Kinga Kądziołka [*]

Transakcje kryptowalutą bitcoin - wybrane zagrożenia

Streszczenie*: W artykule zwrócono uwagę na wybrane zagrożenia związane z internetowym systemem płatności kryptowalutą bitcoin. Poruszone zostały zagadnienia związane z anonimowością w sieci bitcoin, pozyskiwaniem bitcoinów, ryzykiem związanym z inwestowaniem w kryptowalutę oraz atakiem na sieć bitcoin. Dla kilku przykładowych adresów portfeli bitcoin (stron w transakcjach kryptowalutą) sporządzono diagramy przepływu środków. Mimo iż informacje o transakcjach dokonywanych za pomocą kryptowaluty są jawne i publikowane na ogólnodostępnych stronach to jednak możliwość ustalenia użytkownika danego adresu, powiązania użytkownika ze wszystkimi wykorzystywanymi przez niego adresami czy ustalenia źródeł pochodzenia środków jest znikoma.*

Słowa kluczowe: Bitcoin, kryptowaluta, ryzyko

Wprowadzenie

Bitcoin został opisany w 2009 r. przez osobę (bądź grupę osób) o pseudonimie Satoshi Nakamoto w artykule „*Bitcoin: A Peer-to-Peer Electronic Cash System*". Nie istnieje jak dotąd jednoznaczna definicja, która określałaby, czym jest bitcoin. Bitcoin może być rozumiany jako „system elektronicznego pieniądza funkcjonujący w ramach modelu płatności peer-to-peer, który łączy dwie strony transakcji bez udziału instytucji finansowych[1]". Z informatycznego punktu widzenia jest to pewien system komunikacji internetowej, umożliwiający wymianę danych między użytkownikami. Bitcoin bywa też określany jako kryptowaluta lub waluta kryptograficzna, co z kolei tłumaczone jest jako „waluta cyfrowa oparta na kryptografii i działająca w sieci peer-to-peer[2]". Jednakże bitcoin posiada pewne własności, odróżniające go od walut tradycyjnych. Nie występuje w postaci monet lub banknotów. Jest ogólnodostępny w Internecie, transfer środków zachodzi bezpośrednio między użytkownikami, nie ma opłat transakcyjnych (lub są niewielkie) i nie ma możliwości „zamrożenia" konta właścicielowi (por. [Szymankiewicz M.(2014), s.21]).

Transakcje w sieci bitcoin

Transakcja kryptowalutą bitcoin między dwoma użytkownikami polega na „przepisaniu środków z jednego adresu źródłowego lub większej liczby adresów źródłowych na jeden adres docelowy lub wiele takich adresów[3]". Pojedyncza transakcja może więc mieć wiele wejść i wyjść. Adres w sieci bitcoin jest z kolei ciągiem 27 – 34 znaków alfanumerycznych (rozpoczynającym się od cyfry 1 lub 3). Aby dokonywać transakcji w sieci bitcoin należy posiadać tzw. portfel Bitcoin. Portfel taki (po zainstalowaniu odpowiedniego oprogramowania, np. Bitcoin-qt) może być przechowywany na dysku twardym komputera. Można również przechowywać wirtualne monety

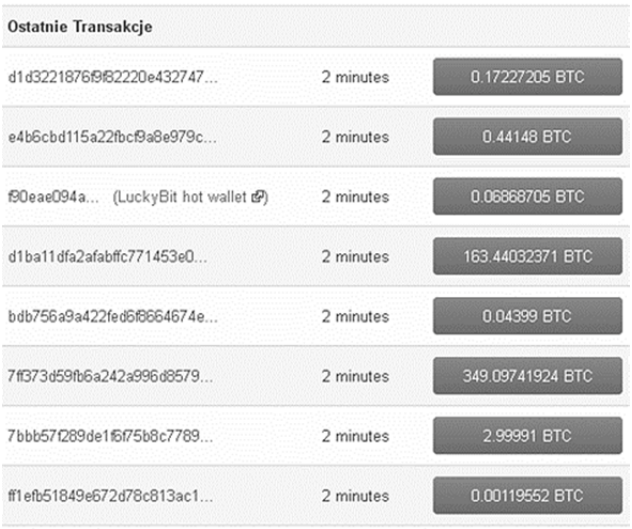
[*] Autorka ukończyła studia magisterskie na Uniwersytecie Śląskim (matematyka i informatyka). Była słuchaczką Studium Doktoranckiego Uniwersytetu Ekonomicznego w Katowicach. Obecnie pracuje jako analityk kryminalny.

[1] cyt. [Perez K., Urbaniak M., *Bitcoin - wirtualny eksperyment czy waluta przyszłości?*, Ruch prawniczy, ekonomiczny i socjologiczny, 4/2013, s. 164]. Peer-to-peer to „rozproszona architektura sieci. W tym modelu każdy użytkownik jest równy i łączy się bezpośrednio z innymi komputerami w sieci" (cyt. [Szymankiewicz M., *Bitcoin wirtualna waluta internetu*, Helion, 2014, s.38]).

[2] cyt. [Szymankiewicz M. (2014), s. 22].

[3] tamże, s. 41.

