Program „Od papierowej do cyfrowej Polski”
Strumień Blockchain/DLT i Waluty Cyfrowe

# Podstawy korzystania z walut cyfrowych

Redakcja naukowa

Krzysztof Piech

**Autorzy:**
Konrad Brzeziński – Polski Akcelerator Technologii Blockchain
dr Anton Bubiel – Szkoła Główna Handlowa w Warszawie
Kamil Jaczewski – Polski Akcelerator Technologii Blockchain
prof. nadzw. dr hab. Krzysztof Piech (red.) – Uczelnia Łazarskiego (Centrum Technologii Blockchain), Polski Akcelerator Technologii Blockchain
Jakub Piwko – Polski Akcelerator Technologii Blockchain
Judyta Rykowska – Polski Akcelerator Technologii Blockchain
dr Grzegorz Sobiecki – Szkoła Główna Handlowa w Warszawie
Łukasz Wiśniewski – Polski Akcelerator Technologii Blockchain

**Recenzenci:**
Tomasz Kurowski – Crypto@Cracow
Filip Pawczyński – Prezes Zarządu Polskiego Stowarzyszenia Bitcoin
Jacek Sieradzki – Crypto@Cracow
dr inż. Jacek Wytrębowicz – adiunkt w Instytucie Informatyki Politechniki Warszawskiej
dr hab. Konrad Zacharzewski – adwokat, Kierownik Katedry Prawa Handlowego WPiA UMK w Toruniu

**Wydawnictwo:**
Instytut Wiedzy i Innowacji


ISBN-13: 978-83-60653-28-9

**Patronat merytoryczny:**

## *Spis treści*

# Wstęp

Celem niniejszego opracowania jest możliwie proste, a jednocześnie rzetelne przedstawienie obecnego stanu tematyki kryptowalut. Dostrzegalna jest bowiem społeczna potrzeba opracowania takiego materiału. Zagadnienia te pozostają pojęciami rozumianymi jedynie przez stosunkowo nieliczną, choć stale rosnącą grupę osób[1]. Często różne wątpliwości i obawy kierowane pod adresem walut cyfrowych, w tym w szczególności kryptowalut, wynikają właśnie z niewiedzy czy szukających zwykle sensacji przekazów medialnych. Tymczasem, można na nie spojrzeć w szerszym kontekście: nie obaw, problemów technicznych czy prawnych związanymi z nowym zjawiskiem, ale w kontekście innowacyjnej technologii i tworzącego się, nowego sektora gospodarki.

Podobne obawy towarzyszyły kiedyś powstaniu Internetu. Mimo że wymykał się narodowym jurysdykcjom, nadal niekiedy służy do przestępczych celów (np. pobierania plików muzycznych z naruszeniem praw autorskich do nich), to nie pozostało nam nic innego jak zaakceptować ten fakt. I obecnie trudno jest sobie wyobrazić możliwość powrotu do świata bez Internetu. Podobnie, być może, w przyszłości będzie ze światem kryptowalut i technologii blockchain – nawet jeśli obecnie są to pojęcia nadal dość niejasne, dla niektórych obce i niepokojące, to

1 Kantor kryptowalut Coinbase ma już ponad 12 mln klientów (www.coinbase.com/about), natomiast największa polska giełda BitBay ma ponad 215 tysięcy klientów (https://bitbay.net/pl/o-nas). Oznacza to, że kryptowaluty może posiadać wciąż nieco ponad 0,5% dorosłych Polaków.

jesteśmy świadkami tworzenia się „nowej gospodarki". I tak jak każda rewolucja techniczna, również i ta wiąże się z narastaniem, a później być może z pęknięciem „bąbla spekulacyjnego". Patrząc jednak na długofalowe efekty dla gospodarek najbardziej rozwiniętych krajów, nie ma co się tego bać, a zaakceptować oraz podejmować działania dla zmniejszenia negatywnych skutków dla ludności bez blokowania rozwoju całego rynku.

Celem niniejszego opracowania jest opisanie wybranych elementów rynku kryptowalut i podstawowych pojęć związanych z nimi możliwie od początku procesu ich pozyskiwania do obracania nimi. Zawarte w nim są m.in. zasady funkcjonowania giełd kryptowalutowych oraz sposobów bezpiecznego utrzymywania kryptowalut. Jest to wiedza ogólnodostępna, jednak autorom opracowania wydawało się zasadne zebranie jej w jednym miejscu i zaprezentowanie w możliwie przystępnej formie. Jest to pierwsze, tak kompleksowe i wielowymiarowe opracowanie w naszym kraju.

W niniejszym opracowaniu używamy, niekiedy tożsamo, dwóch pojęć: walut cyfrowych i kryptowalut. Pierwsza pozycja ma szersze znacznie. Waluty cyfrowe to zarówno kryptowaluty, jak i środki wymiany stosowane w specyficznych systemach np. w grach czy sieciach społecznościowych. Na świecie istnieją już tysiące kryptowalut. Niewiele z nich ma szanse na powszechną adopcję i zyskają status porównywalny do pieniądza. Inne zaś będą służyły do specyficznych zastosowań. Ich częstą cechą wspólną jest wbudowany w nie mechanizm ekonomiczny, poprzez który społeczność na bieżąco może szacować popularność i wartość danego projektu, przez co dana kryptowaluta może stać się przedmiotem spekulacji. Rozdzielenie technologii blockchain od kryptowalut, które na niej bazują, jest bardzo trudne. Próby takie na tym etapie rozwoju technologii raczej ograniczyłyby rozwój nowych rynków, niż pomogłyby.

Przyjęta została konwencja, że gdy użyta jest nazwa danej kryptowaluty w kontekście walutowym, wtedy jej nazwa pisana jest z małej litery (podobnie jak pojęcie „dolar amerykański" pisany jest z małych liter). Natomiast tam, gdzie chodzi o system informatyczny, używana jest duża litera (wtedy „Bitcoin", a nie „bitcoin").

Przestrzegamy tutaj, że zbyt pochopne wchodzenie w świat kryptowalut może wiązać się z zagrożeniami. W szczególności, spekulowanie zawsze jest obarczone ryzykiem. Jednak rynek ten funkcjonuje już na tyle długo, że wiadomo, jakie są to ryzyka i jak je ograniczyć. Informacje takie są również zebrane w niniejszym opracowaniu.


# 1. Kryptowaluty i bąbel spekulacyjny

Pomimo pęknięcia bańki internetowej[2] na początku 2000 roku to aktualnie, właśnie firmy sektora IT przodują w gospodarce amerykańskiej pod względem wyceny (kolejno: Apple, Alphabet, Microsoft, Facebook, Amazon[3]). Dekadę temu pod względem kapitalizacji giełdowej dominowały spółki petrochemiczne, np. Exxon Mobile, PetroChina, Petrobras czy Royal Dutch Shell[4]. Czy doszłoby do tak dużej zmiany, gdyby podjęto skuteczną walkę z narastaniem bańki spekulacyjnej w 2. poł. lat 90.?

2 K. Smith, *History of the Dot-Com Bubble Burst and How to Avoid Another*, Money Crashers, https://www.moneycrashers.com/dot-com-bubble-burst [dostęp:30.10.2017].

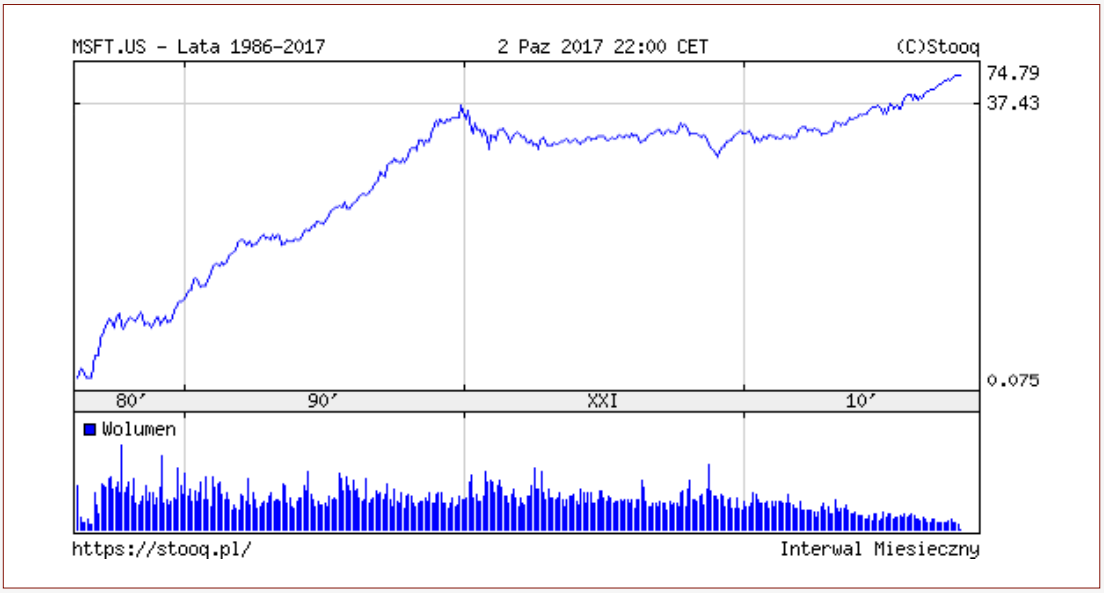
3 K. Kiesnowski, *The Top 10 US Companies by Market Capitalization*, CNBC.com, updated: 27 October 2017, https://www.cnbc.com/2017/03/08/the-top-10-us-companies-by-market-capitalization.html

4 K. Schwab, *The Fourth Industrial Revolution*, World Economic Forum, 2016.

## *Case study - Bańka na akcjach firmy Microsoft w 2. połowie lat 90. XX w.*

Jedna z czołowych firm branży IT w latach 90. była przedmiotem wzrostu cen jej akcji, który można określić mianem bańki spekulacyjnej.

*Wykres 1 Ceny akcji firmy Microsoft w latach 1986-2017*




*Uwaga: skala logarytmiczna.*

*Źródło: Stooq.pl [dostęp: 2 października 2017 r.]*

Na początku XXI w. część z inwestorów posiadających akcje Microsoft rzeczywiście straciła. Akcje tych, co je kupowali na szczycie bańki dopiero po 15 latach odzyskałyby swoją wartość. Jednak biorąc pod uwagę szerszy okres, od debiutu rynkowego w 1986 r. do dziś inwestorzy na akcjach Microsoft zarobili ponad 111 tysięcy procent (dane na początek listopada 2017 r.).

Ekonomista zadałby pytanie o to, jakie były efekty bańki internetowej? Czy doprowadziła ona gospodarkę USA do ruiny a społeczeństwo do życia w nędzy? Microsoft to obecnie największy producent oprogramowania na świecie, zatrudnia 114 tys. osób, a dzięki IPO (1986 r.), **12 tys. pracowników firmy stało się milionerami** (a trzech – miliarderami). Gospodarka amerykańska jest jedną z najbardziej innowacyjnych na świecie – w dużej mierze właśnie dzięki branży IT.

Ekonomista rozróżnia perspektywę mikroekonomiczną (jednej firmy czy rynku) od makroekonomicznej (całej gospodarki). Postawiłby więc sobie takie pytania:

- Czy bańki spekulacyjne są jednoznacznie złe? A jeśli są naturalnym elementem wyłaniania się nowego sektora gospodarki?
- Czy strach przed bańką nie doprowadziłby do ograniczenia rozwoju nowoczesnych technologii?

Jako Polacy mamy niewielki wpływ na rozwój rynków nowoczesnych technologii. Są to trendy światowe, nie zaś lokalne. Wygrają ci, którzy będą umieli je wykorzystać – szybciej niż inni będą umieli pozyskać do swojego kraju więcej pieniędzy, więcej talentów i startupów, niż sąsiedzi. Tak właśnie robi Szwajcaria, tak od niedawna robi nawet nieodległa od nas – Litwa, tworząc kolejne ułatwienia.

Należy pamiętać, że ci, którzy łatwiej zaadaptują się do zmian, mają szansę na tym dużo zyskać. Te kraje, które szybciej będą w stanie dostosować się do wyzwań technicznych, mają szansę na wykształcenie bardzo nowoczesnego rynku, na którym mogą powstać nowe przedsiębiorstwa pokroju Google lub Facebook. A takie „jednorożce" mogą później być „towarem eksportowym" kraju, w którym powstały, jego wizytówką, jak i źródłem przychodów budżetowych. Zwłaszcza, że Polska ma dobre podstawy do włączenia się do obecnej rewolucji przemysłowej – nasze kadry informatyczne są wysoko cenione w świecie.

Na nowe technologie można patrzeć z obawą, lecz nie można ograniczać postępu technologicznego z powodu braku dostatecznej wiedzy na ich temat. Takie obawy są naturalne – często boimy się nowego. Tym częściowo dr hab. K. Zacharzewski[5] tłumaczy komunikat NBP i KNF z lipca 2017 r. w sprawie „walut wirtualnych"[6].

Komunikat NBP nie zawiera wyczerpującej informacji o ryzykach związanych z kryptowalutami, wyolbrzymia niektóre zagrożenia a inne pomija, a także nie wskazuje, jak istniejące ryzyka zmniejszyć. Należy pamiętać, że kryptowaluty (mimo że już sama ta nazwa może wydawać się podejrzana – por. niżej) są w Polsce oraz w większości krajów legalne.

Słowo „kryptowaluty" jest mylnie kojarzone ze słownikowym znaczeniem jego przedrostka "krypto-", które oznacza coś niewidocznego, ukrytego, zamiast z prawidłową etymologią tego słowa, czyli jego pochodzeniem od **kryptografii**, która jest poddziedziną matematyki oraz informatyki. Kryptografia była używana chociażby w Enigmie w czasie II wojny światowej.

Europol (Europejski Urząd Policji) przypomniał niedawno, że bitcoin jest legalnym środkiem przechowywania wartości i metodą płatności[7]. W Szwajcarii można nim opłacać podatki

5 K. Zacharzewski, *Nie taki bitcoin straszny*, „Rzeczpospolita", 14 lipca 2017, http://archiwum.rp.pl/artykul/1347938-Nie-taki-bitcoin-straszny.html.

6 *Komunikat Narodowego Banku Polskiego i Komisji Nadzoru Finansowego w sprawie „walut" wirtualnych*, Narodowy Bank Polski, 7 lipca 2017 r., http://www.nbp.pl/home.aspx?f=/aktualnosci/wiadomosci_2017/ww-pl.html.

7 K. Helms, *Europol Discusses Bitcoin as Store of Value and Payment Method With the Industry*, Bitcoin.com, 6 lipca 2017 r., https://news.bitcoin.com/europol-bitcoin-store-of-value-legitimate-payment-method.

lokalne, a od kwietnia 2017 r. w Japonii jest on równoprawną metodą płatniczą[8], ze wszystkimi tego konsekwencjami[9]. Ponadto, wbrew często podnoszonym głosom, żaden publicznie dostępny raport na świecie nie wskazał dotąd choć jednego przypadku wykorzystania kryptowalut przez terrorystów; zaś dla przestępców są one na ogół zbyt trudne[10] lub zbyt mało anonimowe, co potwierdził niedawno raport UE[11].

W raporcie zamówionym i sygnowanym przez Parlament Europejski wskazano, że wraz ze wzrostem popularności walut cyfrowych gospodarstwa domowe zmniejszą ilość przetrzymywanej przez siebie gotówki, gdyż zaczną niektórych płatności dokonywać za ich pomocą[12]. W tym kierunku – zwiększenia obrotu bezgotówkowego – zmierza polski rząd. Jest to zapisane w programie „Od papierowej do cyfrowej Polski", będącym częścią „Strategii na rzecz Odpowiedzialnego Rozwoju" (tzw. Plan Morawieckiego). Prace te wspiera powołany przez Minister Cyfryzacji Annę Streżyńską Strumień „Blockchain/DLT i Waluty Cyfrowe"[13]

8 Japońska Agencja ds. Usług Finansowych (FSA) ogłosiła zmienioną Ustawę o usługach płatniczych, która jest częścią ustawy o bankowości, w której bitcoin i inne waluty wirtualne zostały skategoryzowane jako formy przedpłaconego instrumentu płatniczego („wartościowa własność" ang. *property of value*), a zatem jako formę płatności, a nie prawnie uznaną walutę, jak to często błędnie w Polsce media przytaczały. Por. L. Parker, *Bitcoin regulation overhaul in Japan*, 1 April 2017, Brave New Coin – Digital Currency Insights, https://bravenewcoin.com/news/bitcoin-regulation-overhaul-in-japan/

9 Na giełdy i kantory kryptowalutowe nałożony został szereg wymogów. Podlegają one teraz konieczności rejestracji, regulacjom dot. zapobieganiu praniu brudnych pieniędzy, zasadom identyfikacji tożsamości klientów (*know-your-customer*), wymogom kapitałowym (tak jak inne instytucje finansowe) czy postanowieniom dotyczącym cyberbezpieczeństwa. Firmy te są również zobowiązane do prowadzenia programów szkoleń pracowników i przedkładania rocznych audytów. (por. Financial Services Agency, 24 marca 2017 r., http://www.fsa.go.jp/news/28/ginkou/20170324-1.html).

10 N. Reiff, *Criminals Are Too Stupid to Use Cryptocurrency: EU Report*, Investopedia, 12 lipca 2017 r., http://www.investopedia.com/news/criminals-are-too-stupid-use-cryptocurrency-eu-report.

11 Secretary-General of the European Commission, "Commission Staff Working Document" Accompanying the document: Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundeirng and terrorist financing affecting the internal market and relating to cross-border situations, Bruksela, 4 lipca 2017 r., http://europeanmemoranda.cabinetoffice.gov.uk/files/2017/07/10977-17-ADD-2.pdf.

12 D. Heller, Directorate-General for Internal Policies. Policy Department A. Economic and Scientific Policy, *The Implications of Digital Currencies for Monetary Policy. Monetary Dialogue*, Maj 2017, http://www.europarl.europa.eu/cmsdata/118907/PIIE_FINAL%20upload.pdf, s. 9.

13 *Strumień Blockchain/DLT i Waluty Cyfrowe*, Ministerstwo Cyfryzacji, https://www.gov.pl/cyfryzacja/strumien-blockchain/dlt-i-waluty-cyfrowe [dostęp: 9 listopada 2017 r.].

– grupa ponad 50 ekspertów różnych specjalności doradzających *pro bono* Ministerstwu Cyfryzacji w tym zakresie. Pozycja Narodowego Banku Polskiego jest nieco inna – wydaje się raczej wspierać wykorzystanie gotówki[14], zaś Prezes jest przeciwnikiem kryptowalut[15]. Wiceprzewodnicząca sejmowej Komisji Gospodarki i Rozwoju M. Nykiel uważa, że zagrożenia wskazywane przez NBP i KNF są wyolbrzymione i nie oddają rzeczywistości[16]. Natomiast Parlament Europejski pociesza, że mimo że „upowszechnienie użycia walut cyfrowych zmniejszy popyt na pieniądz banku centralnego i przez to zmniejszy rozmiar bilansów banków centralnych", to „zyski banków centralnych zmniejszą się, ale nie znikną" i że „będą wciąż zdolne do efektywnego prowadzenia polityki pieniężnej"[17].

