i Innych Kryptowalut. Gliwice: Wydawnictwo Helion.

Kimball Smith Alice, Weiner Charles. 1980. Robert Oppenheimer: Letters and recollections. Cambridge: Harvard University Press.

Szymankiewicz Marcin (2014). Bitcoin. Wirtualna waluta Internet. Gliwice: Wydawnictwo Helion.

ŹRÓDŁA INTERNETOWE

Baranowska-Skimina Aleksandra. 2014. Jak działa system ELIXIR, W http:// www. finanse .egospodarka.pl/110971,Jak-dziala-system-ELIXIR,1,60,1.html.

Bereziński Jacek. 2014. Potężna pomoc dla Bitcoina – do gry wchodzi kosmiczny Richard Branson W http://www.biztok.pl/waluty/potezna-pomoc-dla-bitcoina-do-gry-wchodzi-kosmiczny-richard-branson_a16182.

Bitlaunder.com. How Bitcoin Laundering Works W https://bitlaunder.com/launder-bitcoin.

Focus.pl. 2014. Bitcoin: Waluta przyszłości?, http://www.focus.pl/technika/bitcoin-waluta-przyszlosci-10879.

Grabowski Jacek. 2012. Darknet – Internet do którego lepiej nie wchodzić W http:// www. komputerswiat.pl/artykuly/redakcyjne/2012/05/darknet---internet-do-ktorego-lepiej-nie-wchodzic.aspx.

Korus Jakub. 2013. Wirtualna waluta Bitcoin warta ponad 1000 dolarów, W http:// biznes. newsweek.pl/bitcoin-przekroczyl-wartosc-1000-dolarow-na-newsweek-pl,artykuly,275833,1.html.

Michalik Łukasz. 2015. Bitcoin – waluta wolnych ludzi czy pomysłowa piramida finansowa?, W http://gadzetomania.pl/4279,bitcoin-waluta-wolnych-ludzi-czy-pomyslowa-piramida-finansowa.

Rochowicz Paweł. 2013. Wirtualna waluta pod lupą fiskusa W http://prawo.rp.pl/artykul/1042170.html.

Tomański Rafał. 2013. Co powinniśmy wiedzieć o Bitcoin? W http://technowinki.onet.pl/ artykuly/co-powinnismy-wiedziec-o-bitcoin/b30nk.

TVN24bis. 2014. „Dr. Zagłada" atakuje Bitcoina. „To piramida finansowa" W http:// TVN 24 bis. pl/ wiadomości -gospodarcze, 71/dr- zaglada- atakuje –bitcoina -to-piramida-finansowa, 406152. html.

Węglewski Miłosz. 2014. Bitcoin. Kasa, czyli zera i jedynki W http://biznes.newsweek.pl/bitcoin--kasa--czyli-zera-i-jedynki,104481,1,1.html.