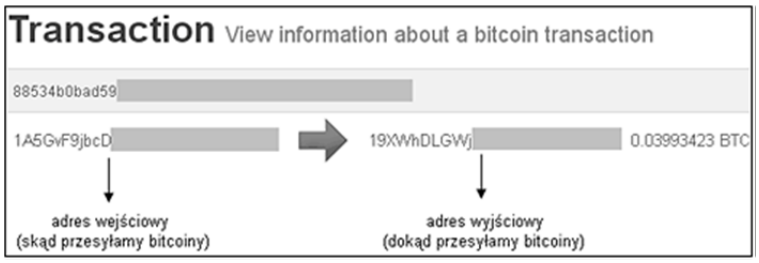
u jednego z zewnętrznych operatorów, co jest możliwe po utworzeniu nowego adresu na jednym z portali zajmujących się przechowywaniem bitcoinów. Każdy użytkownik może mieć wiele adresów (które wraz z kluczami[4] przechowuje w portfelu Bitcoin) i każda transakcja może odbywać się na nowym adresie. Wykorzystywanie różnych adresów podczas dokonywania transakcji powoduje zwiększenie anonimowości użytkownika i utrudnia analizę przepływu środków. Informacje o wszystkich wykonanych transakcjach są publicznie dostępne, m. in. na stronie internetowej blockchain.info, jednakże adresy Bitcoin w żaden sposób nie zdradzają tożsamości użytkownika.



Rysunek 1. Fragment wykazu dokonanych transakcji kryptowalutą Bitcoin.

Źródło: blockchain.info, 11.03.2015

Dla każdej transakcji (oprócz jej identyfikatora) dostępne są m. in. informacje o adresach wejściowych i wyjściowych transakcji oraz ilości bitcoinów (ozn. BTC) przesyłanych między adresami. Informacja o przykładowej transakcji mającej miejsce w sieci bitcoin została przedstawiona na Rysunku 2. Z adresu „1A5G...” przesłano na adres „19XW...” kwotę 0.03993423 BTC. Informacje o adresach w transakcjach są udostępniane publicznie, jednakże w tym artykule zdecydowano się „zakryć” fragmenty adresów oraz identyfikatorów transakcji.



Rysunek 2. Informacje o transakcji kryptowalutą bitcoin.

Źródło: blockchain.info, 12.03.2015

[4] Z każdym kontem w systemie transakcji kryptowalutą bitcoin związana jest para kluczy: prywatny i publiczny. Klucze te służą do cyfrowego podpisywania transakcji i weryfikacji podpisów cyfrowych.

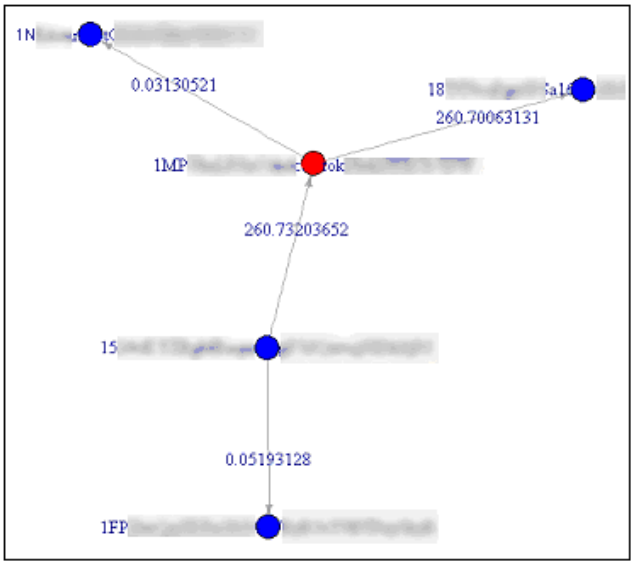
W szczegółach dotyczących transakcji widnieje również adres IP wraz z ustaloną na jego podstawie geolokalizacją. Adres ten może (ale nie musi) być adresem komputera, z którego dokonano przesyłu bitcoinów. Celem zwiększenia anonimowości użytkownicy mogą wykorzystywać sieci TOR czy anonimizujące serwery proxy (por. [Szymankiewicz M. (2014), s. 84]). Ponadto adres ten może się okazać adresem węzła rozgłaszającego transakcje. W związku z czym powiązanie transakcji z rzeczywistą lokalizacją osoby dokonującej przesyłu bitcoinów jest zadaniem trudnym (o ile w ogóle możliwym).

Wykorzystując ogólnodostępne informacje dotyczące poszczególnych transakcji można dla danego adresu przedstawić diagram powiązań z innymi adresami. Na diagramie takim można zobrazować z jakich adresów przesyłano na dany adres bitcoiny oraz na jakie adresy przesyłano z danego adresu bitcoiny. Na Rysunkach 3 – 7 przedstawiono diagramy powiązań dla wybranych adresów, z których dokonywano transferu bitcoinów. Diagramy wygenerowano wykorzystując darmowy program R. Do sporządzenia diagramów wykorzystano funkcję nazwaną *diagram.transakcji* wzorowaną na procedurze zaproponowanej przez B. Koehlera (2015). Oryginalna procedura autorstwa B. Koehlera generująca diagramy została uzupełniona m. in. o informacje na temat całkowitych kwot BTC przetransferowanych pomiędzy poszczególnymi adresami (informacja ta zamieszczona jest na krawędziach diagramu) oraz informacje na temat adresów (umieszczone w wierzchołkach diagramu). Poniżej umieszczono kod źródłowy funkcji *diagram.transakcji*[5]:

```
diagram.transakcji=function(adres) {
operacje <- blockchain.api.query(adres)
 txs <- operacje$txs
 bc <- data.frame()
 for (t in txs) {
 hash <- t$hash
 for (inputs in t$inputs) {
 from <- inputs$prev_out$addr
 for (out in t$out) {
 to <- out$addr
 va <- out$value
 bc <- rbind(bc, data.frame(from=from,to=to,value=va,stringsAsFactors=F))
 }
 }
 }
 btc <- ddply(bc, c("from", "to"), summarize, value=sum(value/100000000))
 btc.net <- graph.data.frame(btc, directed=T)
 V(btc.net)$color <- "blue"
 V(btc.net)$color[unlist(V(btc.net)$name) == adres] <- "red"
 nodes <- unlist(V(btc.net)$name)
 plot.igraph(btc.net, vertex.size=10, edge.arrow.size=0.5,edge.label=btc$value,
main=paste("Diagram transakcji BTC dla adresu\n", adres))
}
```