Pozytywny wpływ walut cyfrowych na gospodarkę wskazuje wiele instytucji np. Komisja Gospodarcza i Monetarna Parlamentu Europejskiego[18], Światowe Forum Gospodarcze, czy część banków centralnych. Część najbardziej postępowych banków centralnych podjęło prace badawcze, a także niektóre z nich – wdrożeniowe, dla tworzenia „narodowych" kryptowalut. Przykładem jest Dubaj, który na początku października 2017 r. zapowiedział emisję swojej kryptowaluty[19]. W Chinach upatruje się w tym dużych korzyści dla społeczeństw i dla gospodarki[20]. Ponadto nie możemy wykluczyć, że w przyszłości pieniądz kryptowalutowy wyprze zwykły, słabiej zabezpieczony bankowy pieniądz elektroniczny. K. Piech od lat promuje też tezę, że taki pieniądz będzie marzeniem urzędów skarbowych – wszystkie transakcje na blockchainie bitcoinowym są jawne, zebrane są w jednej bazie danych i można prześledzić ich przepływy. Dlatego też w niektórych krajach (np. Wielka Brytania) testowano wydawanie tokenów cyfrowych opartych na technologii blockchain w zakresie śledzenia wykorzystania środków pomocy społecznej.

14 J. Uryniuk, *Prezes NBP chyba woli gotówkę. Bank centralny wystąpił z organizacji promującej rozwój obrotu bezgotówkowego w Polsce*, Cashless.pl, 16 lipca 2017 r., https://www.cashless.pl/felietony/2831-prezes-nbp-chyba-woli-gotowke-bank-centralny-wystapil-z-organizacji-promujacej-rozwoj-obrotu-bezgotowkowego-w-polsce

15 J. Wilk, *Prezes NBP chętnie wprowadziłby zakaz dla kryptowalut*, FXMag, 9 listopada 2017 r., https://www.fxmag.pl/artykul/prezes-nbp-chetnie-wprowadzilby-zakaz-dla-kryptowalut

16 P. Dziubak, *KNF i NBP są zbyt konserwatywne w sprawie kryptowalut. Posłanka PO staje w obronie bitcoina*, Cashless.pl, 12 lipca 2017 r., https://www.cashless.pl/temat-dnia/2825-poslanka-nykiel-nbp-i-knf-sa-zbyt-konserwatywne-w-sprawie-kryptowalut

17 D. Heller, op. cit., s. 4.

18 Według niej istnieją „potencjalne korzyści z walut wirtualnych i związanych z nimi technologii dla konsumentów, przedsiębiorstw, organizacji charytatywnych i gospodarki ogółem, polegające między innymi na zwiększeniu prędkości i efektywności transakcji płatniczych i przelewów oraz na zmniejszeniu ich kosztów, zwłaszcza w kontekście transgranicznym, a także na wspieraniu włączenia społecznego pod względem finansowym oraz ułatwianiu sektorowi biznesu i MŚP dostępu do finansowania i zasobów finansowych". Komisja Gospodarcza i Monetarna, *Sprawozdanie w sprawie wirtualnych walut*, 3 maja 2016 r., http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2016-0168+0+DOC+XML+V0//PL.

19 D. J. Galeon, *Dubai just got its first official cryptocurrency*, Business Insider, 2 października 2017 r., http://www.businessinsider.com/dubai-official-cryptocurrency-blockchain-emcash-2017-10?IR=T.

20 W Chinach uważa się, że dzięki temu spadną koszty transakcyjne, przez co usługi finansowe będą bardziej dostępne. Zmniejszy się odsetek oszustw i fałszerstw, zmniejszy skala korupcji, zwiększy się odsetek transakcji międzynarodowych, co przyspieszy wzrost gospodarczy. T. Ward, *China Becomes First Country in the World to Test a National Cryptocurrency*, Futurism, 23 czerwca 2017 r., https://futurism.com/china-becomes-first-countrchina-becomes-first-country-in-the-world-to-test-a-national-cryptocurrencyy-to-test-national-cryptocurrency.

### *Czy bitcoin jest piramidą finansową?*

Przeciwnicy kryptowalut wielokrotnie opatrują je etykietą „piramidy finansowej". Jednakże przed wydawaniem tak radykalnego osądu warto najpierw sprawdzić definicję tego pojęcia.

- W strukturze wielu najpopularniejszych walut cyfrowych, w przeciwieństwie do mechanizmów opartych na „schemacie Ponziego" (ang. Ponzi scheme) brak jest centralnego emitenta lub innego podmiotu, który zarabiałby na sprzedaży jednostek dopiero co utworzonych lub na zmianie wartości tych, które zostały utworzone wcześniej.
- W modelu funkcjonowania kryptowalut próżno szukać wypłat dywidend lub odsetek za sam fakt ich posiadania, co jest jedną z cech charakterystycznych dla piramid finansowych.
- Ilość jednostek kryptowaluty wprowadzanych do obrotu jest określona przez algorytm, który – w większości przypadków najbardziej popularnych kryptowalut – nie jest kontrolowany przez żadną instytucję.
- Wymiana jednostek walut cyfrowych opiera się na cenie, którą proponuje sprzedający, zaakceptowanej przez kupującego. W związku z tym zarówno zyski jak i straty z zakupu kryptowaluty nie zależą od żadnej instytucji[21].

W związku z tym nie mamy podstaw do nazywania kryptowalut mianem piramidy finansowej.

Warto również wspomnieć o pseudo-kryptowalutach (tj. o projektach „kryptowalutopodobnych"), czyli takich, które jedynie podszywają się pod kryptowaluty wykorzystując ich rosnącą popularność (i ceny), ale w rzeczywistości nie spełniają ich prawdziwych cech, takich jak między innymi: kod otwartoźródłowy (*open source*), dostępny i weryfikowalny opis projektu (*whitepaper*), transparentność transakcji (czyli otwarta księgowość – blockchain), brak konieczności zaufanych trzecich stron odpowiadających za działanie kryptowaluty[22]. Są one często piramidami finansowymi.

Coraz więcej krajów tworzy warunki ku temu, by rynek firm kryptowalutowych się rozwijał; ostatnio nawet Rosja[23], której prezydent spotkał się niedawno z twórcą Ethereum[24]. Jednym z najbardziej znanych przykładów jest Crypto Valley Zug. Malutkie miasteczko, głównie za sprawą aktywności jednego, lokalnego polityka – Dolfiego Müllera, stało się siedzibą wielu,

21 A. Bubiel, *Bitcoin – determinanty i skutki jego akceptacji przez przedsiębiorstwa*, rozprawa doktorska, Kolegium Nauk o Przedsiębiorstwie Szkoły Głównej Handlowej w Warszawie, Warszawa 2017. Rozprawa ta (zawierająca ww. dowód na to, że bitcoin nie jest piramidą finansową) 25 października 2017 r. została obroniona z wyróżnieniem.

22 W. Kwiatek, Fragment wykładu: *Czym się różnią kryptowaluty od pseudowalut*, https://www.wykop.pl/link/3951739/fragment-wykladu-wojciecha-kwiatka-czym-sie-roznia-kryptowaluty-od-pseudowalut [dostęp:16.10.2017].

23 H. Amos, *Russia Is Becoming a Cryptocurrency Haven*, The Moscow Times, 9 lipca 2017 r., https://themoscowtimes.com/articles/russia-is-becoming-a-cryptocurrency-haven-58175.

24 M. del Castillo, *Vladimir Putin and Vitalik Buterin Discuss Ethereum 'Opportunities'*, CoinDesk, 5 czerwca 2017 r., http://www.coindesk.com/vladimir-putin-vitalik-buterin-discuss-ethereum-opportunities-recent-forum.

wiodących w branży firm (np. Ethereum, Xapo, ShapeShift, Tezos, czy nawet nasz rodzimy projekt Golem).

Dlaczego nie można by pójść tą drogą i stworzyć „dolinę blockchainową" w Polsce? Intelektualnie nasi informatycy nie ustępują tym z USA, Singapuru czy Szwajcarii, a jak wskazuje liczba i ranga wygranych konkursów oraz otrzymanych nagród – często bijemy ich na głowę[25]. Mamy więc unikalną szansę, zdarzającą się **raz na kilkanaście lat**, aby wejść do światowej czołówki technologicznej – obecnie jeszcze przy niewielkich nakładach kapitałowych. Za kilka lat będą potrzebne specjalne programy rządowe, by móc „dogonić Zachód", a wtedy może to być już zbyt trudne. Będziemy zmuszeni kupować rozwiązania technologiczne z zagranicy ze względu na brak rodzimych rozwiązań – już teraz polscy programiści biorą udział w wielu projektach blockchainowych realizowanych przez międzynarodowe zespoły. A to w dużej mierze przez strach przed „piramidami finansowymi", strach przed nowymi technologiami, przez brak jasnych regulacji oraz gdzie trzeba – deregulacji (np. w formie dedykowanego środowiska regulacyjnego do testowania rozwiązań).

25 T. Staśkiewicz, *Polscy programiści jednymi z najlepszych na świecie. Jest nawet kategoria, w której wygrywamy*, INNPoland, 31 sierpnia 2016 r., http://innpoland.pl/129313,polscy-programisci-docenieni-w-rankingu-hackerrank-jest-kategoria-w-ktorej-jestesmy-najlepsi-na-swiecie; J. Kuźniak, *Polscy programiści coraz częściej zostawiają w tyle dotychczasowych liderów*, Forsal.pl, 14 grudnia 2013 r., http://forsal.pl/artykuly/764634,polscy-programisci-coraz-czesciej-zostawiaja-w-tyle-dotychczasowych-liderow.html.

Źródło: www.canva.com

# 2. Technologia blockchain

Eksperci z zakresu cyberbezpieczeństwa i kryptografii oceniają, że technologia przechowywania danych i systemów rejestrowanych oparta na technologii blockchain (na której jest oparty m.in. bitcoin), nie jest możliwa do rozszyfrowania i złamania[26]. Dodatkowymi jej zaletami są niższe koszty jej użytkowania w porównaniu do systemów centralnych oraz większe bezpieczeństwo – również odporność na ingerencję obcych służb czy zorganizowanych, międzynarodowych grup hakerskich. Oczywiście, blockchain blockchainowi nie jest równy, więc docelowe rozwiązania (ich koszty czy bezpieczeństwo) zależą od szczegółowych wyborów. Przykładowo, prywatne blockchainy wcale nie muszą być bardzo bezpieczne tylko dlatego, że są blockchainami. Poniżej przybliżymy kilka podstawowych zagadnień związanych z tą technologią.

## 2.1. Blockchain bitcoinowy

Zrozumienie technologii blockchain jest kluczowe w kontekście poznawania kryptowalut. Żeby zrozumieć fenomen bitcoina, warto cofnąć się do 2008 roku i przyjrzeć się sytuacji gospodarczej. Na świecie rozpoczął się wtedy kryzys finansowy. Zaufanie wielu osób do instytucji

26 Przy współczesnym stanie techniki – przy czym sam kod kryptowaluty można zmieniać, a zatem uodpornić ją nawet na postęp w łamaniu zabezpieczeń kryptograficznych w przyszłości.

finansowych legło w gruzach. Odpowiedzią na to, a także na potrzebę znalezienia nowej, bezpiecznej drogi komunikacji między systemami informatycznymi, stał się projekt systemu Bitcoin opublikowany przez Satoshiego Nakamoto w październiku 2008 roku[27]. 3 stycznia 2009 roku wydana została pierwsza wersja oprogramowania do obsługi portfela bitcoinowego. Przełomową jest nie tylko koncepcja waluty cyfrowej, co sama technologia, na której jest oparta, czyli blockchain.

Sama idea blockchaina nie jest trudna do zrozumienia (choć szczegóły technologii – już tak). Pomijając wszystkie kwestie programistyczne i matematyczne **blockchain to księga rozrachunkowa zawierająca listę transakcji** (dokonywanych w danej kryptowalucie – o ile została ona przewidziana w danym blockchainie), a także jednocześnie system transakcyjny. Poniżej opiszemy tę technologię na przykładzie najbardziej popularnego jej zastosowania – w bitcoinie.

Blockchain bitcoinowy zaczyna się od wpisu mówiącego o tym, iż właściciel danego adresu publicznego (przez analogię: numer rachunku) o oznaczeniu 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa wygenerował pierwszych 50 bitcoinów (tzw. *genesis block*). Każdy następny wpis zaczyna się właśnie od takiego wygenerowania kolejnej transzy i przydzielenia do konkretnego adresu. W blokach, oprócz zapisów dotyczących nowo powstałych bitcoinów, zawarte są również transakcje dotyczące już istniejących cyfrowych „monet”[28]. Bloki, czyli kolejne rozdziały księgi pt. blockchain, mają ograniczoną pojemność. W przypadku bitcoina wielkość bloku to dotychczas 1 MB (trwają negocjacje nad jego zwiększeniem[29]). W konsekwencji tego, iż bloki mają ograniczoną wielkość, to jeśli popyt na transakcje przewyższa możliwości techniczne systemu, to część wykonanych w danym okresie transakcji pozostaje w kolejce oczekiwania na dodanie przy kolejnej, możliwej okazji. Zazwyczaj kryterium dodawania transakcji do bloku jest wartość opłaty transakcyjnej – również wyrażona w bitcoinach. Im wyższa, tym większe prawdopodobieństwo, iż dana transakcja zostanie dodana do blockchaina już w kolejnym bloku[30].

27 S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin.org, https://bitcoin.org/bitcoin.pdf.

28 Profesor Marian Srebrny z Polskiej Akademii Nauk uważa, że w odniesieniu do bitcoina (i innych kryptowalut) właściwsze byłoby używanie pojęcia cyfrowych „banknotów”, niż monet. Każdy banknot ma swoje indywidualne oznaczenie (seria i numer), podczas gdy monety ich nie posiadają. Podobnie każdy bitcoin ma indywidualne oznaczenie. Przy czym, inaczej niż w przypadku banknotów, każdy fragment bitcoina jest oznaczony niezależnie czy jest to ich 1000 sztuk, czy 1/1000 bitcoina.

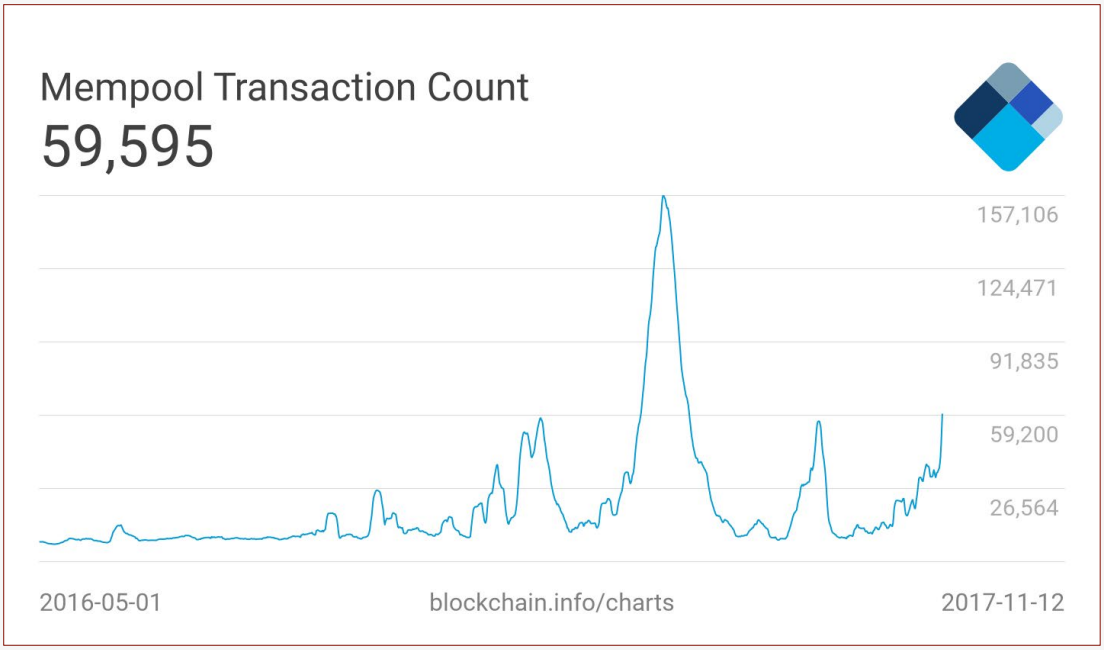
29 W przypadku odłamu bitcoina – bitcoin casha, wielkość bloku to aż 8 MB.

30 Zob. K. Piech (red.), *Leksykon pojęć na temat technologii blockchain i kryptowalut*, Strumień „Blockchain i kryptowaluty”, Ministerstwo Cyfryzacji, 8 listopada 2016 r., https://www.gov.pl/documents/31305/0/leksykon_pojec_na_temat_technologii_blockchain_i_kryptowalut.pdf.

## *Opłaty transakcyjne w sieci Bitcoin*

Należy uważać, aby nasz „przelew" kryptowalutowy poparty został odpowiednią opłatą transakcyjną, gdyż może „utknąć w kolejce" (*mempool*) – na bardzo długo. W rekordowym maju 2017 r. liczba transakcji oczekujących na zatwierdzenie przekraczała 125 tysięcy (ostatnio prawie 60 tysięcy).

*Wykres 2 Liczba transakcji bitcoinowych oczekujących na potwierdzenie*




*Źródło: blockchain.info [dostęp: 13 listopada 2017 r.]*

Jeśli się tak stanie, można „dopłacić" do takiej transakcji, by ją przyspieszyć. Warto przy tym zaznaczyć, iż system Bitcoin jest technologią, która podlega ciągłemu rozwojowi (por. BIP – Bitcoin Improvement Proposal). Trwają prace nad zwiększeniem liczby transakcji, które można zapisać w jednym bloku blockchaina bitcoinowego[31]. Zaplanowana na 16 listopada 2017 r. implementacja takiej „reformy" została odwołana (co odbiło się na cenie bitcoina).

Transakcje dodawane są przez komputery należące do członków społeczności bitcoin zwanych „górnikami" (ang. *miners*), poprzez analogię do górników wydobywających złoto – tutaj: cyfrowe. Osoby te angażują moc obliczeniową swojego sprzętu (kiedyś zwykłych komputerów, później wyspecjalizowanych urządzeń zaprojektowanych wyłącznie do tego celu) otrzymują „nagrodę" w postaci nowych bitcoinów (obecnie co ok. 10 minut algorytm rozdziela 12,5 bitcoina

31 A. Hertig, *Calm Before the Fork? Segwit2x Goes Silent as Bitcoin Split Looms*, CoinDesk, https://www.coindesk.com/calm-fork-segwit2x-goes-silent-bitcoin-spilt-looms [dostęp: 16 października 2017 r.].

pomiędzy wszystkie osoby zaangażowane w „wykopywanie" bitcoinów) oraz zebranych opłat transakcyjnych. Każdy górnik samotnie kopiący kryptowaluty musi przechowywać na swoim komputerze równoprawną kopię blockchaina (tj. księgi rozrachunkowej), jednakże w większości przypadków górnicy łączą się w tzw. poolach (spółdzielniach) i nie jest wtedy wymagane, aby każdy górnik z osobna posiadał na swoim komputerze kopię całej bazy blockchain.