Rysunek 3. przedstawia diagram transakcji dla adresu „1MP...” uzyskany poprzez wywołanie funkcji *diagram.transakcji('1MP...')*. Zwrot strzałki wskazuje kierunek przepływu bitcoinów, tzn. z jakiego adresu na jaki transferowano środki. Można zauważyć, że z adresu „15...” przesłano na adres „1MP...” 260.73203652 BTC a następnie z adresu „1MP...” przesłano 260.70063131 BTC na adres „18...”. Celem uzyskania informacji o dalszym przepływie tych środków można wykorzystać narzędzia wizualizacji transakcji dostępne na stronie blockchain.info (Rysunek 8) lub w podobny sposób zobrazować diagram powiązań dla adresu „18...”.

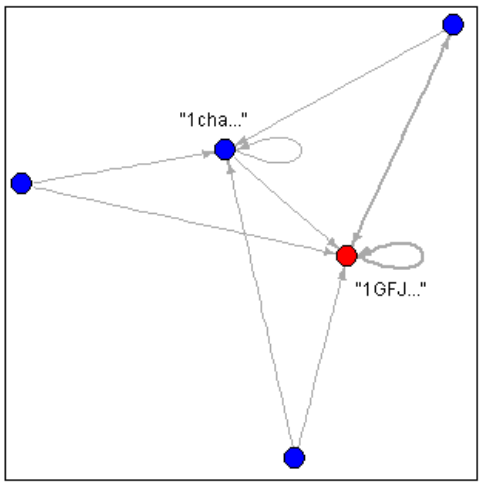
[5] Aby funkcja działała niezbędne jest wcześniejsze zainstalowanie pakietów *Rbitcoin*, *igraph* oraz *plyr*.



Rysunek 3. Diagram transakcji dla adresu „1MP...".

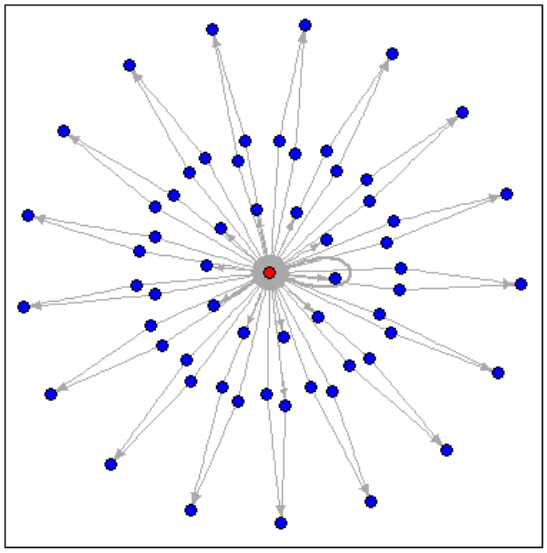
Źródło: opracowanie własne na podstawie danych ze strony blockchain.info

W przypadku diagramów dla niektórych adresów obserwowano pewne „schematy zachowań" lub „regularne" kształty diagramów. Rysunek 4 przedstawia diagram powiązań dla adresu „1GFJ...". Można zauważyć, że wszystkie transakcje przychodzące były transakcjami o dwóch wyjściach – bitcoiny trafiały również na adres „1cha...". Diagram ten ma małą liczbę węzłów (adresów), jednakże łączna liczba transakcji dla adresu „1GFJ..." na dzień 11.03.2015 wynosiła 1704. Z kolei diagram powiązań dla adresu „15ekh..." (węzeł zaznaczony kolorem czerwonym) ma pewien regularny kształt (Rysunek 5). W przypadku diagramów zaprezentowanych na Rysunkach 4 – 6 zrezygnowano z podawania informacji o adresach i ilości przesłanych między nimi bitcoinów, celem uzyskania większej przejrzystości diagramów.



Rysunek 4. Diagram transakcji dla adresu „1GFJ...".

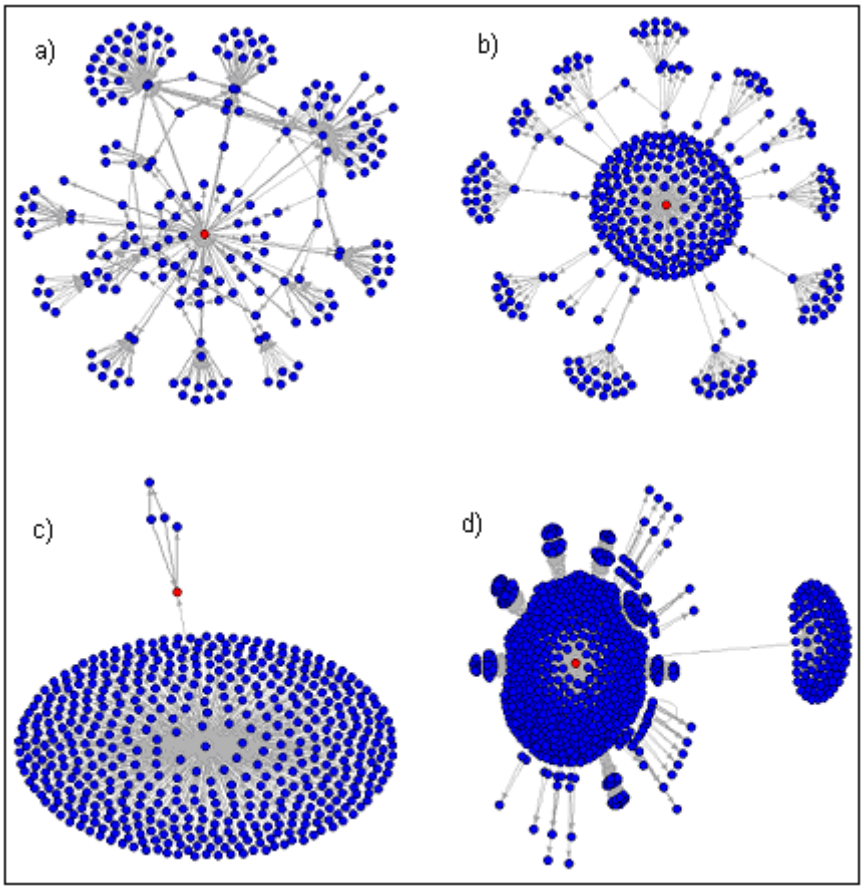
Źródło: opracowanie własne na podstawie danych ze strony blockchain.info



Rysunek 5. Diagram transakcji dla adresu „15ekh...".

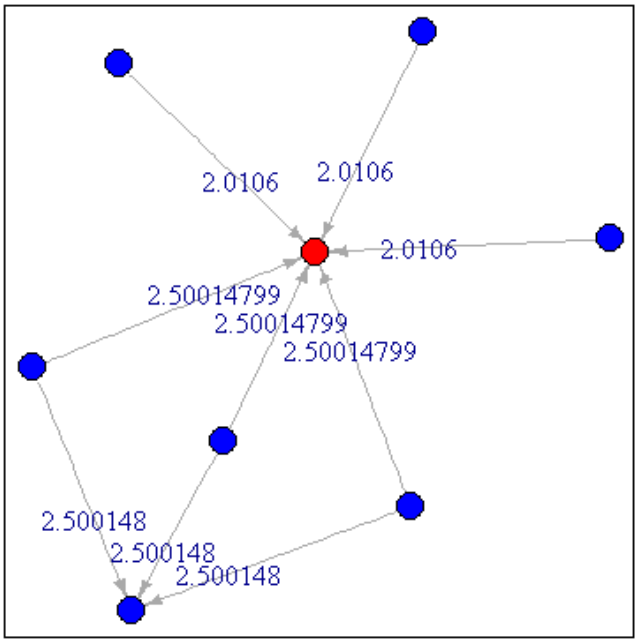
Źródło: opracowanie własne na podstawie danych ze strony blockchain.info

Diagramy sporządzane dla niektórych adresów charakteryzowały się dużą liczbą wierzchołków (Rysunek 6). Kolorem czerwonym zaznaczono węzeł (adres), dla którego sporządzano diagram powiązań. Duża liczba powiązań utrudnia wykrycie ewentualnych schematów transakcji. Jednak uwzględniając wielkość transferowanych kwot między poszczególnymi adresami, można zaprezentować diagram zredukowany np. do powiązań między tymi adresami, dla których wartość transferowanych środków przewyższała pewną ustaloną kwotę. Przykładowo, transakcje dla diagramu z Rysunku 6b dotyczą małych kwot BTC. Zostawiając tylko informacje o transakcjach na kwotę co najmniej 2 BTC diagram przedstawiony na Rysunku 6b uległ istotnej redukcji i zawierał tylko 8 wierzchołków (Rysunek 7). W tym konkretnym przypadku można zauważyć (Rysunek 7) takie same wartości transferowanych kwot, które były przesyłane na analizowany adres (było to 2.0106 BTC dla transakcji o jednym wyjściu lub 2.50014799 BTC w przypadku transakcji o dwóch wyjściach). Ponadto w przypadku transakcji o dwóch wyjściach dodatkowe 2.500148 BTC przesyłane było na inny wspólny adres.



Rysunek 6. Diagramy powiązań dla 4 różnych adresów.