Blockchain bitcoina zawiera zapisy operacji dla każdej wyemitowanej „monety" bitcoin od momentu jej powstania do chwili obecnej. Bitcoin jest podzielony na 100 000 000 jednostek zwanych satoshi. Blockchain zawiera zapisy o każdym transferze każdej jednostki danej kryptowaluty. W efekcie tego rozmiar blockchaina stale się powiększa. Wielkość blockchaina bitcoinowego to aktualnie bowiem aż 166 GB, a wielkość blockchaina drugiej pod względem kapitalizacji waluty – ethereum to 140 GB[32].

Blockchainy publiczne są ogólnodostępne, a do przeszukiwania tej bazy służą bezpłatnie dostępne eksploratory łańcuchów bloków. Najpopularniejsze z nich to dla Bitcoina – www.blockchain.info, a dla Ethereum – www.etherscan.io.

Publiczny blockchain z reguły (choć nie zawsze) ma taką właściwość, że wszystkie zapisy w nim są dostępne do sprawdzenia przez każdego i każdy węzeł sieci przetrzymuje pełną informację o wszystkich, dokonanych w przeszłości wpisach do tej bazy danych. Wszelkie zatem próby fałszerstwa mogłyby zostać zatem szybko zidentyfikowane.

Większość publicznych blockchainów jest transparentna. Oznacza to, że wszystkie adresy użyte do transakcji oraz wszystkie transakcje są jawne. Jest to dla niektórych wadą – stąd powstały blockchainy ukrywające transakcje. Bitcoin (i wiele innych kryptowalut) to system pseudonimowy, bo z jednej strony zapewnia jawność transakcji, ale z drugiej – nie pozwala jej powiązać z konkretną osobą. Aktualnie jednak transakcje oparte na bitcoinie nie są w 100% anonimowe i istnieją metody skutecznego wyśledzenia konkretnej osoby[33]. Metodami stosowanymi w celu próby śledzenia transakcji bitcoinowych są między innymi techniki śledzenia „ciasteczek" i badania z użyciem analizy heurystycznej[34].

Warto podkreślić, iż w blockchain bitcoinowy (oraz w wiele innych publicznych) wbudowany jest kryptograficzny mechanizm autoregulacji. Polega to na tym, iż mimo zmian mocy sprzętu obliczeniowego zaangażowanego w ochronę sieci i autoryzację transakcji w niej, każdy kolejny blok transakcji powstaje średnio co 10 minut. Odstęp ten pomaga też regulować podaż

32 Cryptocurrency statistics, https://bitinfocharts.com [dostęp: 12 listopada 2017 r.].

33 *Bitcoin Transactions Aren't as Anonymous as Everyone Hoped*, MIT Technology Review, 23 sierpnia 2017 r., https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped.

34 S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. Voelker, S. Savage, *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, University of California – San Diego, https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf [dostęp: 12 listopada 2017 r.].

nowych bitcoinów do sieci oraz zapobiega zbyt częstym rozgałęzieniom łańcucha[35]. W blockchainie litecoina nowy blok transakcji powstaje średnio do 2,5 minuty, a w Ethereum przez długi czas (przez ok. rok – do kwietnia 2017 r.) było to jedynie 14 sekund[36].

Opisane powyżej cechy technologii blockchain są jedynie podstawowymi informacjami, które ułatwiają ogólne zrozumienie tego zagadnienia. W kolejnym podrozdziałach opisano na podstawie przykładów bardziej szczegółowe aspekty blockchaina, a szczególnie jej kryptowalutowych implementacji.

## 2.2. Problem bizantyjskich generałów

Przedstawienie problemu bizantyjskich generałów często pomaga czytelnikom w zrozumieniu trudności, jakie musiał pokonać Satoshi Nakamoto. Udało mu się rozwiązać problem, który od lat był wyzwaniem dla informatyków. Nie chodziło tu tyle o stworzenie kryptowaluty, ale o zapewnienie niezaprzeczalności komunikacji pomiędzy nieufającymi sobie podmiotami informatycznymi oraz jej zabezpieczenie przed fałszerstwem.

Analogia, od której często się zaczyna prezentację logiki funkcjonowania blockchaina i kryptowalut, polega na przedstawieniu sytuacji oblężenia zamku, w którym uczestniczy kilka niezależnych oddziałów, każdy pod dowództwem jednego generała. Ze względu na odległość pomiędzy poszczególnymi oddziałami komunikacja na szczeblu dowództwa nie jest natychmiastowa. **Jedynym sposobem zdobycia zamku jest jednoczesny atak**. Jeśli ktoś wyłamie się z ustaleń o jednoczesnym ataku, wygrają obrońcy zamku.

Przy dwóch generałach wydawałoby się, że komunikacja powinna być prosta. Generał A wysyła wiadomość o terminie ataku. Generał B otrzymuje ją. Jednak generał A nie może być tego pewien. Prosi zatem o potwierdzenie otrzymania wiadomości. Generał B zatem wysyła to potwierdzenie, ale nie wie, czy dotarło ono do adresata oraz jaką miało treść – posłaniec mógłby bowiem po drodze zaginąć, komunikat mógłby zostać przejęty przez wroga i zastąpiony inną wiadomością. Musi poczekać zatem z podjęciem decyzji o ataku do czasu, aż generał A wyśle mu odpowiedni komunikat. Jednak jak go otrzyma, nadal nie może być w pełni pewien o tym, czy nie został on sfałszowany. Poza tym, generał A musi być pewien, czy B otrzymał jego potwierdzenie, bo – jeśli zaatakuje sam – jego armia poniesie klęskę. I tak dalej[37].

Sytuacja komplikuje się jeszcze bardziej, gdy generałów jest więcej niż dwóch (dla trzech z nich problem ten jest nierozwiązywalny), a także gdy istnieje ryzyko, że wśród nich jest

35 E. Lendzion-Stachera, *Rozłamy w sieciach blockchain*, Uczelnia Łazarskiego, https://www.lazarski.pl/pl/wydzialy-i-jednostki/instytuty/wydzial-ekonomii-i-zarzadzania/centrum-technologii-blockchain/rozlamy-w-sieciach-blockchain [dostęp: 24.08.2017].

36 Następnie do połowy października 2017 r. wzrosło do prawie 30 sekund, po czym ponownie jest to 14 sekund

37 Zob. *Problem bizantyjskich generałów*, Wikipedia, https://pl.wikipedia.org/wiki/Problem_bizantyjskich_genera%C5%82%C3%B3w [dostęp 19 lipca 2017 r.].


zdrajca. Dla uzmysłowienia sobie skali problemu wyobraźmy sobie, że trzeba by było skoordynować i skomunikować ze sobą nie kilka osób, ale kilka tysięcy osób, z których nikt się nie zna i nie musi sobie ufać, a wielu z nich może chcieć po prostu oszukać innych. Z takim właśnie problemem zmierzył się Satoshi Nakamoto – i udało mu się rozwiązać ten problem.

Rozwiązanie polegało na tym, że każdy z generałów (a w szerszej wersji – każda osoba autoryzująca transakcje w blockchainie) otrzymuje wiadomości od innych. Zbiera je w określonym wcześniej czasie (dla przypomnienia w bitcoinie – co ok. 10 minut), a następnie potwierdza je wysyłając informację do innych, załączając oryginały wiadomości, które otrzymał. Następnie również wszyscy wysyłają do siebie wiadomości – również w oznaczonym czasie. Porównują je i jeśli gdzieś zobaczą rozbieżność, takiej informacji mogą nie uwzględniać. Po kilku takich iteracjach (potwierdzeniach) uzyskuje się duże prawdopodobieństwo (w przypadku zwyczajowo przyjmowanych sześciu potwierdzeń w bitcoinie – graniczące z pewnością[38]), że generałowie ustalą, co jest prawdą. System można by sfałszować wtedy, gdyby ponad 50% generałów okazało się być zdrajcami lub też, gdyby ponad 50% z nich musiało wykonywać czyjeś polecenia (dlatego w blockchainie czy ktoś jest kelnerem, czy szefem banku centralnego – ma takie same prawa i dzięki temu system jest bezpieczny). Stąd w blockchainie ważne jest, by nie było podmiotu dominującymi nad innymi, np. by tzw. kopanie nie było na tyle scentralizowane, by można było przeprowadzić tzw. ataku 51%[39], a także by żadna firma nie mogłaby kontrolować

38 W większości przypadków w systemie Bitcoina przyjmuje się, że sześć potwierdzeń jest wystarczające, by uzyskać pewność co do tego, czy transakcja miała miejsce. Nie jest to jakaś specjalna liczba, a wynika z rozkładu prawdopodobieństwa. Nakamoto przyjął założenie występowania rozkładu Poissona. Jeśli atakujący miałby do dyspozycji aż 10% mocy obliczeniowej tej sieci, wtedy prawdopodobieństwo, że przy 6 potwierdzeniach transakcja zostałaby sfałszowana wynosiłoby 0,024%. S. Nakamoto, op. cit., s. 8. Jeśli ktoś miałby do dyspozycji 1% mocy sieci, to przy już dwóch potwierdzeniach prawdopodobieństwo udanego ataku wynosiłoby 0,05%. Różne warianty parametrów można przetestować na stronie: https://people.xiph.org/~greg/attack_success.html.

39 Atak ten oznacza, że jedna osoba, grupa osób lub pewna organizacja posiadająca 51% mocy obliczeniowej całej sieci będzie mogła przejąć kontrolę nad siecią i akceptować te transakcje, które będą dla niej korzystne. Aktualnie „atak 51%" („atak większości") jest mało prawdopodobny, ponieważ moc obliczeniowa całej sieci jest zbyt duża, zaś „spółdzielnie" górników (*mining pool*) są wystarczająco rozproszone. „W praktyce system Bitcoin jest skonstruowany tak, że bardziej opłaca się autoryzować transakcje i zarabiać na prowizjach i nagrodach za tę pracę, niż <niszczyć własne bogactwo>". D. Homa, *Sekrety Bitcoina i innych kryptowalut*, Helion, Gliwice 2015, s. 165.

blockchaina – jak to bywa w tzw. prywatnych blockchainach (wtedy bowiem decyzją tej firmy można by modyfikować zawartość bazy danych).

Blockchain jest technologią rozproszonych rejestrów, ale jest on wiarygodny tylko wtedy, jeśli decentralizacja jest dobrze zaprojektowana, tj.:

- gdy występuje ona wśród twórców oprogramowania (*developers*) oraz jednostek zajmujących się autoryzacją transakcji (*miners*),
- a także gdy nie ma centralnego punktu podatnego na błędy (*central point of failure*)[40].

## 2.3. Konsensus

Celem osób zajmujących się potwierdzaniem transakcji jest osiągnięcie **konsensusu** co do tego, które transakcje są prawidłowe i które finalnie należy dołączyć do rejestrów w systemie blockchain. Opuszczając pole bitwy i przechodząc do zastosowań finansowych – technologia blockchain uniemożliwia wydanie większej ilości środków, niż się posiada, w tym tzw. skuteczne podwójne wydanie ich (*double spend*). Wszelkie próby sfałszowania stanu rzeczy, przekłamania komunikacji, zostaną wykryte przez innych. Do sfałszowania transakcji mogłoby dojść wtedy, gdy ktoś byłby w stanie podmienić ponad 50% kopii baz danych blockchaina rozsianych po świecie. Przy dobrze zaprojektowanym (tj. odpowiednio rozproszonym) blockchainie nie powinno być to możliwe. Dowodem na to jest fakt, że Bitcoin działa bezbłędnie i nieprzerwanie od ponad 8 lat. Przez blockchain bitcoinowy przeszły już transakcje o wartości setek miliardów dolarów. I ani ułamek z nich nie został sfałszowany, ani utracony[41]. Systemy zarówno IT jak i księgowe nie są doskonałe, przez co zdarzają się sytuację, gdy stan środków się nie zgadza. Absolutną pewność, co do stanu wzajemnych rozliczeń ma się dlatego, ponieważ zaangażowana jest w ich potwierdzanie „strona trzecia”[42]. Zwykle taką czynność przeprowadza instytucja rozliczeniowa (*clearing house*), której się ufa, albo dokonywane jest to poprzez audyt. W blockchainie nie ma jednej, centralnej instytucji będącej tą „zaufaną trzecią stroną” (ang. *trusted third party*) – jest ona rozproszona (i zastąpiona przez tzw. „górników”). I w dodatku można jej ufać, nawet jeśli nie zna się tożsamości osób, które za takimi jednostkami stoją.

By tak się stało, musi zostać osiągnięty tzw. konsensus. W jakiś sposób trzeba ustalić, co jest prawdą, co jest prawdziwym stanem zapisów w bazie danych, a co nie. W blockchainach

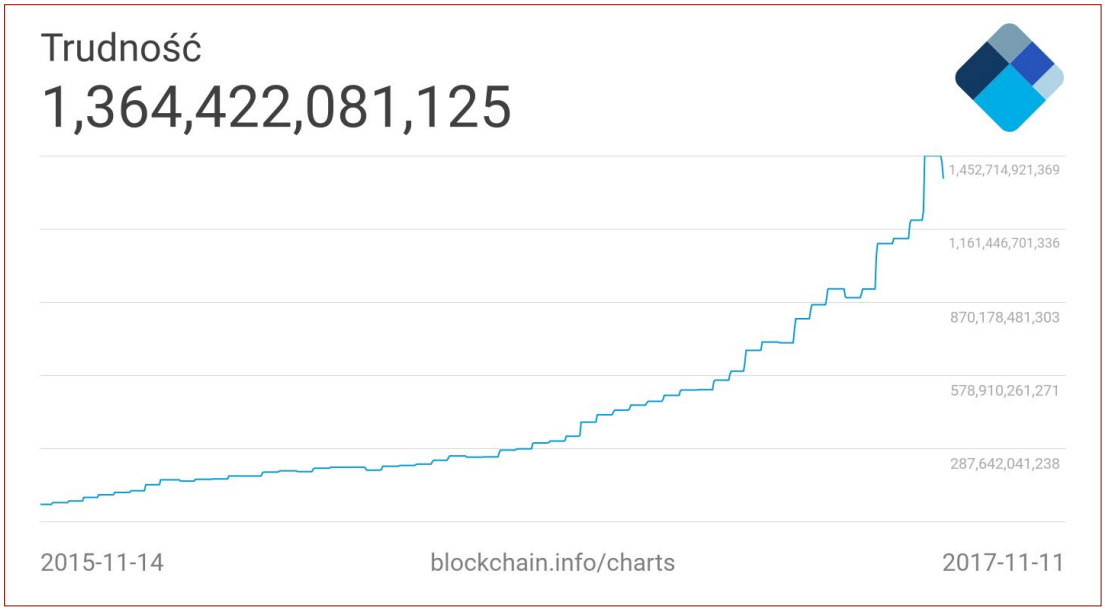
40 Bardzo dobry artykuł na ten temat napisał na swoim blogu V. Buterin, *The Meaning of Decentralization*, Medium, 6 lutego 2017 r., https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274 [dostęp: 24.08.2017].

41 Choć istnieją już poole, jak np. Large Bitcoin Collider (LBC, https://lbc.cryptoguru.org), które dla udowodnienia, że jest to możliwe, próbują uzyskać dostęp do istniejących kluczy prywatnych przez odnajdywanie kolizji prywatnych kluczy.

42 W księgowości obowiązuje zasada tzw. podwójnego księgowania; blockchain wprowadza potrójne, tj. wszystkie transakcje pomiędzy dwiema jej stronami potwierdzane są jeszcze przez trzecią stronę, którą jest blockchain. J.M. Tyra, *Triple Entry Bookkeeping With Bitcoin*, “Bitcoin Magazine”, 10 lutego 2014 r., https://bitcoinmagazine.com/articles/triple-entry-bookkeeping-bitcoin-1392069656.

kryptowalutowych potwierdzaniem transakcji zajmują się „górnicy", zaś ściślej – mówiąc ich sprzęt obliczeniowy. Porozumienie pomiędzy nimi osiągane jest najczęściej na podstawie okazania przez nich tzw. dowodu wykonania pracy (ang. *proof-of-work*, PoW). W systemie Bitcoin każdy „górnik" rozwiązuje pewne równanie matematyczne. Aby zachęcić go do tego (w tym zachęcić go do udostępnienia w tym celu mocy obliczeniowej swojego sprzętu[43]), za każdy zweryfikowany blok otrzymuje „nagrodę" (w postaci bitcoinów lub innej, natywnej kryptowaluty). I tu uwidacznia się geniusz, nie tylko informatyczny, ale i ekonomiczny Satoshiego Nakamoto. „Górnicy" – jako racjonalne jednostki – kierują się maksymalizacją swoich korzyści, tj. chcą mieć więcej jednostek danej kryptowaluty. Zatem – jeśli uznają, że może im się to opłacać – będą podłączać do sieci kryptowaluty sprzęt obliczeniowy o coraz to większej mocy. Jednak – jak wspomniano – sieć automatycznie dostosuje poziom trudności rozwiązywania obliczeń (poziom trudności zmienia się co 2016 bloków, co stanowi średnio 14 dni). Dzieje się tak po to, by średnio w tym samym przedziale czasu taka sama liczba nowych jednostek kryptowaluty była uwalniana do sieci. Ponadto, w przypadku bitcoina, co ok. 4 lata ich liczba dwukrotnie się zmniejsza. Początkowo było to nawet 50 bitcoinów, teraz (2017 r.) 12,5 BTC.

*Wykres 3 Zmiany poziomu trudności sieci Bitcoin w ciągu ostatnich dwóch lat*




*Źródło: blockchain.info [dostęp: 13 listopada 2017 r.]*

43 Podobnym eksperymentem z zakresu udostępniania mocy obliczeniowej był program Seti@home. Był on koordynowany przez Uniwersytet Kalifornijski w Berkley. Zainicjowany został w 1999 r. i miał na celu znalezienie sygnałów pochodzących od pozaziemskich cywilizacji. By to osiągnąć wykorzystano możliwość rozproszenia przeprowadzania obliczeń dla wyeliminowania szumów zarejestrowanych przez radioteleskop. Dzięki temu w szczytowym momencie (2013 r.) miał moc obliczeniową 670 teraflopsów, czyli 50 razy mniej od największego w tamtym czasie superkomputera (Seti@home, Wikipedia, https://en.wikipedia.org/wiki/SETI@home [dostęp: 12 listopada 2017 r.]. Tymczasem sieć Bitcoin już w 2013 r. miała moc obliczeniową ponad 250 razy większą, niż 500 największych superkomputerów na świecie razem wziętych. R. Cohen, *Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined!*, Forbes, 28 listopada 2013 r., https://www.forbes.com/sites/reuvencohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/#28f8da4d6e5e

Jak można się domyślać, pomiędzy „górnikami" trwa wyścig o to, kto pierwszy odkryje rozwiązanie i uzyska nagrodę. Doprowadziło to w konsekwencji do powstania nowego przemysłu – twórców sprzętu obliczeniowego dedykowanego wyłącznie do autoryzowania transakcji w sieci Bitcoin (a także do wzrostu popytu na karty graficzne, które mogą być wykorzystywane do „kopania" w innych blockchainach, np. Ethereum, Litecoin). Porównując „kopanie" eteru i bitcoina do zużycia energii przez jedno państwo, „cyfrowi górnicy" zajęliby 71. pozycję na świecie, z zużyciem energii większym niż np. Islandia[44].

Oprócz PoW, istnieją inne sposoby uzyskiwania konsensusu.

- Proof-of-Stake (dowód stawki) – sposób oparty na ilości posiadanej waluty. Im większą liczbę jednostek danej kryptowaluty posiada uczestnik tym większa szansa, że to on utworzy nowy blok. Osoba zatwierdzająca otrzymuje tylko opłaty użytkowników. Są dwie metody wyboru twórcy bloku: pseudolosowa, gdzie znaczenie ma tylko ilość stawki oraz 'coin-age based', w której pod uwagę bierze się też czas jej posiadania. Kryptowaluty oparte na PoS to np. NXT, BlackCoin. W Ethereum wprowadzenie PoS jest nadal w trakcie przygotowań (stan na październik 2017 r.).
- Delegated Proof-of-Stake (delegowany dowód stawki) – sposób opiera się na wyborze przez posiadaczy waluty określonej liczby delegatów w drodze głosowania. Tylko delegaci są uprawnieni do dodawania nowych bloków do łańcucha bloków, za co otrzymują nagrody. Konsensus oparty na dPoS zastosowano np. w BitShares.
- Provable Data Possession (PDP) – pozwala użytkownikowi wysłać dane na określony serwer i później sprawdzać, czy te dane nadal się tam znajdują.
- Proof-of-Retrievability (PoRet) – rozwinięcie PDP, umożliwiające także odzyskanie wysłanych danych. Jednak wymaga to wysłania kilku zapytań i rekonstrukcji danych z otrzymanych fragmentów.
- Proof-of-Storage (PoS) – opiera się na zleceniu innemu użytkownikowi przechowywania danych, a następnie wielokrotnego sprawdzania czy są one nadal przechowywane. Ten schemat jest uogólnieniem PDP oraz PoRet.
- Proof-of-Replication (PoRep) – jest to rodzaj Proof-of-Storage, który dodatkowo wymaga poświęcenia danym unikalnej pamięci fizycznej. Uniemożliwia to przechowywanie tych samych danych dwukrotnie w jednym miejscu.
- Proof-of-Space (PoSpace) – schemat wymagający udowodnienia przez uczestnika, że poświęcił on część swojej pamięci. Nie wymaga to tak dużych nakładów energii elektrycznej jak PoW[45].
- Proof-of-Spacetime (PoSt) – jest to PoSpace z sekwencją sprawdzeń rozłożonych w czasie.
- Proof-of-Importance (PoI) – jest to pochodna systemu Proof-of-Stake, ale z szeregiem

44 B. Sanak, T. Kurowski, *Konsensus w sieci blockchain - czym jest i jak go osiągnąć?*, FXMag, 11 sierpnia 2017 r., https://www.fxmag.pl/artykul/konsensus-w-sieci-blockchain-czym-jest-i-jak-go-osign.

45 Warto uzupełnić, że autorem koncepcji *proof of space* jest polski kryptograf prof. Stefan Dziembowski z Uniwersytetu Warszawskiego. Por. S. Dziembowski, S. Faust, V. Kolmogorov, K. Pietrzak, *Proofs of space*, [In:] r. Gennaro, M. Robshaw (eds.), *Advances in Cryptology – CRYPTO 2015*, Springer, Heidelberg 2015, str. 585-605. Została ona wykorzystana w kryptowalucie Burst (Burstcoin). Por. *What is Burstcoin*, http://burstblast.site/guides/what-is-burstcoin/ [dostęp: 12 listopada 2017 r.].

ulepszeń. Zastosowane formuły matematyczne przetwarzają informacje o koncie, aby zdecydować, jak ważna dla grupy jest dana osoba. Im większą masz ważność, tym większe masz szanse na uzyskanie opłat transakcyjnych pozostawionych przez innych użytkowników podczas „kopania". Aktualnie najpopularniejszą kryptowalutą korzystającą z tego typu rozwiązania jest NEM[46].

Pozostałe sposoby na otrzymanie konsensusu to np.: Proof-of-Authority, Proof-of-Capacity, Proof-of-Burn oraz hybrydy łączące dwa wcześniej wymienione sposoby. Są one jednak znacznie mniej upowszechnione (w związku z tym ma się do nich znacznie mniejsze zaufanie), a niektóre nie wyszły poza fazę eksperymentalną.

## 2.4. Koncepcja „ekonomicznej większości"

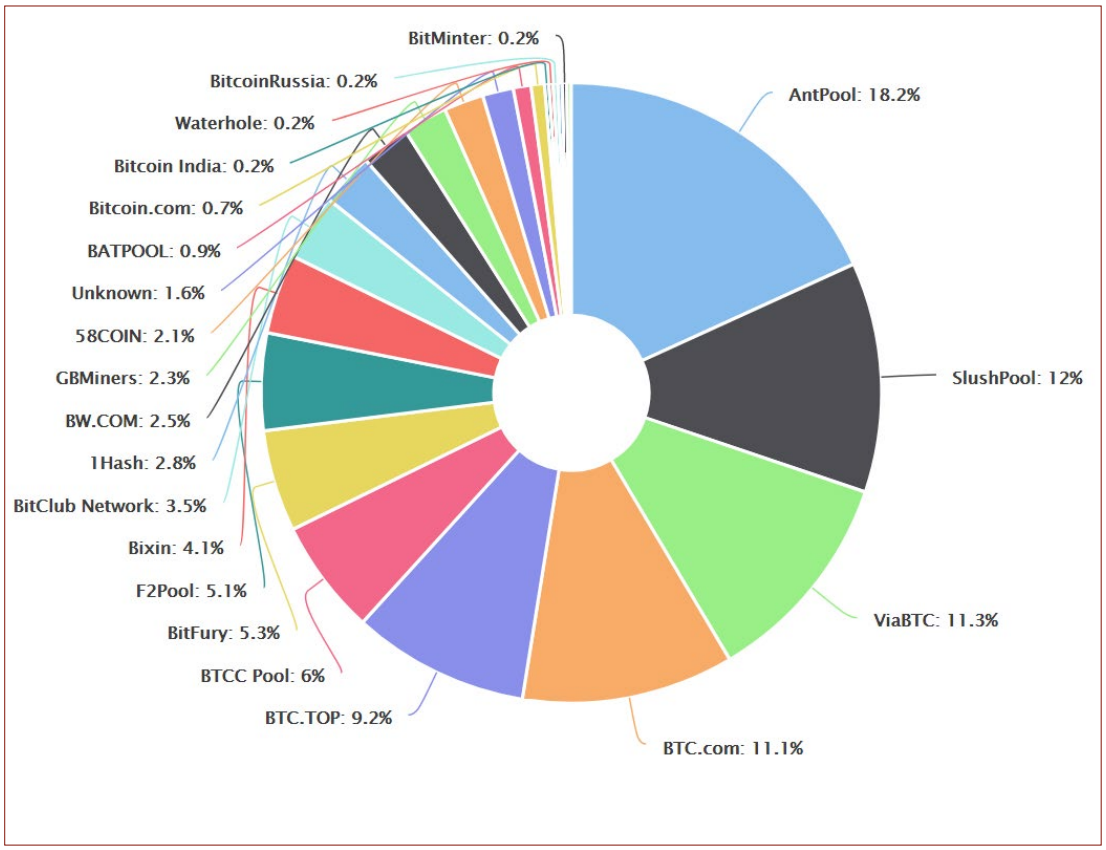
Ciekawym, teoretycznym jak się przez długi czas wydawało (ze względu na brak możliwości sprawdzenia go w praktyce) zabezpieczeniem systemów, opisanym z myślą o bitcoinie, jest koncepcja „większości ekonomicznej" (*economic majority*)[47]. Mówi ona, że zdolność do kontrolowania protokołu Bitcoin leży nie po stronie jednostek zajmujących się autoryzacją transakcji („górników"), po stronie osób zdolnych i skłonnych oferować rzeczy wartościowe dla Bitcoina (czy to towarów, usług czy innych walut). Jeśli „górnicy" wprowadziliby zmiany w protokole Bitcoina, które byłyby oczekiwane przez społeczność mającą „większość ekonomiczną", wtedy możliwe by było, że „monety" wydobywane przez nich nie zostaną uznane przez tych, którzy nie zaakceptowali zmian. Wtedy zaś „górnicy" nie zyskaliby na wprowadzaniu zmian nie uzgodnionych z „większością ekonomiczną".

Zdolność do pomyślnego wdrożenia zmian w protokole Bitcoin w ostateczności spoczywa na tych, którzy akceptują bitcoiny w zamian za wartość. Ogólnie rzecz biorąc, to będą kupcy. Koncepcja „większości ekonomicznej" sugeruje, że nawet oligopolizacja pooli kopalni nie będzie miała pełni władzy nad systemem i musiała uzgadniać zmiany z akceptantami. W skrajnym przypadku, gdyby jeden z nich uzyskał większość mocy obliczeniowej i zdolność do przeprowadzenia „ataku 51%", sytuacja taka mogłaby zostać uznana przez społeczność za niebezpieczną, za grożącą ryzykiem dla utrzymania bezpieczeństwa systemu, a w efekcie tego cena bitcoina by spadła (co nie byłoby po myśli tych, chcących ewentualnie przeprowadzić ww. „atak").

46 B. Sanak, T. Kurowski, op.cit.

47 *Economic majority*, Wikipedia, https://en.bitcoin.it/wiki/Economic_majority; https://en.bitcoin.it/wiki/Bitcoin_is_not_ruled_by_miners [dostęp:16.10.2017].

*Wykres 4 Rozkład mocy największych kopalni bitcoinów*

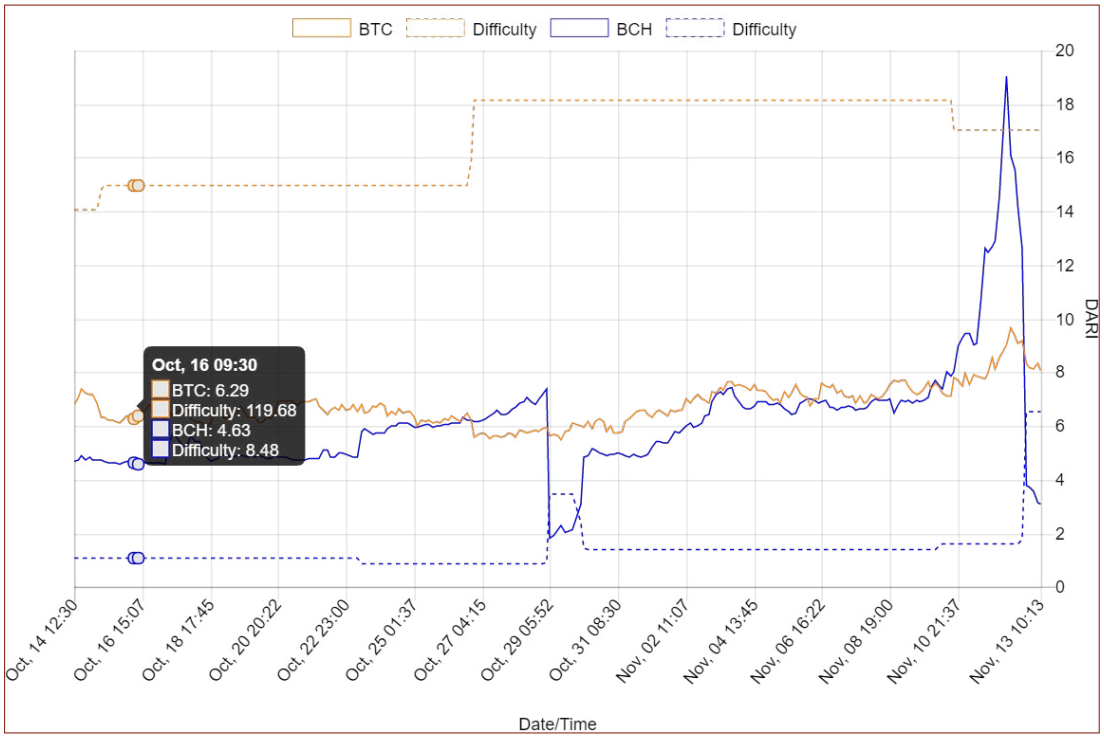



*Źródło: blockchain.info [dostęp: 13 listopada 2017 r.]*

Koncepcja ta przez długi czas wydawała się teoretyczną. Sytuacja zmieniła się, gdy pojawił się dla Bitcoina realny konkurent – Bitcoin Cash. Odpowiadał on w większej mierze na potrzeby użytkowników, niż utrzymanie statusu quo, który wspierali „górnicy". Gdy okazało się, że zapowiadane od długiego czasu i negocjowane od ponad dwóch lat zmiany w protokole Bitcoina (SegWit2x) zapowiedziane na 16 listopada 2017 r. jednak nie dojdą do skutku, w konsekwencji część społeczności ogłosiła wsparcie dla bezpośredniego konkurenta Bitcoina, tj. dla Bitcoin Casha. Efektem tego był nagły wzrost kursu tegoż ostatniego, kosztem dotychczasowego Bitcoina. Co więcej, do tak zdefiniowanej „większości ekonomicznej" (tu: do oczekiwań użytkowników Bitcoina narzekających na przepełnienie bloków oraz wysokie koszty transakcyjne) szybko przyłączyli się sami „górnicy", którzy szybko policzyli, że bardziej opłacalne jest dla nich „kopanie" bitcoinów cash. Na szczęście dla „głównego" bitcoina, wraz ze spadkiem ceny jego rozgałęzienia (ang. *fork*)[48] jego atrakcyjność ekonomiczna dla „górników" również zmalała.

48 E. Lendzion-Stachera, *Rozłamy*..., op. cit.

*Wykres 5 Porównanie zyskowności „kopania" bitcoinów i bitcoinów cash bazujące na opłatach, kursach wymiany i trudności kopania*




*Źródło: www.fork.lol [dostęp: 13 listopada 2017 r.]*

## 2.5. Kryptografia kryptowalut

Istotnym elementem funkcjonowania kryptowalut jest zabezpieczenie sieci przed próbami oszustwa. Kryptografia jest to praktyka i badanie technik bezpiecznej komunikacji w obecności osób trzecich. Oparta jest na teorii matematyki i informatyce. Jej celem jest skuteczne przechowanie lub przekazanie poufnej informacji w sposób bezpieczny i tajny, uniemożliwiając tym samym naruszenie jawności, integralności i niezaprzeczalności danych przez osoby trzecie. Jednymi z najbardziej znanych polskich kryptologów były osoby zajmujące się łamaniem szyfrów Enigmy.

Z zagadnieniem kryptowalut związane są pojęcia kryptografii symetrycznej i asymetrycznej.

- Kryptografia symetryczna polega na użyciu tego samego klucza do zaszyfrowania danych, jak i ich odszyfrowania. Jej wadą jest kwestia bezpieczeństwa klucza, który jest narażony na zwiększone ryzyko, ponieważ znają go obie strony. W przypadku, gdy taki klucz wpadnie w niepowołane ręce, może to doprowadzić nie tylko do rozszyfrowania tajnej wiadomości, ale również do wysłania fałszywej.
- Kryptografia asymetryczna klucza publicznego polega natomiast na tym, iż występują dwa klucze: publiczny (jawny) i prywatny (tajny). Zależnie od tego, w jakim celu planujemy użyć tej metody: podpis cyfrowy, czy szyfrowanie – występują pewne różnice. Za pomocą

otwartego oraz prywatnego klucza można przekazywać dane online. Jeżeli chcemy wysłać komuś wiadomość, to bierzemy jego publiczny klucz, który jest publicznie znany (w tym dla oszustów) szyfrujemy nim dane. Natomiast te dane można deszyfrować tylko prywatnym kluczem, który zna tylko i wyłącznie adresat wiadomości[49].

Co do kwestii cyfrowego podpisu my posiadamy klucz prywatny, którego używamy w celu zaszyfrowania, „podpisania" dokumentu. Natomiast klucz publiczny służy w celu zweryfikowania naszej tożsamości, na przykład przez bank (tylko my posiadamy klucz prywatny jest on powiązany z nami i świadczy o naszej tożsamości). Natomiast w celu szyfrowania danych używamy ogólnodostępnego klucza publicznego, a klucz prywatny, za którego pomocą będzie możliwe odszyfrowanie dokumentu, posiada adresat[50].

Wydajny system kryptograficzny to podstawa działania kryptowalut. Jest on jednocześnie gwarantem bezpieczeństwa. Kryptografia kryjąca się za takimi kryptowalutami jak bitcoin jest praktycznie nie do złamania biorąc pod uwagę zaangażowaną w ochronę tego systemu moc obliczeniową. Może się to zmienić po wprowadzeniu komputerów kwantowych, ale również i wtedy nie będzie to zadanie proste[51]. Techniki kryptograficzne zabezpieczają przed manipulacją oraz próbą naruszenia integralności baz danych[52].

Aby w pełni zrozumieć bezpieczeństwo i poprawność transakcji zapewnianych przez technologie typu blockchain należy również zapoznać się z działaniem kryptografii klucza publicznego oraz tzw. funkcji skrótu.

Wiele innych jeszcze pojęć zostało zebranych i w skrócie opisanych np. w udostępnianym przez Ministerstwo Cyfryzacji „Leksykonie pojęć"[53].