Źródło: opracowanie własne na podstawie danych ze strony blockchain.info



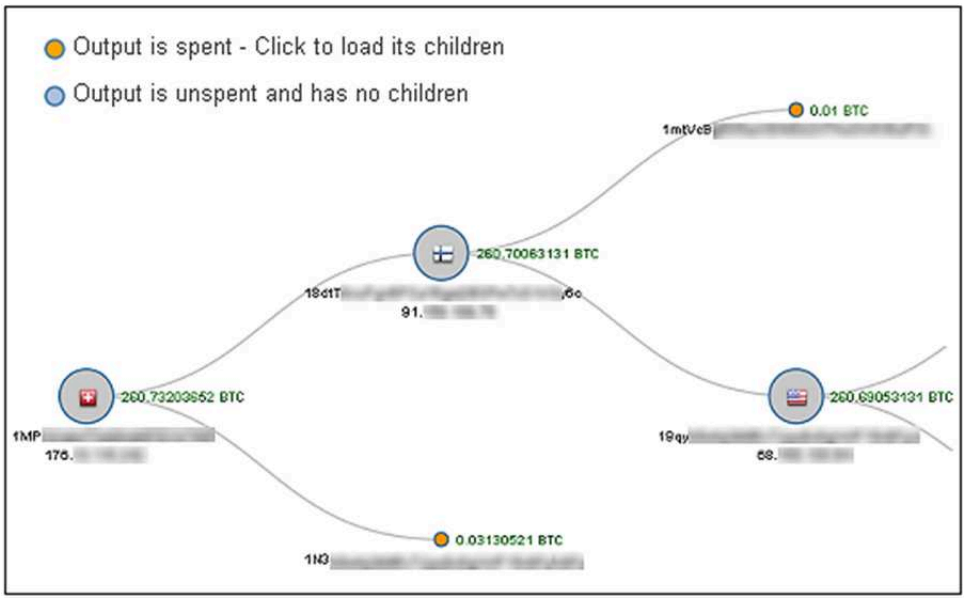
Rysunek 7. Zredukowany diagram z Rysunku 6b.

Źródło: opracowanie własne na podstawie danych ze strony blockchain.info.

W przypadku analizy transakcji w sieci bitcoin diagramy powiązań umożliwiają zobrazowanie przepływu bitcoinów między adresami. Dodatkowo można w analizach uwzględnić transfer bitcoinów w czasie między poszczególnymi adresami. Rysunek 8 przedstawia dalszy przepływ bitcoinów w przypadku transakcji zaprezentowanej na Rysunku 3, która dotyczyła przesyłu 260.73203652 BTC z adresu „15...” na adres „1MP...”. Jawność i ogólna dostępność informacji o transakcjach dokonywanych w sieci bitcoin pozwala przykładowo ustalić, na jaki adres trafiły środki w przypadku kradzieży bitcoinów. Jednakże praktycznie nie ma możliwości powiązania adresu ze sprawcą kradzieży, o ile sprawca przez „nieuwagę” nie udostępni swojego adresu portfela np. na jakimś forum dyskusyjnym wraz z innymi swoimi danymi, które pomogłyby go zidentyfikować. Ponadto dany użytkownik na potrzeby każdej transakcji może wykorzystywać inny adres, co dodatkowo utrudnia powiązanie wszystkich adresów użytkowanych przez jednego użytkownika z tym użytkownikiem. Ta anonimowość może powodować skierowanie zainteresowań potencjalnych przestępców na dokonywanie transakcji kryptowalutą. W szczególności ten sposób dokonywania transferów może stanowić kuszącą alternatywę dla osób zajmujących się np. handlem narkotykami, praniem pieniędzy czy finansowaniem terroryzmu. Przykładem była działalność serwisu Silk Road oferującego sprzedaż narkotyków, za które płacono kryptowalutą. W pracy *Anonymity in the Bitcoin network*[6] podjęto próbę identyfikacji nietypowych transakcji dla przykładowo wybranych sześciu adresów portfeli Bitcoin. Badano zgodność rozkładu Benforda z rozkładem cyfr w przypadku kwot transakcji związanych z tymi adresami. Żaden z nich nie był zgodny z rozkładem Benforda. Jednakże należy mieć na uwadze, że brak zgodności z rozkładem Benforda jest co najwyżej wskaźnikiem możliwości występowania nieprawidłowości i wymaga dalszych analiz, co w przypadku transakcji kryptowalutą jest szczególnie utrudnione ze względu na anonimowość, jaką oferuje ten system transferu środków. Na problem anonimowości w sieci bitcoin zwracają uwagę również m. in.:

[6] por. [Kądziołka K., 2015, w recenzji].

A. Borodo, Ł. Dopierała (2014), D. Breuker i in. (2013, 2014), M. Raskin (2012). S. Lee, P.T. Pham (2013), J. Hirschman i in. (2014), M. Phil i in. (2014) wykorzystując wybrane techniki data mining (m. in.: sieci neuronowe, metody grupowania danych, metodę wektorów wspierających) podjęli próbę identyfikacji schematów zachowań użytkowników sieci bitcoin. Zidentyfikowali adresy użytkowników, których zachowania różniły się od „typowych" zachowań użytkowników sieci bitcoin, jednakże problem anonimowości i szczegółów transakcji (np. czego dotyczyła) pozostał.



Rysunek 8. Fragment wizualizacji dalszego transferu środków dla wybranej transakcji.