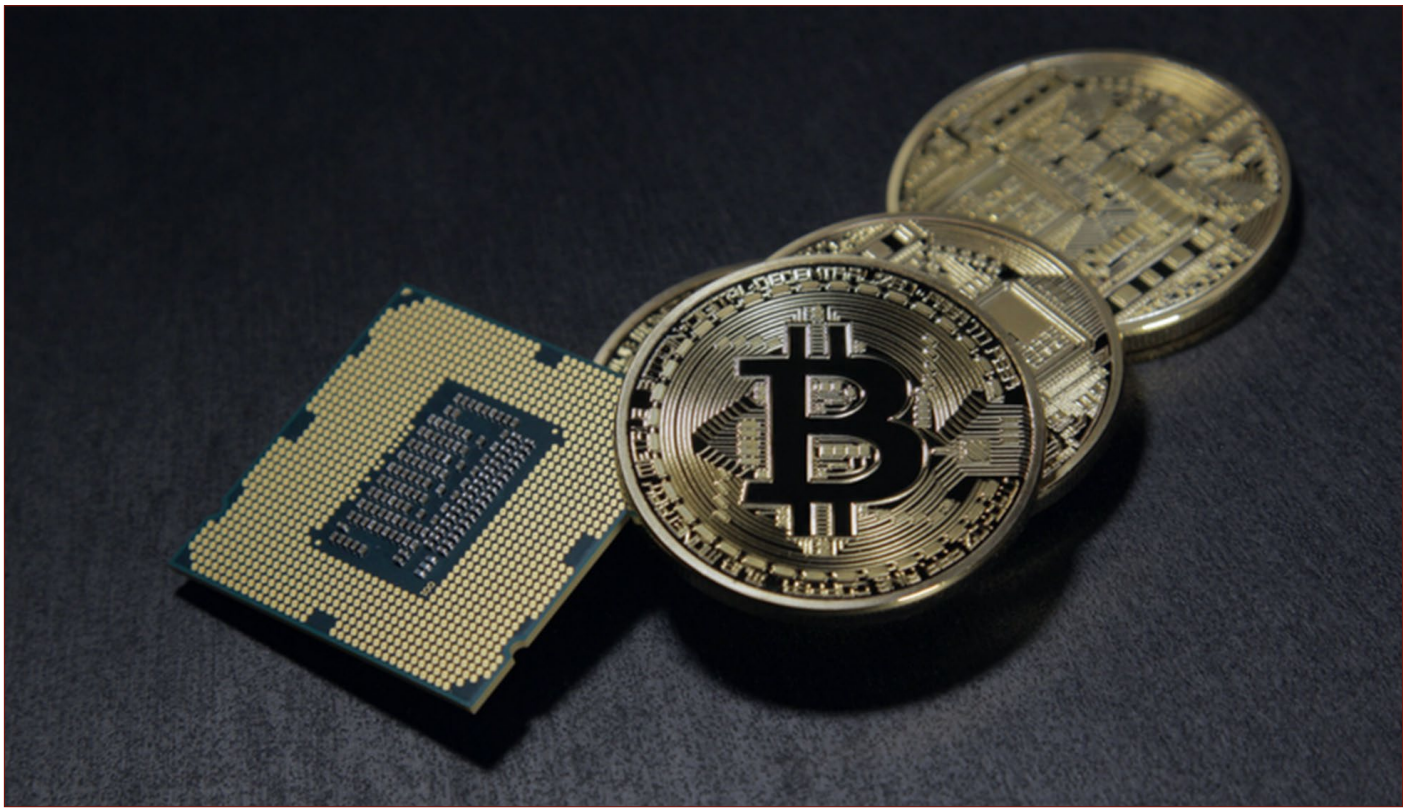
49 M. Olszański, K. Piech (red.), *E-biznes – innowacje w usługach. Teoria, praktyka, przykłady*, PARP, Warszawa 2012 (też: https://www.parp.gov.pl/images/PARP_publications/pdf/20506.pdf).

50 *Matematyka kryjąca się za Bitcoin*, Krypto Polonia, 25 marca 2015 r., http://kryptopolonia.info/matematyka-kryjaca-sie-za-bitcoin [dostęp: 12 listopada 2017 r.].

51 Komputery kwantowe nie będą od razu dostosowane do tego typu obliczeń, które będą w stanie od razu drastycznie wpłynąć na kryptografię stojącą za kryptowalutami.

52 S. Lujan, *Is Bitcoin as Risk as Google and IBM Aim for 50-Qubit Quantum Computers?*, Bitcoin.com, 30 kwietnia 2017 r., https://news.bitcoin.com/is-bitcoin-at-risk-as-google-and-ibm-aim-for-50-qubit-quantum-computers [dostęp: 24 sierpnia 2017 r.].

53 K. Piech (red.), *Leksykon…*, op. cit., s. 13.



# 3. Emisja kryptowalut

## 3.1. Zakup urządzeń

Podstawowym sposobem pozyskiwania nowych kryptowalut jest ich „wydobycie". Uzyskuje się je w zamian za zaangażowanie mocy obliczeniowej, która jest potrzebna dla weryfikacji dokonywanych w danej kryptowalucie transakcji. Tak zwani „górnicy" to właśnie osoby, które zdecydowały dołączyć się do wybranej społeczności wirtualnej waluty od strony nieco bardziej technicznej. „Górnicy" spełniają kluczową rolę w podtrzymywaniu poprawności funkcjonowania danej waluty. Ich głównym zadaniem jest wspólne tworzenie i utrzymywanie danego blockchaina oraz osiąganie konsensusu.

Udostępnienie mocy obliczeniowej (w przypadku PoW, a w przypadku innych metod konsensusu – np. przestrzeni dyskowej) wiąże się przede wszystkim z pozyskiwaniem nowo wyemitowanych jednostek waluty w przypadku udziału w rozwiązaniu celowo wbudowanych w system „zagadek matematycznych" oraz z otrzymywaniem wynagrodzenia w postaci opłat transakcyjnych.

Te odgórne warunki ustanawiane są przez twórców waluty jeszcze przed pierwszą emisją i służą automatycznej regulacji ilości emitowanych monet. Zatem, im więcej osób chce brać udział w procesie potwierdzania transakcji, tym bardziej zwiększa się trudność „zagadki

matematycznej", którą w przypadku Bitcoina jest otrzymanie wyniku funkcji skrótu o określonych parametrach. Regulacja poziomu trudności skutkuje stabilizacją tempa emisji waluty na zamierzonym poziomie.

Warto przy tym zaznaczyć, iż osoby decydujące się na zakup sprzętu służącego do potwierdzania transakcji (tzw. koparek) muszą liczyć się z ryzykiem braku opłacalności podjętego przedsięwzięcia. Jak wspomniano powyżej, zmianie ulega trudność „zagadki matematycznej", ale także kurs emitowanej kryptowaluty oraz łączna wartość prowizji uzyskanych za aktualizację Blockchain. Są to czynniki niezależne od pojedynczych „górników". Muszą oni brać je pod uwagę kalkulując opłacalność inwestowania w „kopanie".

Poniżej zestawiono kwestie, które należy wziąć pod uwagę, jeżeli ktoś chciałby zaangażować się w działalność związaną z wydobywaniem kryptowalut:

1. Koszty początkowe i koszty stałe wydobywania:
- Do ceny urządzenia oferowanego przez zagranicznych producentów należy doliczyć koszt transportu oraz podatki związane z zakupem (cło, VAT).
- Część oferowanych urządzeń nie posiada wbudowanych zasilaczy. Zatem należy sprawdzić parametry potrzebnego zasilacza i doliczyć jego cenę do kosztów początkowych. Należy zwrócić uwagę m.in. na moc zasilacza, gdyż te używane do zwykłych komputerów stacjonarnych, mogą nie być wystarczające.
- Szacowanie kosztów poboru prądu należy przeprowadzić na podstawie analizy umowy z dostawcą energii. Warto zwrócić uwagę na to, iż „koparki" pracują przez całą dobę, a niektóre umowy zawierają zróżnicowanie stawki w zależności od pory dnia.
- Rozbudowane zestawy urządzeń potrzebują zazwyczaj dodatkowego chłodzenia (np. kilka kart graficznych podłączonych do jednej płyty głównej), co dodatkowo zwiększa koszty potrzebnej w tym celu energii elektrycznej.
- Koszt komputerów kupowanych za granicą podawany jest w walucie obcej (lub – niekiedy – w bitcoinach). Od zapowiedzi urządzenia do sprzedaży pierwszej partii zwykle mija kilka miesięcy. W tym czasie może zmienić się kurs walutowy (złotego do dolara).

2. Analiza opłacalności:
- Do analizy opłacalności „kopania" można użyć kalkulatorów dostępnych online. Niekiedy zakłada się w nich stałość parametrów, które w rzeczywistości ulegają zmianie.
- Trudność „kopania" co do zasady w praktycznie każdej popularnej kryptowalucie wzrasta. Warto poszukać kalkulatorów uwzględniających procentowy przyrost trudności i na podstawie danych historycznych wyliczyć średnią stopę przyrostu (nie musi on być jednak liniowy).
- Ze względu na dużą ilość zamówień, odległość, formalności importowe, faktyczny czas dostawy może przerosnąć nasze oczekiwania, a trudność „kopania" w sytuacji wprowadzania na rynek urządzeń nowej generacji zazwyczaj rośnie skokowo.
- Dosyć oczywistą kwestią jest również zmienność kursów kryptowalut. Wartość kryptowalut, które nie są wymieniane bezpośrednio na polski złoty w dużej mierze zależy od kursu PLN/USD.

- Kupując dedykowane urządzenia nie musimy martwić się o ustawienie jego parametrów wydajnościowych. Jeżeli jednak mamy w planach „kopanie" kryptowalut za pomocą kart graficznych należy wziąć pod uwagę to, iż ich moc obliczeniowa i pobór prądu zależeć będą od konfiguracji ustawień.
- Konfiguracje można znaleźć w Internecie, ale niekiedy przy tych samych ustawieniach osiągamy inne wyniki. Może to być spowodowane wieloma czynnikami (sterowniki, system operacyjny itp.).
- W analizie opłacalności warto wyliczyć i wziąć pod uwagę przedział bezpieczeństwa planowanej inwestycji (obliczenie minimalnego opłacalnego kursu i maksymalnej trudności, zestawienie różnych wariantów itp.). Analizę opłacalności warto powtórzyć na moment zakupu.

3. Porady o charakterze ogólnym:

- Sprzęt zaangażowany do wydobywania kryptowalut generuje wysoki poziom hałasu oraz bardzo szybko nagrzewa pomieszczenia – należy zadbać o prawidłową wentylację (choć są już sposoby odzyskiwania ciepła np. do podgrzewania wody w instalacjach centralnego ogrzewania). Warto wziąć również pod uwagę wilgotność powietrza, która może działać niekorzystnie na poszczególne podzespoły.
- W celu lepszej ochrony naszego zestawu warto zaopatrzyć się w listwę antyprzepięciową.
- Kupowanie urządzeń o wielu zastosowaniach wiąże się z mniejszym ryzykiem znacznej utraty wartości. Urządzenia, które dają „urobek" niższy od kosztów potrzebnego do tego prądu, skupowane są jedynie przez osoby dysponujące „darmową" energią lub jeśli są zbyt stare – mogą być niesprzedawalne (z ostatniego powodu „kopanie" na kartach graficznych obarczone jest mniejszym ryzykiem).
- W popularnych serwisach aukcyjnych pojawiają się oferty zakupu urządzeń przed oficjalną datą wydania pierwszej partii. Należy zapoznać się ze szczegółami licytacji, istnieje bowiem ryzyko wysyłki ze znacznym opóźnieniem.
- Przed zakupem jakiejkolwiek komputera dedykowanego do „kopania" kryptowalut należy wnikliwie sprawdzić reputację producenta oraz komentarze dotyczące samej technologii. Niekiedy bowiem zdarzało się, iż nawet najwięksi producenci mają problemy z ukończeniem urządzeń na czas, a przedsprzedaż jest jedynie sposobem na poprawę kondycji finansowej spółki.
- Dodatkowo, w celu zabezpieczenia się przed ewentualnymi stratami związanymi z ryzykiem awarii lub „spalenia się" sprzętu warto zainwestować w dodatkowe ubezpieczenie, które pozwoli nam na odzyskanie części strat.
- Podobnie, dobrze jest dysponować minimum dwoma, niezależnymi źródłami internetu, na wypadek gdyby jedno z połączeń nie działało.

Przedsięwzięcia nazywane „kopalniami" łączą moc obliczeniową wielu komputerów indywidualnych osób we wspólne „pools" (spółdzielnie), przez co prawdopodobieństwo rozwiązania „zagadki" przez daną grupę zwiększa się, a przychody stają się bardziej regularne. Nagroda za każdy rozwiązany blok jest dzielona na wszystkich zaangażowanych z uwzględnieniem udostępnionej przez poszczególnych „górników" mocy obliczeniowej.

## 3.2. Zakup mocy obliczeniowej

Drugą możliwością pozyskiwania nowych jednostek kryptowalut za wydobywanie jest „kopanie" w chmurze. Sposób ten polega na zakupie praw do określonej wartości mocy obliczeniowej. Firmy oferujące tego typu usługi zazwyczaj hurtowo kupują urządzenia dedykowane do potwierdzania transakcji kryptowalutowych po znacznie niższych cenach. Z uwagi na skalę i rodzaj przedsięwzięcia, co do zasady cena jednostkowa prądu jest również niższa w porównaniu do stawek oferowanych gospodarstwom domowym.

Zasada działania typowej „chmury" (z ang. cloud) polega na tym, iż spółka oferuje jednostkę mocy obliczeniowej za określoną cenę, do której należy doliczyć koszty utrzymania (prąd i konserwacja). Po zakupie w regularnych odstępach czasowych (np. jeden dzień) otrzymujemy „urobek" zakupionej mocy obliczeniowej pomniejszony o wymienione koszty. Przesyłanie należnych nam jednostek kryptowaluty trwa do momentu przekroczenia punktu opłacalności. Niektóre serwisy oferują odsprzedanie mocy obliczeniowej na wewnętrznej giełdzie. Jeżeli moc obliczeniowa przywiązana jest do konkretnych komputerów handel mocą obliczeniową nie jest przeważnie możliwy. Tak samo jak w klasycznym wydobywaniu, tak i tutaj występują ryzyka związane ze zmiennością „środowiska kryptowalut" (tj. trudność wydobycia, kurs, wartość opłat transakcyjnych).

Jednak ważniejszą od zmienności „środowiska" jest wiarygodność sprzedawcy mocy obliczeniowej. Nowopowstałe firmy udostępniające za opłatą moc obliczeniową często okazywały się piramidami finansowymi. Co jakiś czas w Internecie pojawiają się spółki oferujące moc obliczeniową po okazyjnych cenach. Często takie podmioty dla uwiarygodnienia swojego istnienia udostępniają na swoich stronach zdjęcia sprzętu (niekiedy nie własnego), wyciągi z rejestrów sądowych itp. Nawet to nie daje stuprocentowej pewności, że dane przedsięwzięcie nie jest oszustwem. Z poziomu domowego biurka nie ma skutecznej metody upewnienia się, czy firma np. z Islandii rzeczywiście zakupiła sprzęt obliczeniowy oraz czy to, co przedstawia na zdjęciach odpowiada stanowi faktycznemu.

Stawiając na „kopanie" w chmurze należy kierować się tym, jak długo dana spółka działa na rynku oraz jakie są na jej temat komentarze. Warto jest również szukać ofert zakupu mocy obliczeniowej całej maszyny z możliwością podłączenia pod dowolny serwer zrzeszających kopiących (usługa „hosted mining").

Oprócz ryzyka, kopanie w chmurze niesie ze sobą również wiele zalet, takich jak: brak hałasu i nadmiernego nagrzewania się pomieszczeń, brak odpowiedzialności za awarie sprzętu, automatyczna instalacja itp.

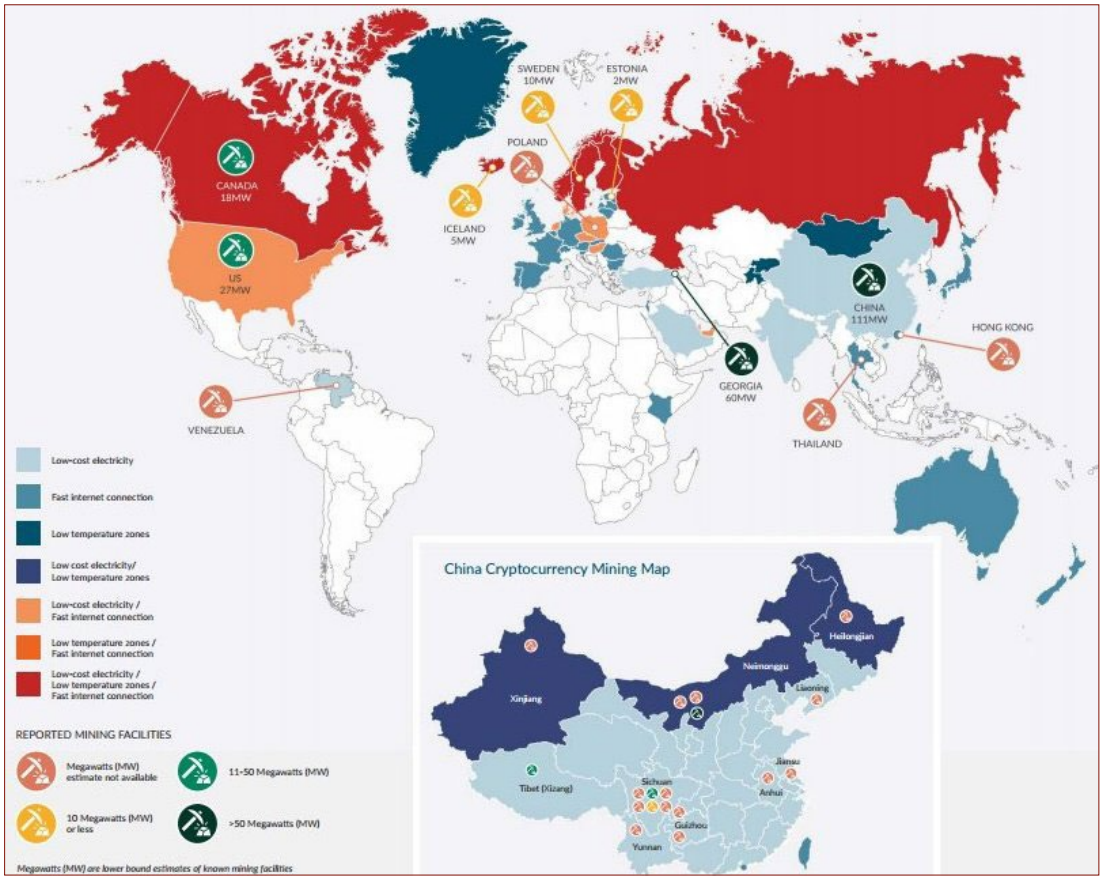
## 3.3. Kopanie kryptowalut w Polsce

Zarówno kiedyś, gdy do opłacalnego potwierdzania transakcji w systemie Bitcoin wystarczał zwykły domowy komputer, tak i teraz, gdy rolę tę przejęły dedykowane urządzenia lub chmury

obliczeniowe, śmiało można przedstawić Polskę jako pioniera w tej dziedzinie. Mowa tu nie tylko o start-upach technologicznych, ale przede wszystkim o zainteresowaniu i zrozumieniu tej dość zawiłej w szczegółach technologii przez rzeszę indywidualnych osób. Dowodem na potwierdzenie tej tezy może być fakt, iż w 2014 r. polska „kopalnia" zajmowała piątą pozycję na świecie pod względem wartości mocy obliczeniowej.

Pod względem mocy obliczeniowej wykorzystywanej w „kopaniu" bitcoinów, po bardzo dobrym początku udział Polski w światowym ich „urobku" systematycznie spada, choć nadal jest wysoki. Pod tym względem Polska może być nadal na ok. 4-5 miejscu na świecie. Spółdzielnie górnicze (*mining pools*) pochodzą głównie z Chin (58%) oraz z USA (16%)[54].

*Rozkład geograficzny największych kopalni bitcoinów na świecie*




*Źródło: G. Gileman, M. Rauchs, Global cryptocurrency benchmarking study, Cambridge University, 2017, s. 94.*

Po bardzo dobrym wejściu Polski na światowe rynki kryptowalutowe, przez długi czas niejasne były w naszym kraju zagadnienia podatkowe związane z obrotem kryptowalut. W szczególności, urzędy skarbowe narzuciły stawkę 23% na kryptowaluty (podczas gdy na podstawie tego samego prawa unijnego w Wielkiej Brytanii było to 0%). Dopiero po wyroku Europejskiego

54 G. Gileman, M. Rauchs, *Global cryptocurrency benchmarking study*, Cambridge University, 2017, s. 93.

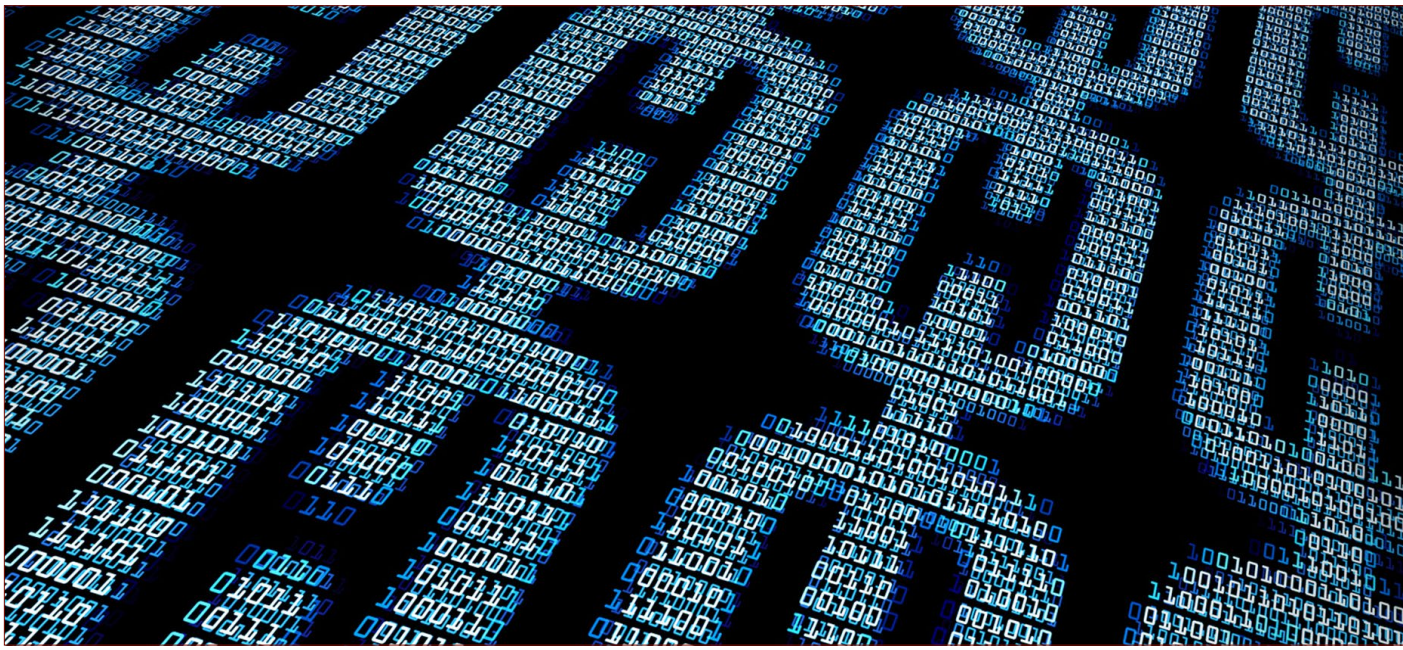
Trybunału Sprawiedliwości 22 października 2015 r. w Polsce, jak i w całej UE, transakcje wymiany walut konwencjonalnych na bitcoiny korzystają ze zwolnienia z podatku od towarów i usług [55]. Niektóre kraje, np. Gruzja a ostatnio również Rosja – otwarcie popierają „kopanie" kryptowalut i tworzą korzystne warunki dla jego rozwoju (nawet ułatwienia podatkowe). Są też kraje, które są zdecydowanie przeciwne (np. Wenezuela).

Większość polskich górników cyfrowych, działając prywatnie i na swój rachunek, woli nie ujawniać skali swojej działalności. Dostępne są jednak oferty niektórych firm. Przed skorzystaniem z nich warto sprawdzić u osób profesjonalnie zajmujących się kryptowalutami, czy dane przedsięwzięcie jest wiarygodne, czy też może być organizowane przez piramidy finansowe. W tym celu np. można:

- skontaktować się z Polskim Stowarzyszeniem Bitcoin,
- zadać pytanie na największym w kraju forum Bitcoin Polska w serwisie Facebook (ponad 22 tys. członków na początku listopada 2017 r.) lub
- samodzielnie sprawdzić w internecie np. wpisując daną nazwę i dodając słowo „scam" by sprawdzić, jak często pojawiały się w jego kontekście informacje o możliwym oszustwie.

Pojawiają się też międzynarodowe grupy przestępcze dysponujące sporym kapitałem i kancelariami prawnymi (grożące pozwami krytykującym je osobom). Część z nich sprzedaje „pakiety edukacyjne", które w przyszłości miałyby uprawniać posiadaczy do ich zamiany na kryptowalutę. Używają one bardzo dobrze zorganizowanego marketingu, sprawdzonego w niejednym już schemacie oszukańczym, zaś – z racji posiadanego doświadczenia – ich twórcy na ogół pozostają na wolności, tworząc kolejne, bardziej zaawansowane piramidy finansowe.

55 Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 22 października 2015 r. w sprawie wspólnego systemu podatku od wartości dodanej (VAT), dotyczący odpłatnego świadczenia usług – Transakcje wymiany wirtualnej waluty „bitcoin" na waluty tradycyjne, w sprawie Skatteverket przeciwko Davidowi Hedqvistowi, http://curia.europa.eu/juris/document/document.jsf?text=&docid=170305&pageIndex=0&doclang=PL&mode=req&dir=&occ=first&part=1&cid=757455.



# 4. Nabywanie i przechowywanie kryptowalut

Innym niż wydobywanie i w praktyce najczęstszym sposobem pozyskania kryptowalut jest ich zakup na rynku wtórnym.

### *Lista 10 najpopularniejszych walut cyfrowych*

| # | Name | Market Cap | Price | Volume (24h) | Circulating Supply | Change (24h) | Price Graph (7d) |
|---|---|---|---|---|---|---|---|
| 1 | Bitcoin | $118 403 176 704 | $7103.50 | $2 822 330 000 | 16 668 287 BTC | -3.88% | |
| 2 | Ethereum | $28 262 851 357 | $295.70 | $574 076 000 | 95 578 507 ETH | -2.45% | |
| 3 | Bitcoin Cash | $10 206 117 093 | $608.65 | $528 798 000 | 16 768 450 BCH | -3.47% | |
| 4 | Ripple | $8 013 827 997 | $0.207981 | $108 649 000 | 38 531 538 922 XRP * | 0.44% | |
| 5 | Litecoin | $3 117 941 089 | $58.04 | $203 706 000 | 53 718 057 LTC | 3.93% | |
| 6 | Dash | $2 224 510 454 | $289.87 | $95 368 200 | 7 674 139 DASH | 4.74% | |
| 7 | NEO | $1 685 931 000 | $25.94 | $41 123 300 | 65 000 000 NEO * | -2.08% | |
| 8 | NEM | $1 632 906 000 | $0.181434 | $5 751 390 | 8 999 999 999 XEM * | -2.33% | |
| 9 | Monero | $1 470 517 809 | $95.98 | $120 272 000 | 15 321 006 XMR | 5.82% | |
| 10 | Ethereum Classic | $1 382 100 435 | $14.22 | $200 753 000 | 97 211 214 ETC | -5.62% | |

*Źródło: https://coinmarketcap.com [dostęp: 8 listopada 2017 r.]*

## 4.1. Metody nabywania kryptowalut

Wyróżnia się trzy główne metody zakupu kryptowalut.

1. Podstawową i jedną z pierwszych z nich było zakupienie kryptowaluty od innego użytkownika. Metoda ta jednak rodziła pewne problemy. Przede wszystkim trudne było znalezienie osoby chętnej na wymianę kryptowaluty. Kolejnym problemem była niepewność, czy po dokonaniu przez nas zapłaty otrzymamy kryptowalutę od użytkownika. Na dzień dzisiejszy istnieją strony internetowe, na przykład **LocalBitcoins**, które w pewnym stopniu rozwiązują te problemy. Strony te świadczą usługi, dzięki którym można łatwo znaleźć osoby chętne do wymiany kryptowalut na pieniądze, najczęściej w formie gotówki. Ostatecznie jednak nie zaleca się korzystania ze stron tego typu, ze względu na ewentualne ryzyko oszustwa i braku pewności co do legalności pochodzenia środków. Ponadto, w przeciwieństwie do giełd i kantorów (por. niżej), często nie jest przeprowadzana weryfikacja tożsamości, a przez to stosowane przez sprzedawców marże są wysokie (sięgają nawet 10%). Nie zalecamy więc tej formy.
2. Kolejną metodą zakupu kryptowalut jest zakup w **kantorach** kryptowalutowych, tj. od przedsiębiorstwa specjalizującego się w wymianie walut. Kantory oferują szybki zakup walut cyfrowych, mają niekiedy biura dostępne dla osób „z ulicy", lecz niestety często z dodatkowo naliczoną marżą uwzględniającą koszty prowadzenia lokalu i zatrudnienia pracowników. Można jednak liczyć w nich na bezpłatne doradztwo, na edukację w zakresie kryptowalut. Niekiedy weryfikacja tożsamości nie jest tak rygorystyczna, jak w przypadku większości polskich giełd kryptowalutowych.
3. Inną możliwością jest wykorzystanie bankomatów bitcoinowych (w Polsce przyjęła się krótsza nazwa zaproponowana przez Sylwestra Suszka, tj. bitomat). Jednakże w naszym kraju forma ta nie przyjęła się, ze względu m.in. na wysoki udział operacji bezgotówkowych w naszym społeczeństwie – w przeciwieństwie przykładowo do USA, gdzie bitomatów jest ponad tysiąc, a w Polsce jedynie cztery (na początku listopada 2017 r.)[56].
4. Najbardziej popularną metodą są **giełdy** kryptowalut, na których ceny zakupu i sprzedaży są ustalane przez wolny rynek. Aktualnie występuje ponad 1000 kryptowalut, a ich liczba stale rośnie. Stroną internetową, która wymienia najbardziej popularne z nich, jest Coin Market Cap[57] (jej popularność na początku sierpnia 2017 r. stała się nawet wyższa, niż The Wall Street Journal). Jeśli jakiejś waluty cyfrowej nie ma w tym spisie oznacza to, że albo jest to piramida finansowa podszywająca się pod kryptowalutę, albo że jeszcze nie została ona w nim umieszczona (gdyż np. trwa jeszcze ICO – por. dalej) lub że jej obroty / kapitalizacja są zbyt niskie by zyskały uwagę redaktorów serwisu. Warto zaznaczyć, iż to, że gdy jakaś kryptowaluta znajduje się na stronie coinmarketcap - to wcale nie oznacza, że nie może być ona również piramidą finansową. Zawsze przed zainwestowaniem środków w daną kryptowalutę, należy przeprowadzić jej dogłębną analizę pod kątem ewentualnej próby oszustwa.

56 W burgerowni Bobby Burger obok Złotych Tarasów w Warszawie, w restauracji nepalskiej Siddhartha w Warszawie, w galerii Zielone Arkady w Bydgoszczy, w restauracji sushi w pobliżu biura BitBay w Katowicach.

57 www.coinmarketcap.com.

Występują giełdy umożliwiające wymianę pieniądza fiducjarnego (ang. *fiat money*) na kryptowaluty oraz takie, które tylko dają możliwość wymiany jednej kryptowaluty na inną. Najpopularniejszą giełdą na świecie jest założona w Stanach Zjednoczonych giełda Bitfinex, Bitstamp, Poloniex oraz Kraken[58]. Natomiast największymi giełdami działającymi na polskim rynku są BitBay, BitMarket, BitMarket24 a także serwis InPay[59]. Jest też kilka innych serwisów[60]. Te, które zdecydowały się poddać środowiskowej samoregulacji (w formie tzw. „Kanonu Dobrych Praktyk dla giełd kryptowalutowych" – jeden z pierwszych na świecie), co zostało potwierdzone wydaniem odpowiedniego certyfikatu sygnowanego przez Ministerstwo Cyfryzacji i Polskie Stowarzyszenie Bitcoin, wymienione są na stronie Ministerstwa[61].

Zalecane jest korzystanie z tych giełd, które posiadają renomę oraz funkcjonują od dłuższego okresu, aby uniknąć ewentualnych problemów prawnych i próby oszustwa ze strony giełdy. Nie gwarantuje to jednak 100-procentowego bezpieczeństwa. Znany jest przypadek funkcjonującej od 2012 roku, najstarszej, działającej wówczas polskiej giełdy kryptowalutowej – Bitcurex, która pod koniec 2016 roku nagle, bez ostrzeżenia zawiesiła swoją działalność. Giełda ta posiadała nawet certyfikat *compliance* wystawiony przez jedną z firm, potwierdzających jej zgodną z prawem działalność. W efekcie poszkodowani zostali użytkownicy tej giełdy – niektórzy stracili kwoty nawet kilkudziesięciu tysięcy złotych. W skali całego rynku nie była to duża strata: „suma zdeponowanych środków na giełdzie Bitcurex to tylko kilka procent (ok. 3-5%) wszystkich środków (kryptowalutowych i fiducjarnych) utrzymywanych łącznie na polskich giełdach"[62]. Właściciele Bitcurexa poinformowali, że utracili pieniądze w związku z atakiem hakerskim na konta giełdy. Wciąż jednak nie ma pewności czy rzeczywiście doszło do ataku hakerskiego, czy może do defraudacji, szczególnie z tego powodu, że użytkownicy utracili nie tylko kryptowaluty, ale również złotówki, które były zdeponowane na rachunkach bankowych. Trwa postępowanie prokuratorskie w tej sprawie.

Aktualnie są prowadzone różne działania, takie jak powstanie „Kanonu dobrych praktyk"[63], które mają na celu to, aby przypadek Bitcurexa się nie powtórzył, zaś by funkcjonowanie giełd było bardziej przejrzyste, w pełni zgodne z całym polskim prawem oraz etyczne względem klientów.

58 R. Bielecki, *Analiza wybranych giełd kryptowalutowych na świecie*, Uczelnia Łazarskiego – Centrum Technologii Blockchain, http://www.lazarski.pl/pl/wydzialy-i-jednostki/instytuty/wydzial-ekonomii-i-zarzadzania/centrum-technologii-blockchain/analiza-wybranych-gield-kryptowalutowych-na-swiecie [dostęp: 24 sierpnia 2017 r.].

59 A. Adamowicz, M. Zacharski, *Analiza wybranych giełd kryptowalutowych w Polsce*, Uczelnia Łazarskiego – Centrum Technologii Blockchain, http://www.lazarski.pl/pl/wydzialy-i-jednostki/instytuty/wydzial-ekonomii-i-zarzadzania/centrum-technologii-blockchain/analiza-wybranych-gield-kryptowalutowych-w-polsce [dostęp: 24 sierpnia 2017 r.].

60 Część z giełd w skrócie jest opisanych w artykule: U. Azarko, U. Yakauleu, *Przegląd kilku wybranych giełd kryptowalutowych*, Uczelnia Łazarskiego – Centrum Technologii Blockchain, http://www.lazarski.pl/pl/wydzialy-i-jednostki/instytuty/wydzial-ekonomii-i-zarzadzania/centrum-technologii-blockchain/przeglad-kilku-wybranych-gield-kryptowalutowych [dostęp: 24 sierpnia 2017 r.].

61 Sygnatariusze „Kanonu dobrych praktyk podmiotów rynku kryptowalutowego w Polsce", Ministerstwo Cyfryzacji – Strumień „Blockchain / DLT i Waluty Cyfrowe", https://www.gov.pl/documents/31305/0/signatories_2.11.2017.pdf/ [dostęp: 12 listopada 2017 r.].

62 K. Piech, *O upadkach giełd bitcoinowych – ciąg dalszy*, http://piech.blog.pl/2016/10/25/o-upadkach-gield-bitcoinowych-ciag-dalszy [dostęp: 24 sierpnia 2017 r.].

63 K. Zacharzewski, K. Piech, L. Wilczyński (red.), *Kanon dobrych praktyk podmiotów rynku kryptowalutowego w Polsce*, Ministerstwo Cyfryzacji – Strumień „Blockchain / DLT i Waluty Cyfrowe", 10 kwietnia 2017 r., https://www.gov.pl/documents/31305/0/kanon_justowany.pdf/ [dostęp: 13 listopada 2017 r.].

## 4.2. Weryfikacja tożsamości klienta

**Przed zarejestrowaniem się na jakiejkolwiek giełdzie kryptowalutowej warto jest zapoznać się z jej regulaminem.** Wiele osób nie przywiązuje uwagi do tego wagi, aczkolwiek zrozumienie treści często jest w stanie oszczędzić niemiłych konsekwencji w przyszłości. Warto przynajmniej sprawdzić, czy w regulaminie jest wymieniony podmiot prawny, który reprezentuje dany serwis (wciąż można spotkać takie serwisy kryptowalutowe (choć coraz rzadziej – giełdy), które nie są prowadzone przez jakikolwiek, zarejestrowany gdziekolwiek podmiot prawny), a także w jakiej jurysdykcji jest umiejscowiony. Jeśli giełda operuje w USA, w UE czy innych, bardziej wiarygodnych krajach (np. Japonia, Australia) – potencjalne pole do oszustw jest mniejsze, aczkolwiek wciąż istnieje ryzyko. Jeśli przykładowo jest to Hongkong, koszty ewentualnego procesu sądowego prowadzonego z Polski mogą przewyższać ewentualną skalę strat wynikających z oszukańczej działalności władz giełdy.

Jedną z kluczowych kwestii poruszanych w regulaminach jest weryfikacja konta. Zgoda na nią stanowi warunek zarejestrowania się na wielu giełdach kryptowalutowych. W przeszłości, wiele giełd nie wymagało weryfikacji tożsamości klientów – dziś jest to coraz bardziej powszechne. Na niektórych giełdach procedury weryfikacji dokumentów są na tyle dokładne, że ich pracownicy są w stanie wychwycić fałszerstwa – nawet dokonane przez FBI[64].