Źródło: blockchain.info

Pozyskiwanie bitcoinów

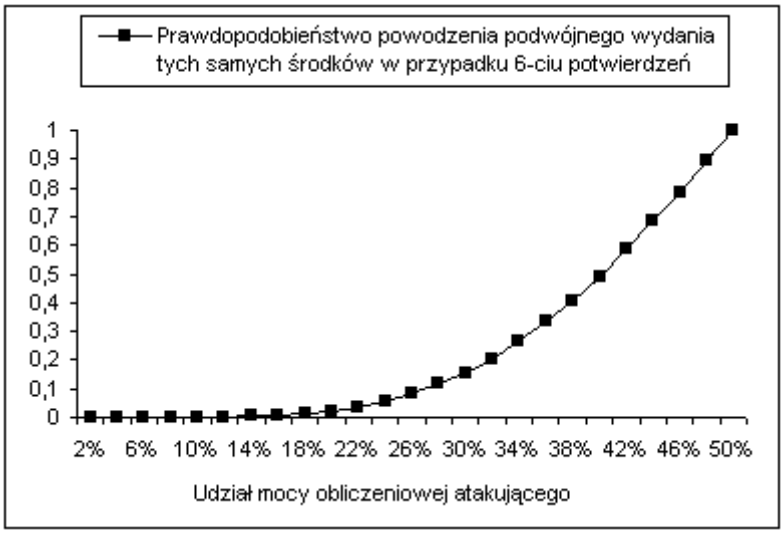
Wirtualne waluty można nabyć w tzw. bankomatach bitcoin. Można je też kupić bezpośrednio od osoby, która je posiada albo na aukcji internetowej bądź też w kantorach internetowych oferujących tego typu usługi. Handel wirtualną walutą odbywa się na giełdach, takich jak np. Bitstamp.net, Bitcoin.de. Istnieje również internetowa giełda Bitcurex w Polsce. Umożliwia ona wymianę bincoin na EUR i USD i odwrotnie[7]. Bitcoiny można również zdobyć jako nagrodę za udostępnioną przez użytkowników moc obliczeniową w tzw. procesie wydobywania bitcoinów. W wielkim uproszczeniu wydobywanie polega na rozwiązaniu „zagadki" matematycznej, która jest niezbędna do tzw. rozwiązania bloku. Szczegółowo proces ten opisuje M. Szymankiewicz (2014). Początkowo nagroda za rozwiązanie bloku wynosiła 50 BTC. Jeden blok jest generowany średnio co 10 minut a 210000 bloków generowanych jest średnio co 4 lata. Po każdorazowym rozwiązaniu 210000 bloków (średnio raz na 4 lata) nagroda za rozwiązanie bloku jest zmniejszana o połowę. Wraz ze wzrostem mocy obliczeniowej sieci rośnie trudność rozwiązania bloku, tak aby rozwiązanie bloku odbywało się w czasie zbliżonym do 10 minut. Maksymalnie może zostać wydobyte 21 mln bitcoinów. Obecnie w obiegu jest około 14 mln bitcoinów. Teoretycznie, zgodnie z przedstawionym algorytmem, wydobywanie bitcoinów

[7] por. [Perez K , Urbaniak M. (2013), s. 175-176].

zakończy się około 2140 r., z uwagi na ograniczoną liczbę bitcoinów, która może zostać wydobyta oraz to, że bitcoin jest podzielny do ósmego miejsca po przecinku.

Problem podwójnego wydawania tych samych środków

Sieć bitcoin jest wyposażona w mechanizm zapobiegający przesłaniu przez użytkownika tych samych środków więcej niż raz. Zabezpieczeniem przed podwójnym wydaniem środków (ang. *double spending*) są potwierdzenia od innych węzłów. Wraz ze wzrostem liczby potwierdzeń maleje prawdopodobieństwo podwójnego wydania tych samych środków. Jednakże atakujący, który posiada ponad 50% mocy obliczeniowej sieci bitcoin może ingerować w bieżące transakcje. Przed tzw. atakiem 50%+ nie jest w stanie uchronić żadna liczba potwierdzeń (por. [Szymankiewicz M. (2014), s. 84-86]). Wzór na prawdopodobieństwo sukcesu podwójnego wydania tych samych środków podaje M. Rosenfeld (2012). Wykres (Rysunek 9) przedstawia zależność między prawdopodobieństwem sukcesu podwójnego wydania tych samych środków a udziałem mocy obliczeniowej atakującego w przypadku stosowania 6 potwierdzeń niezbędnych do zaakceptowania transakcji. Sześć potwierdzeń jest używane w aplikacji Bitcoin-qt. Z uwagi na ogromne koszty, jakie wiązałyby się z utworzeniem własnej sieci mającej ponad 50% mocy obliczeniowej sieci bitcoin, sześć potwierdzeń zostało uznane za bezpieczne (przy założeniu, że jest bardzo mało prawdopodobne, aby potencjalny atakujący posiadał chociaż 10% mocy obliczeniowej sieci bitcoin).



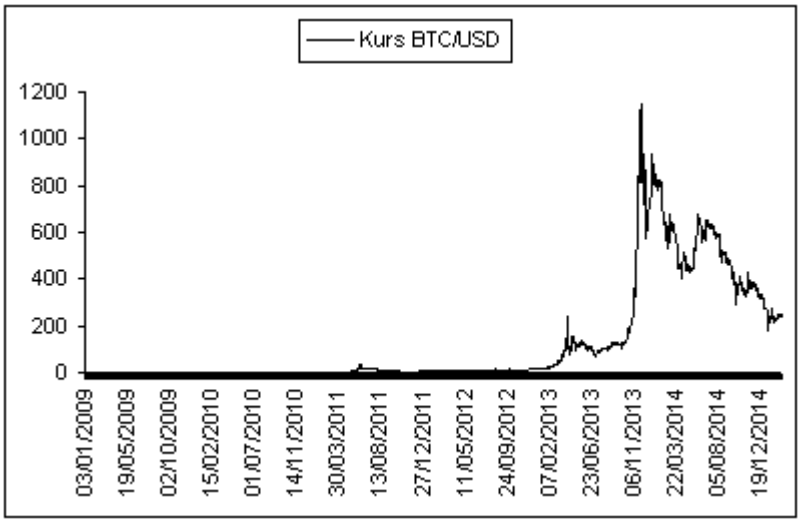
Rysunek 9. Prawdopodobieństwo sukcesu double spending w zależności od mocy obliczeniowej atakującego.