W większości przypadków w UE weryfikacja jest wymagana, gdy wartość przekazanych środków przekracza 15 tys. euro rocznie[65]. Dotyczy to również przypadków, w których transakcja taka wykonywana jest za pomocą więcej niż jednej liczby operacji. Jest to konsekwencją unormowania przewidzianego w art. 8 Ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Niektóre giełdy zaostrzają ten obowiązek zapisując w regulaminach, że weryfikacja obowiązuje już przy niższych kwotach albo przy transakcjach na walutach konwencjonalnych. Często w regulaminach zastrzeżona jest także weryfikacja w razie wykonywania przez użytkownika operacji, które mogą zostać uznane za podejrzane. Taki użytkownik może zostać również zablokowany, a jego operacje mogą być wstrzymane do wyjaśnienia. Związane jest to z wewnętrznymi wymogami bezpieczeństwa poszczególnych giełd.

Giełdy wręcz prześcigają się w opracowywaniu nowych metod weryfikacji, aby zapewnić jak największe bezpieczeństwo transakcji. Do najpopularniejszych sposobów należą m.in.: przesyłanie skanów dokumentów tożsamości, selfie z dokumentem, wykonywanie przelewów uwierzytelniających czy nawet rozmowa przez Skype lub telefon. Możliwa jest również wysyłka listu na adres podany przy rejestracji, w którym to znajduje się kod odblokowujący konto.

64 P. Rizzo, *Federal Agents Face Arrest for Alleged Silk Road Bitcoin Theft*, CoinDesk, 30 marca 2015 r., https://www.coindesk.com/federal-agents-face-arrest-for-alleged-silk-road-bitcoin-theft/

65 *Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, Dz.U. 2000 Nr 116 poz. 1216.

Warto zaznaczyć, iż w przypadku, gdy giełda bądź inna instytucja wymaga od nas przesłania skanu jakiegokolwiek dokumentu potwierdzającego naszą tożsamość, to wskazane jest opatrzyć takowy skan w unikalny „watermark" – znak wodny z przykładowym dopiskiem „tylko do celów weryfikacji konta na portalu XXX". W przypadku „wycieku" dokumentów, użycie naszego skanu w nielegalny sposób będzie znacząco utrudnione.

Nawet jeśli nie jest to zbyt wygodne i zajmuje nieco czasu, to użytkownicy powinni unikać giełd, które nie przewidują weryfikacji. Inaczej może to oznaczać, że giełda może działać nielegalnie, co może skutkować utratą środków np. w przypadku zablokowania jej działalności przez odpowiednie służby, czy w przypadku braku podstaw do procesu sądowego.

## 4.3. Bezpieczeństwo na giełdach

Korzystając z giełd kryptowalutowych musimy pamiętać o zachowaniu ostrożności i zabezpieczeniu się przed ewentualnym niepożądanym dostępem osób trzecich do naszego konta. Dotyczy to zarówno hakerów, jak i osób, które znajdą się w posiadaniu należącego do nas komputera.

Warto zwrócić uwagę na trzy aspekty dotyczące bezpieczeństwa naszego konta na giełdzie kryptowalutowej:

1. Weryfikacja dwuczynnikowa (tzw. 2FA) – uwierzytelnienie dostępu do konta składające się z dwóch etapów: pierwszego, kiedy podajemy nazwę użytkownika i hasło, oraz drugiego, podczas którego podajemy kod, do którego dostęp mamy tylko my[66]. Kod ten możemy otrzymać ze specjalnej aplikacji, np. Google Authenticator. Innym, choć uważanym za mniej bezpiecznym, sposobem jest uzyskanie go przez SMSa lub maila. Uwierzytelnienie takie może dotyczyć nie tylko dostępu do konta, ale także wypłat kryptowalut i walut fiducjarnych poza giełdę czy zmiany danych logowania.
2. Przechowywanie haseł – powinniśmy unikać zapamiętywania haseł w przeglądarkach. Najlepiej gdybyśmy je zapamiętali, albo utrwalili w taki sposób, który zapewni nam pewność, że nikt nie zdobędzie do nich dostępu. Hasło do konta na giełdzie powinno różnić się od hasła do maila, który podaliśmy przy rejestracji.
3. Zabezpieczenie konta e-mail – warto byłoby, także w przypadku konta e-mail zastosować weryfikację dwuczynnikową, dodać numer telefonu dla weryfikacji oraz zastosować silne hasło. Należy też zadbać, aby komunikacja z serwerem dostawcy usług pocztowych była szyfrowana (np. z użyciem https). Warto też dbać o potwierdzanie tożsamości nadawcy przy wymianie korespondencji, wzajemnie sprawdzając podpisy cyfrowe (S/MIME lub OpenPGP) lub chociaż zakładając skrzynki pocztowe u dostawców stosujących technikę DMARC do weryfikacji nadawcy (np. Google, Onet).

66 S. Rosenblatt, J. Cipriani, *Two-factor authentication: What you need to know (FAQ)*, CNET, 15 czerwca 2015 r., https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/.

## 4.4. Rodzaje i charakterystyka portfeli kryptowalutowych

Zakupioną kryptowalutę należy zabezpieczyć. Jeśli nie zamierzamy nią aktywnie obracać, czyli jeśli chcemy np. przez kilka dni nie wykonywać za jej pomocą transakcji, to należy pamiętać o jednym z podstawowych „przykazań" inwestora kryptowalutowego:

**Nie trzymamy środków na giełdach kryptowalutowych!**

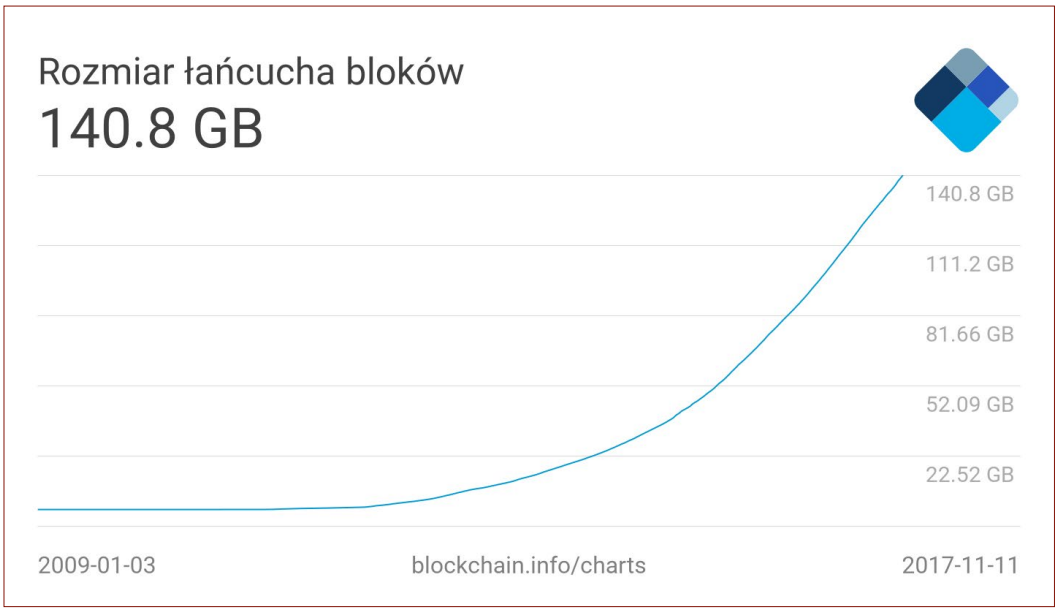
Na tyle dużo z nich już upadło, że praktyka pokazuje, że nie można z całkowitą pewnością stwierdzić, które z nich są w pełni bezpieczne. Nawet jeśli giełda jest zabezpieczona przed hakerami, zawsze pozostają inne ryzyka, np. tzw. man-in-the-middle attack lub zajęcie sprzętu przez organy ścigania.

Po dokonaniu wyboru kryptowaluty, jaką planujemy zakupić, następuje kolejny krok – wybór portfela kryptowalutowego. Kryptowaluty przechowuje się tak samo jak w przypadku pieniądza papierowego (banknotów i monet) w portfelu (ang. *wallet*) lub sejfie (ang. *vault*), tylko że w formie cyfrowej. Portfel jest to oprogramowanie lub urządzenie (choć nie zawsze), które przechowuje nasze prywatne i publiczne klucze oraz wchodzi w interakcje z różnymi bazami blockchain, umożliwiając użytkownikowi przesyłanie i otrzymywanie kryptowalut. Warto tu zaznaczyć, że portfel kryptowaluty (wbrew temu co sugeruje nazwa) nie przechowuje posiadanych przez nas środków, lecz klucz prywatny dający dostęp do nich; środki te przypisane są do naszego klucza w blockchainie. Portfele mogą występują w różnych formach. Różnią się one stopniem zabezpieczeń, funkcjonalnością, mobilnością, czasem synchronizacji z bazą danych oraz zużyciem zasobów (na przykład zajętym miejscem na dysku).

W przypadku kryptowaluty Bitcoin wyróżnia się następujące typy portfeli (podobnie jest również dla innych kryptowalut):

- **Portfele w postaci aplikacji na komputer (*software wallets*):** występują w formie pełnej i lekkiej. W pełnej – przechowują one całą bazę blockchain. Charakteryzują się długim czasem synchronizacji i bardzo dużym zapotrzebowaniem na przestrzeń dysku twardego, co spowodowane jest faktem, iż baza blockchaina bitcoinowego zajmuje ponad 140 GB. W formie lekkiej – baza blockchain przechowywana jest na serwerach, do których się łączymy.

*Wykres 6 Rozmiar blockchaina bitcoinowego od 2009 r.*




*Źródło: www.blockchain.info/pl/charts/blocks-size [dostęp: 14 listopada 2017 r.]*

Portfele w postaci aplikacji na komputer charakteryzują się bardzo niską mobilnością, ponieważ są przechowywane wyłącznie na naszym komputerze oraz są narażone na ataki hakerów, jeśli komputer jest podłączony do Internetu.

- **Portfele internetowe (online):** dostęp do nich jest zapewniony za pośrednictwem strony internetowej, dzięki której logujemy się do swojego portfela. Charakteryzują się one dużą mobilnością, ponieważ mamy do nich dostęp za pośrednictwem każdego urządzenia z dostępem do Internetu. Minusem portfeli internetowych jest jednak niski stopień zabezpieczeń, ponieważ nasze klucze są przechowywane na serwerach online. Tego typu portfele zaleca się jedynie do doraźnego użytkowania i do przechowywania małych kwot.
- **Portfele mobilne:** występują w formie aplikacji na telefony lub tablety. Aplikacje te często oferują mniej funkcji, niż ich komputerowi odpowiednicy, ale za to charakteryzują się bardzo dużą mobilnością, ponieważ każdy prawie zawsze ma przy sobie telefon komórkowy. Niektóre aplikacje w celu zwiększenia bezpieczeństwa korzystają z faktu, iż coraz więcej nowoczesnych telefonów wyposażonych jest w czytnik linii papilarnych i używają ich do logowania się do aplikacji. Kolejną zaletą portfeli mobilnych jest łatwość dokonywania płatności w sklepie lub w jakimkolwiek innym miejscu, gdzie akceptowane są kryptowaluty. Wystarczy zeskanować aparatem fotograficzny kod QR i dokonać transakcji. Jednak ryzyko zgubienia lub wykradzenia nam urządzenia mobilnego jest niewątpliwie większe aniżeli komputera stacjonarnego.
- **Portfele sprzętowe (*hardware wallets*):** jest to typ portfela, w którym klucze publiczne i prywatne przechowywane są na zewnętrznym dysku USB. Z powodu tego, że dysk jest offline (nie ma połączenia z Internetem) to w porównaniu do swoich poprzedników charakteryzuje się znacznie większym bezpieczeństwem. Gdy użytkownik chce wykonać

transakcję przy użyciu tego typu portfela wystarczy podłączyć dysk zawierający klucze do komputera lub telefonu (przy użyciu specjalnej przejściówki).

*Przykład portfela sprzętowego - Trezor*

*Źródło: trezor.io [31 sierpnia 2017 r.]*

- **Inne portfele fizyczne (papierowe, stalowe):** kategoria ta cechuje się największą różnorodnością. Portfel taki może przybrać postać wydrukowanego specjalnego dokumentu zawierającego klucze publiczne i prywatne lub adres prywatny. Inną wersją tego typu portfela jest polski produkt Cryptosteel i w porównaniu do papierowych wersji portfela jest on wykonany z nierdzewnej stali o bardzo dużej wytrzymałości, w której możemy umieścić dowolną kombinację znaków (kluczy prywatnych/publicznych lub haseł niezbędnych do odzyskania konta). Tego typu portfel jest zalecany jako długotrwała metoda przechowywania dużych wartości kryptowalut. Tego typu „lokatę długoterminową" można na przykład zakopać lub przechowywać w sejfie na tak zwaną „czarną godzinę".
- **Zapamiętywanie (brain wallet):** alternatywą do wymienionych wyżej portfeli jest nauczenie się kluczy na pamięć. Takie rozwiązanie uniezależnione jest od sprzętu i oprogramowania, zatem cechuje je najwyższy stopień bezpieczeństwa. Jedyne ryzyko, które występuje to sytuacja, w której klucz zostanie zapomniany przez użytkownika.

Niezależnie od wybranego typu portfela zdecydowanie zalecane jest stworzenie backupu, np. wygenerowanie specjalnych haseł w formie ciągu znaków. Backup ten umożliwi nam odtworzenie portfela wówczas, gdy z jakiegokolwiek powodu stracimy nasze urządzenie (np. padnie nam dysk, upuścimy telefon do wody lub urządzenie zostanie nam skradzione). W przypadku

niektórych aplikacji jedną z metod odzyskania konta są *mnemonic seed*, czyli ciąg od 12 do 24 losowych słów zapisanych po kolei, które należy zachować w bezpiecznym miejscu.

Posiadając jakikolwiek portfel kryptowalutowy, na przykład na swoim telefonie, należy pamiętać o tym, że wartość tego telefonu to już nie tylko jego cena rynkowa, ale także zawartość portfela. Dlatego należy zwiększyć naszą czujność i dołożyć wszelkich starań, aby nasze pieniądze były bezpieczne. Zabezpieczenie telefonu kodem odblokowującym go to absolutne minimum.

Warto pamiętać, że nie ma portfela, który daje 100% bezpieczeństwa przechowywanych środków, a jego bezpieczeństwo w dużym stopniu zależy od świadomości użytkownika. Portfel nie ma możliwości zapobiegania konsekwencjom nieostrożnych działań użytkownika.

W związku z odmiennymi cechami różnych typów portfeli kryptowalutowych w celu zwiększenia bezpieczeństwa naszych środków, zaleca się korzystanie z wielu portfeli. Przykładowo w celu długoterminowego przechowywania kryptowalut, a także do dużych kwot, zaleca się rozwiązania typu *hardware wallets* i metody offline, które następnie przechowamy w bezpiecznym miejscu (na przykład sejf). Natomiast do codziennych płatności wygodne jest przechowywanie kryptowalut za pomocą aplikacji na smartphonie, na przykład dodatkowo zabezpieczonej skanem linii papilarnych lub skanem twarzy / oka.

# 5. Ekonomiczno-finansowe aspekty kryptowalut

## 5.1. Bitcoin jako pieniądz

Kryptowaluty są nowym pojęciem. Sprawiają trudności w ich zrozumieniu wielu doświadczonym ekonomistom. Jedną z takich kontrowersji jest zaklasyfikowanie kryptowalut jako pieniądza.

Pieniądz spełnia następujące, podstawowe funkcje:

1. Jest **miernikiem wartości** – integruje system określania wartości różnych produktów i usług oraz umożliwia porównywanie różnych cen ze sobą.
2. Pełni funkcję **środka płatniczego**, za pomocą którego możemy płacić za konkretne dobro i realizować zobowiązania związane z zakupem dóbr i usług.
3. Jest **środkiem wymiany**, czyli pośredniczy w transakcjach, w których dochodzi do wymiany pieniądza na produkt lub usługę.
4. Umożliwia gromadzenie i przechowywanie majątku (oszczędności). Oznacza to, że pełni **funkcję tezauryzacyjną**[67].

67 P. Kowalewski, *Pieniądz i jego znaczenia*, Narodowy Bank Polski – Portal Wiedzy Ekonomicznej, https://www.nbportal.pl/wiedza/artykuly/pieniadz/pieniadz-i-jego-znaczenia [dostęp: 17 lipca 2017 r.].

W przeszłości pieniądz przybierał różne postaci np.: sól, muszelki, gliniane lub drewniane tabliczki, skóry, metale w formie sztabek, później monet, w końcu zapisany papier lub tworzywo sztuczne. Obecnie usankcjonowany przez prawo jest również tzw. pieniądz elektroniczny.

Bitcoin pełni następujące funkcje pieniądza:

1. Jest on miernikiem wartości – widać to szczególnie na rynku altcoinów, których wartości niekiedy nie są porównywane do dolara ze względu na brak takich rynków; dla niektórych z nich to bitcoin stał się podstawą do wycen. Ze względu na fakt, iż istnieje przynajmniej 10 000 punktów na świecie, gdzie można płacić bitcoinem, ceny oferowanych towarów bywają także w nim mierzone.
2. Bitcoin jest środkiem płatniczym zarówno w Polsce, Unii Europejskiej (Trybunał Sprawiedliwości Unii Europejskiej stwierdził, że „jedynym przeznaczeniem bitcoina jest funkcja środka płatniczego”[68]), jak i w niektórych krajach na świecie (Japonia).
3. Bitcoin jest środkiem wymiany i płatności – można za jego pomocą kupować towary i usługi oraz – jeśli obie strony się zgodzą – można nim zaspokajać zobowiązania.
4. Funkcję tezauryzacyjną w istocie Bitcoin także realizuje, gdyż umożliwia przechowanie wartości, choć jakość jej realizowania jest niższa niż w przypadku oficjalnych walut, co się wiąże z obciążeniem majątku utrzymywanego w bitcoinie ryzykiem spadku jego wartości. Pod tym względem bitcoina raczej można porównać do papierów wartościowych niż do walut. Jednakże biorąc pod uwagę rosnącą w długiej perspektywie kapitalizację bitcoina, możne go traktować jako środek długoterminowej tezauryzacji, który wspomniane ryzyko sowicie w historii wynagradzał.

*Wykres 7 Kapitalizacja bitcoina w ciągu ostatniego roku*


*Źródło: blockchain.info [dostęp: 13 listopada 2017 r.]*

68 Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 22 października 2015 r. C-264/14.

5. Kryptowaluty, jako że są zapisem cyfrowym, charakteryzują się dużą trwałością i poręcznością, ponieważ można je przechowywać na komputerze, telefonie komórkowym, a nawet w formie papierowej czy stalowej. Ponadto dzięki matematyce oraz kryptografii charakteryzują się bardzo wysokim stopniem zabezpieczania przed fałszerstwem. Inaczej niż w przypadku tradycyjnego pieniądza papierowego, zarówno wygenerowanie „fałszywej" kryptowaluty czy podwójne jej wydanie jest wysoce nieprawdopodobne.
6. Ponieważ kryptowaluty występują głównie w postaci cyfrowej możliwy jest ich podział na wiele mniejszych jednostek. W przypadku bitcoina i większości kryptowalut jest możliwość podziału aż na 100 milionów mniejszych jednostek (osiem miejsc po przecinku).