Źródło: opracowanie własne

Ryzyko inwestycji w kryptowalutę bitcoin

Kurs bitcoina charakteryzuje się dynamicznym tempem zmian (Rysunek 10). Kupując przykładowo w dniu 13.04.2011 pięć tysięcy bitcoinów (po cenie 1$ za sztukę) i sprzedając je w dniu 04.12.2013 (po cenie 1151$ za sztukę) można było w niecałe trzy lata zarobić na tej inwestycji 5750000$. Z drugiej strony, kupując bitcoiny w okresie, gdy ich cena była wysoka można było w krótkim czasie stracić większość zainwestowanych środków. Podejmowane są próby prognozowania kursu bitcoina z wykorzystaniem wybranych metod data mining, próby tworzenia

systemów transakcyjnych, identyfikacji czynników wpływających na zmiany kursu kryptowaluty[8]. Jednakże należy mieć na uwadze, że w odróżnieniu od klasycznych walut, kurs bitcoina kształtuje się wyłącznie na podstawie podaży i popytu użytkowników i nie jest bezpośrednio związany np. z sytuacją w danej branży czy koniunkturą gospodarczą[9]. Z inwestowaniem w kryptowalutę związane jest ryzyko. D.A. Devi i S. Soekarno (2014) porównali ryzyko inwestycji[10] w kryptowalutę bitcoin z ryzykiem inwestycji w złoto oraz indeks LQ45. Analizowali dane od czerwca 2010 do maja 2014. Inwestycja w kryptowalutę obarczona była największym ryzykiem, ale też pozwalała osiągać największe zyski.



Rysunek 10. Kurs BTC/USD.

Źródło: opracowanie własne na podstawie danych ze strony blockchain.info.

Podsumowanie

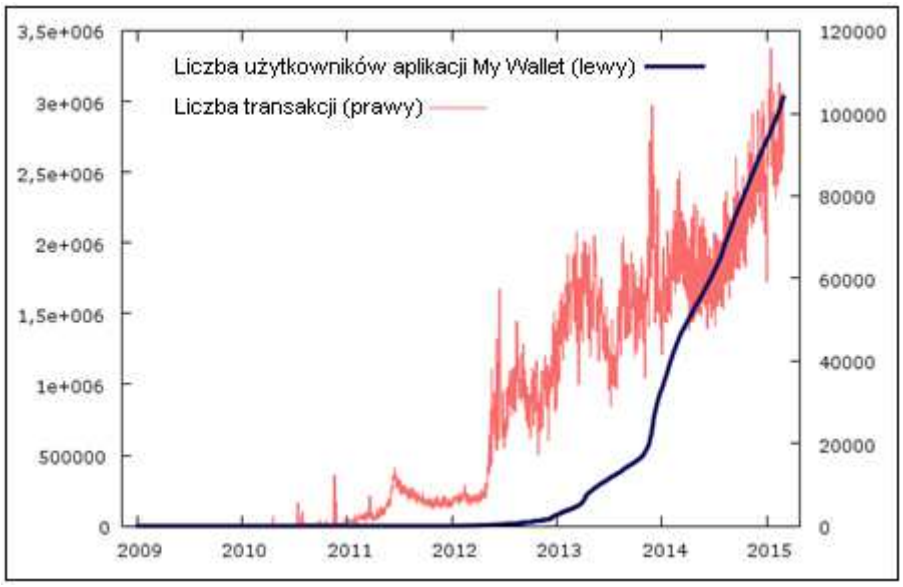
Wprowadzony w 2009 r. internetowy system płatności kryptowalutą bitcoin cieszy się coraz większym zainteresowaniem internautów. Obserwowana jest wzrostowa tendencja zarówno w liczbie dokonywanych transakcji jak i liczbie użytkowników aplikacji umożliwiających dokonywanie płatności kryptowalutą (Rysunek 11). Jednakże należy mieć na uwadze, że z posiadaniem i obrotem wirtualnymi walutami wiążą się rozmaite zagrożenia. Kurs kryptowaluty może szybko ulec zmianie, gdyż nie jest on związany z żadną „realną wartością". Transakcje kryptowalutą mogą być wykorzystywane do działań przestępczych, takich jak pranie pieniędzy, handel narkotykami czy finansowanie terroryzmu. Wirtualna waluta przechowywana jest w tzw. portfelu elektronicznym. Portfel taki może jednak stać się przedmiotem ataku cyberprzestępcy,

[8] m. in. prace: I. Madan i in., *Automated Bitcoin Trading via Machine Learning Algorithms*, http://cs229.stanford.edu/projects2014.html, 11.03.2015; P.A. Gloor, J. Kaminski, *Nowcasting the Bitcoin Market with Twitter Signals*, www.arxiv.org/pdf/1406.7577, 11.03.2015; D. Shah, K. Zhang, *Bayesian regression and Bitcoin*, arxiv.org/pdf/1410.1231, 11.03.2015; X. Li i in., *Exploring the Determinants of Bitcoin Exchange Rate*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2515233, 11.03.2015.

[9] Choć można było zaobserwować np. większe zainteresowanie bitcoinem w okresie blokady bankomatów i środków finansowych na rachunkach bankowych na Cyprze.

[10] Do oceny ryzyka autorzy wykorzystali wariancję oraz współczynnik zmienności stóp zwrotu. Indeks LQ45 jest odpowiednikiem warszawskiego indeksu WIG20 w przypadku giełdy w Dżakarcie (Indonesia Stock Exchange).

który postanowi się wzbogacić nie wychodząc z domu[11]. A osoby korzystające z tej formy dokonywania transakcji nie podlegają ochronie prawnej – nie ma np. systemu gwarantowania depozytów, aby pokryć ewentualne straty związane z kradzieżą wirtualnej waluty.



Rysunek 11. Liczba transakcji bitcoinami oraz liczba użytkowników aplikacji My Wallet.

Źródło: opracowanie własne na podstawie danych ze strony blockchain.info.

Bibliografia

1. Borodo A., Dopierała Ł., *Znaczenie waluty kryptograficznej bitcoin jako środka wymiany*, Współczesna Gospodarka, Vol. 5 Issue 2 (2014), www.wspolczesnagospodarka.pl, data dostępu: 11.03.2015
2. Breuker D. i in., *An inquiry into money laundering tools in the bitcoin ecosystem*. In: Proceedings of the APWG E-Crime Researchers Summit, 2013
3. Breuker D. i in., *Towards Risk Scoring of Bitcoin Transactions*, [w:] Financial Cryptography and Data Security, Lecture Notes in Computer Science Volume 8438, 2014
4. Czarnecki J., *Wybrane zagadnienia prawnokarne związane z bitcoinem*, [w:] Wirtualne waluty, Warszawa, 2014, http://www.bpcc.org.pl/pl/publication/raport-o-wirtualnych-walutach%5B5003425%5D.html (dostęp: 29.03.2015)
5. Devi D.A., Soekarno S., *Alternative Investments Evaluation of Bitcoins, Gold and LQ45 Index*, International Conference on Trends in Economics, Humanities and Management (ICTEHM'14), 2014, Pattaya, icehm.org/siteadmin/upload/9655ED0814058.pdf, (dostęp: 11.03.2015)
6. Gloor P.A., Kaminski J., *Nowcasting the Bitcoin Market with Twitter Signals*, www.arxiv.org/pdf/1406.7577, (dostęp: 11.03.2015)

[11] Ponieważ same bitcoiny fizycznie nie istnieją, więc kradzież bitcoinów polega na nieuprawnionym skopiowaniu klucza prywatnego oraz pozyskaniu adresu a następnie wykorzystaniu ich do transferu bitcoinów na inny adres (por. [Czarnecki J., *Wybrane zagadnienia prawnokarne związane z bitcoinem*, [w:] Wirtualne waluty, 2014, s. 33]).

7. Hirshman J., Huang Y., Macke S., *Unsupervised Approaches to Detecting Anomalous Behavior in the Bitcoin Transaction Network*, http://cs229.stanford.edu (dostęp: 11.03.2015)
8. Kądziołka K., *Anonymity in the Bitcoin network*, 2015, w recenzji
9. Koehler B., *Querying the Bitcoin blockchain with R*, http://beautifuldata.net/ (dostęp: 11.03.2015)
10. Lee S., Pham P.T., *Anomaly Detection in Bitcoin Network Using Unsupervised Learning Methods*, 2013, http://cs229.stanford.edu/projects2014.html, (dostęp: 11.03.2015)
11. Li X., Wang Ch., Wang Q., *Exploring the Determinants of Bitcoin Exchange Rate*, 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2515233, (dostęp: 11.03.2015)
12. Madan I., Saluja S., Zhao A., *Automated Bitcoin Trading via Machine Learning Algorithms*, http://cs229.stanford.edu/projects2014.html, (dostęp: 11.03.2015)
13. Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009, http://bitcoin.org/bitcoin.pdf (dostęp: 11.03.2015)
14. Perez K., Urbaniak M., *Bitcoin - wirtualny eksperyment czy waluta przyszłości?*, Ruch prawniczy, ekonomiczny i socjologiczny, 4/2013
15. Phil M. i in., *Money laundering analysis based on time variant behavioral transaction patterns using data mining*, Journal of Theoretical and Applied Information Technology, vol. 67(1), 2014
16. Raskin M., *Dollar-Less Iranians Discover Virtual Currency*, ,,BloombergBusinessWeek'', 29.11.2012, http://www.bloomberg.com/bw/articles/2012-11-29/dollar-less-iranians-discover-virtual-currency (dostęp: 11.03.2015)
17. Rosenfeld M., *Analysis of hashrate-based double-spending*, 2012, http://arxiv.org/abs/1402.2009 (dostęp: 29.03.2015)
18. Shah D., Zhang K., *Bayesian regression and Bitcoin*, 2014, arxiv.org/pdf/1410.1231, (dostęp: 11.03.2015)
19. Szymankiewicz M., *Bitcoin.Wirtualna waluta Internetu*, Helion, 2014

Some threats of bitcoin cryptocurrency transactions

The article focuses on some risks associated with online payment system with bitcoin cryptocurrency. It discusses the anonymity of the bitcoin network, obtaining bitcoins and the risk associated with investing in cryptocurrency and the risk of attack on the bitcoin network. There are also present cash flow diagrams for a few addressess of bitcoin wallets.

Keywords: Bitcoin, cryptocurrency,risk