Bitcoin spełnia wszystkie funkcje pieniądza. Z ekonomicznego punktu widzenia zatem możemy mówić o nim jak o pieniądzu. Jednakże ze względu na swoje specyficzne cechy z prawnego (formalnego) punktu widzenia bitcoin jest surogatem pieniądza, czyli nieoficjalnym środkiem płatniczym. Analogiczny sposób wnioskowania można zaaplikować także do innych kryptowalut – o ile pełnią ekonomiczne funkcje pieniądza, o tyle można o nich również mówić jako o pieniądzach lub surogatach pieniężnych.

Poza tym, pieniądze spełniają również konkretne cechy:

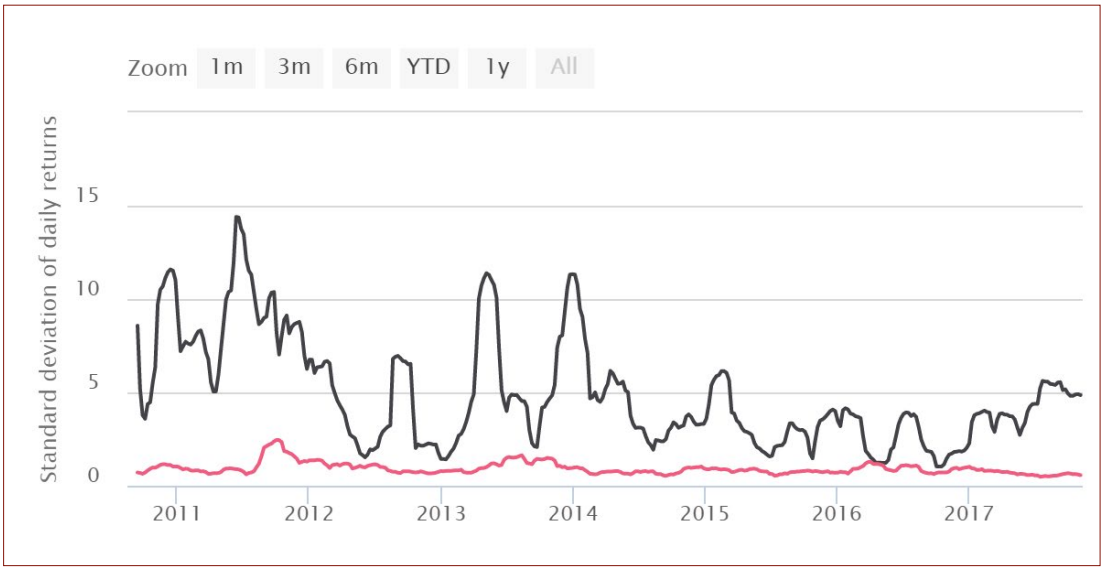
- **trwałość** – pieniądze muszą być wytrzymałe i odporne na uszkodzenia,
- **poręczność** – powinny gwarantować łatwość transportu i użytkowania,
- **oryginalność** – muszą dawać gwarancję wiarygodności i trudności fałszerstwa,
- **podzielność** – powinny posiadać możliwość podziału na mniejsze jednostki,
- **stabilność** – wartość siły nabywczej pieniądza powinna być stała w długim okresie,
- **powszechność** – muszą być powszechnie znane i łatwo rozpoznawalne[69].

Kwestia stabilności ceny kryptowalut często wzbudza kontrowersje. Kryptowaluty bowiem, charakteryzują się bardzo wysoką zmiennością cen względem walut oficjalnych (stąd powstały też takie[70], które są powiązane z ceną dolara amerykańskiego w stosunku 1:1). Bitcoin jest również kilka razy bardziej zmienny od złota.

69 *Cechy pieniądza*, Narodowy Bank Polski – Portal Wiedzy Ekonomicznej, https://www.nbportal.pl/wiedza/prezentacje/nowe-prezentacje/cechy-pieniadza [dostęp: 17 lipca 2017 r.].

70 Jest to np. Tether, https://tether.to [dostęp: października 2017 r.].

*Wykres 8 Zmienność kursu bitcoina oraz złota (odchylenie standardowe dziennych stóp zwrotu w 60-dniowym oknie)*




*Źródło: Bitcoin Volatility Time Series Charts, https://www.buybitcoinworldwide.com/volatility-index/ [dostęp: 13 listopada 2017 r.]*

Podobnie jak w przypadku tradycyjnego pieniądza, bitcoiny można pożyczać i otrzymywać z tego tytułu oprocentowanie. Istnieją już (nawet w Polsce) serwisy zajmujące się tym. Bitcoiny, jak i niektóre inne kryptowaluty mają odgórnie ustalone zasady (w tzw. white paper'ach) dotyczące ich podaży. Są tzw. dobrem rzadkim – ich podaż oraz jej zmiany są automatycznie regulowane przez algorytm zaimplementowany w aplikację służącą do wymiany monet i w przypadku większości kryptowalut ograniczona (np. Bitcoin) lub rośnie w zaprogramowanym wcześniej tempie (np. Ethereum). W przypadku oficjalnych walut niewiele jest takich, które są oficjalnie wykorzystywane w codziennej praktyce w więcej niż jednym kraju. Istnieje kilka globalnych walut rezerwowych, jednak są nimi zainteresowane głównie banki centralne. Kryptowaluty nie są prawie ograniczone geograficznie[71].

Niekiedy zadawane są pytania o „wewnętrzną", fundamentalną wartość bitcoina (ang. *intrinsic value*). W przypadku banknotów nie jest to „cena papieru", na którym są nadrukowane (zresztą często nie jest to papier, a tworzywo sztuczne), tylko decyzje władz monetarnych, które poprzez regulację ilości pieniądza banku centralnego (bilonu i banknotów) oraz politykę stopy procentowej (regulującą ilość pieniądza kreowanego w systemie bankowym) wpływają na wartość wymienną (siłę nabywczą) oficjalnego pieniądza. Jest to pieniądz oparty na zaufaniu do suwerena, iż zadba on o wartość tego pieniądza i jego stabilność.

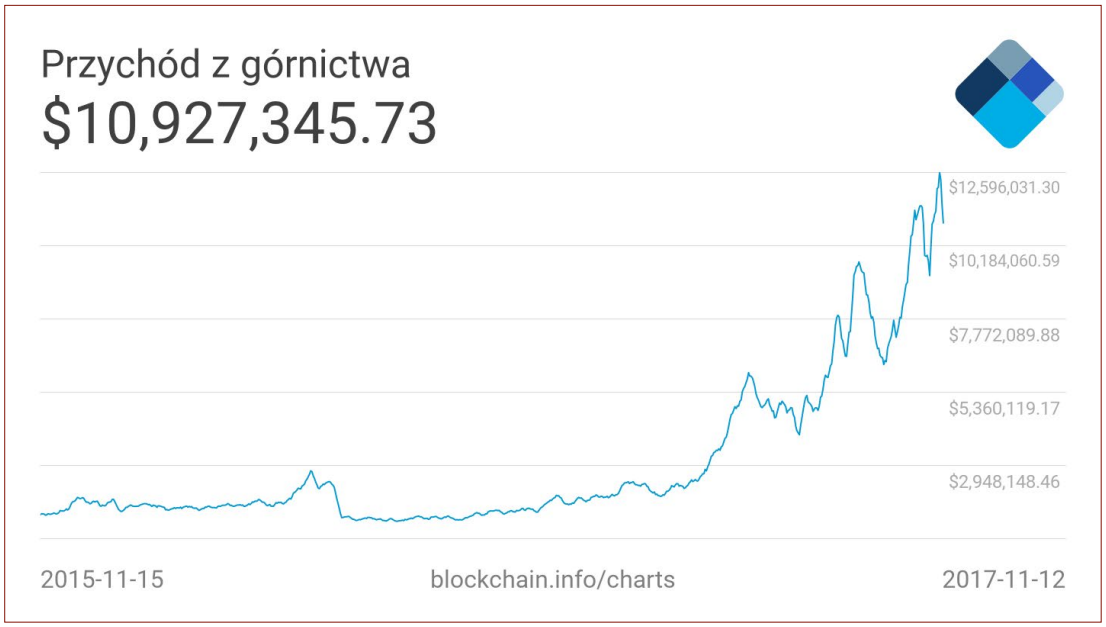
71 JaiChai, *Is Cryptocurrency Real Money? Brief Discussion on Major Issues Surrounding Debate*, Cointelegraph, 22 sierpnia 2017 r., https://cointelegraph.com/news/is-cryptocurrency-real-money-brief-discussion-on-major-issues-surrounding-debate.

Tymczasem cenę kryptowalut wyznacza rynek. Jego wartość fundamentalna może być wyznaczana na kilka sposobów, choć nie opracowano jeszcze kompleksowej metody wyceny tego, szczególnego waloru. Może być wyznaczana, tak jak wartość towarów – przez użyteczność, czyli oszacowanie stopnia zaspokojenia głównych jej aspektów, szczególnie stopnia realizacji funkcji pieniądza. Ze względu na brak metod bezpośredniej oceny stopnia realizacji funkcji pieniądza, należałoby wykorzystać czynniki pośrednio wpływające na użyteczność: stopień stabilności waluty oraz cen w niej wyrażonych, stopień powszechności akceptacji (liczba akceptantów), dostępną wartość dóbr do kupienia za kryptowaluty czy liczbę i nasilenie sygnałów rynkowych sugerujących rozwój lub potencjalne załamanie systemu (wzrost-aprecjację lub spadek-deprecjację wartości kryptowaluty).

Można do wyceny kryptowaluty także podejść jak do wyceny papierów wartościowych, tj. przez pryzmat dochodów jakie są w stanie wygenerować – biorąc pod uwagę (odrębnie) punkt widzenia kopalni, akceptanta, jak i inwestora-spekulanta[72]. W tym przypadku weźmie się pod uwagę zarówno:

- możliwości generowania przychodów (dla inwestora: wzrost ceny; dla akceptanta potencjalny wzrost przychodów w firmie; dla kopalni: wpływy z opłat systemowych) oraz

*Wykres 9 Całkowita, dzienna wartość przychodów z górnictwa bitcoina*




*Źródło: blockchain.info [dostęp: 13 listopada 2017 r.]*

- koszty i ryzyka (dla inwestora: wartość oczekiwana strat związanych z ryzykami opisanymi wcześniej; dla akceptanta: koszty transakcyjne, w tym systemowe koszty płatności czy koszty

72 Można tu wymienić więcej grup osób korzystających, np. ci, którzy są zainteresowani innowacją. Skupiamy się na trzech głównych, które w długiej perspektywie są zainteresowani kryptowalutami.

przystosowania się do korzystania z systemu, koszty „zmiany cenników", „zdartych zelówek"; dla kopalni: koszty energii, koszty osobowe, koszty organizacji „wydobycia" itp.), wszyscy zaś powinni uwzględnić ryzyka i koszty związane ze zmianami prawno-regulacyjnymi.

Jak zauważył P. M. Dudek, „Warto zasygnalizować, że stanowisko Trybunału Sprawiedliwości otwiera pole do traktowania bitcoina jako – wprost – pieniądza lub waluty w świetle prawa prywatnego…"[73]. Ponadto w konsekwencji wyroku: „W zakresie tych dziedzin prawa, które podlegają zharmonizowaniu (…) **bitcoin jest pieniądzem** w Unii Europejskiej"[74]. Kwestią czasu jest właściwe rozpoznanie tego zjawiska przez banki centralne i urzędy nadzoru finansowego oraz dopuszczenie do oficjalnego obrotu (bez nakładania obowiązku akceptacji) środków wymiany nie emitowanych przez władze centralne. Tak jak możliwe stało się prowadzenie korespondencji bez pośrednictwa narodowego operatora pocztowego, a przez Internet, tak samo jest z pieniędzmi – oprócz narodowych, istnieją takie, które nie należą do nikogo indywidualnie, ale należą do wszystkich jednocześnie – tak samo jak aktualnie Internet.

## 5.2. Arbitraż

Jest to jeden z najstarszych sposobów zarabiania na giełdach kryptowalutowych. Polega on na wyszukiwaniu i wykorzystywaniu różnic kursowych pomiędzy nimi: przeprowadza się zakup na giełdzie, na której cena jest najniższa, w celu odsprzedaży na giełdzie, gdzie cena jest wyższa. Podczas stosowania arbitrażu warto wziąć pod uwagę koszty przelania kryptowalut między giełdami oraz koszty transakcyjne (marże giełd). Tą metodę można porównać do tzw. Cross-Border Arbitrage – znanego z rynków kapitałowych.

Obecnie coraz trudniej jest zarobić na tego typu działalności – zajmują się nią coraz większe firmy oraz boty – algorytmy handlujące operujące na różnych giełdach. Napisanie ich i utrzymanie w bezbłędnym działaniu nie jest łatwe. Istnieje na rynku oprogramowanie, które wspomaga automatyzację tego typu transakcji; jednakże ono również nie zawsze jest bezbłędne.

## 5.3. Spekulacja na zmianę kursu

Inwestycję w zmianę kursu wymiany kryptowaluty na waluty fiducjarne (ang. fiat[75]) lub na inne kryptowaluty, czyli tak zwaną spekulację, można podzielić według następujących kryteriów:

73 P. M. Dudek, *Waluta bitcoin – glosa do wyroku Trybunału Sprawiedliwości z 22.10.2015 r. w sprawie C-264/14 Skatteverket przeciwko Davidowi Hedqvistowi*, „Europejski Przegląd Sądowy", czerwiec 2016 r., s. 43.

74 K. Zacharzewski, K. Piech (red.), *Przegląd polskiego prawa w kontekście zastosowań technologii rozproszonych rejestrów oraz walut cyfrowych*, Ministerstwo Cyfryzacji – Strumień „Blockchain i Kryptowaluty", 19 stycznia 2017 r., https://www.gov.pl/documents/31305/52168/przeglad_polskiego_prawa_w_kontekscie_zastosowan_technologii_rozproszonych_rejestrow_oraz_walut_cyfrowych.pdf/, s. 12 [dostęp: 13 listopada 2017 r.].

75 *Pieniądz fiducjarny*, Narodowy Bank Polski, https://www.nbportal.pl/slownik/pozycje-slownika/pieniadz-fiducjarny [dostęp: 17 lipca 2017 r.].

- Czas – inwestować można przyjmując strategię krótkoterminową, bądź też prognozować ceny w perspektywie długoterminowej,
- Kierunek zmiany – wyróżnia się pozycję długą (ang. *long*), czyli grę na wzrost oraz krótką (ang. *short*), czyli grę na spadek.

Inwestowanie krótkoterminowe opiera się na ciągłej analizie zmienności kursu. Pod uwagę bierze się wpływ nawet stosunkowo niewielkich wydarzeń, które mogą mieć przełożenie na decyzje innych inwestorów. Podejmowanie decyzji w krótkim horyzoncie wymaga sporej odporności na stres oraz zrozumienia psychologii tłumów. Warto podkreślić, iż osoby inwestujące krótkoterminowo często wykorzystują do prognozowania cen **analizę techniczną**[76]. Analiza ta bazuje na danych historycznych i co do zasady nie uwzględnia czynników takich jak użyteczność danej kryptowaluty, podstawy techniczne, perspektywy rozwoju itp. Inwestowanie krótkoterminowe zaleca się tylko doświadczonym inwestorom, ponieważ wymaga ono doświadczenia rynkowego oraz specjalistycznej wiedzy. Mimo to, wiele osób się na nią decyduje.

Niektórzy, zwabieni wizją szybkich zysków (np. oglądając wykres bitcoina w dłuższej perspektywie oraz ulegając namową odpowiednich sprzedawców), uważając że to „pewny" interes nawet inwestują w handel z dźwignią. Tylko kilka giełd oferuje taką możliwość. Należy pamiętać, że jest to ekstremalnie ryzykowne – można stracić wszystkie zainwestowane środki.

*Wykres 10 Kurs bitcoina w ciągu ostatnich 3 lat*


*Źródło: https://coinmarketcap.com/currencies/bitcoin [dostęp: 8 listopada 2017 r.]*

Należy podkreślić, iż znaczna większość początkujących inwestorów ulega problemowi zniecierpliwienia. Co do zasady osoby rozpoczynające przygodę z inwestowaniem nie lubią czekać na wyniki. Inwestowanie krótkoterminowe umożliwia im niemal ciągłe działanie poprzez analizę i podejmowanie decyzji każdego dnia, co przy krótkim doświadczeniu inwestycyjnym może zakończyć się stratą.

76 *Analiza Techniczna*, Edukacja Giełdowa, https://www.edukacjagieldowa.pl/gieldowe-abc/analiza-techniczna [dostęp: 19 lipca 2017 r.].

Zaleca się, aby inwestowanie krótkoterminowe rozpocząć od solidnego przygotowania teoretycznego w zakresie wiedzy dotyczącej kryptowalut. Zdecydowanie bardziej bezpieczną ścieżką wyboru dla początkujących jest inwestowanie długoterminowe w kryptowaluty, które znalazły już szerokie zastosowanie (bitcoin, ethereum).

W odróżnieniu od inwestowania krótkoterminowego, w dłuższym horyzoncie czasowym na znaczeniu zyskuje **analiza fundamentalna**[77]. W przypadku tradycyjnych walorów (np. akcji) analizuje się kompleksowo fundamentalne czynniki generujące ich wartość – czyli w przypadku rynku akcji wszystko to, co umożliwia generowanie zysków w przedsiębiorstwie: zarówno z punktu widzenia makroekonomicznego, sektorowego (konkurencji, partnerów) jak i czynniki wewnętrzne czy finansowe. W przypadku kryptowalut sytuacja jest znacznie bardziej złożona, ze względu na to, że kryptowaluty są walorem nieco wymykającym się tradycyjnym metodom analizy (szczególnie wyceny). Są walorem, którego działanie nie podlega wprawdzie żadnym regulacjom jako takim, ale wykorzystanie może wiązać się z różnymi skutkami w różnych krajach. Nie jest też związany wprost z gospodarką pojedynczego kraju, a z globalnym rynkiem walut. Inaczej niż w przypadku akcji czy obligacji, nie stoi za bitcoinem żadne przyrzeczenie dochodu inne niż zysk kapitałowy (spekulacyjny); można co najwyżej rozpatrywać zysk ekonomiczny związany np. ze zmniejszeniem ewentualnych kosztów transakcyjnych. W przypadku kryptowalut zatem należy ocenić czynniki:

- makro (związane ewentualnym wpływem różnych jurysdykcji na cenę, poziom inwestycji w usługi i technologie związane z kryptowalutami, duże włamania na giełdy, czy inne wydarzenia wpływające na cały system[78]),
- „sektorowe" (zależność od innych kryptowalut) a także
- „wewnętrzne" (przychody wykopujących a koszty energii, opłaty transakcyjne, jakość technologii względem innych kryptowalut, czy wycena realnej usługi dostarczania przez system alternatywnego środka wymiany i gromadzenia wartości, która jest pochodną wartości dóbr dostępnych do kupienia za kryptowalutę).

Dobrą praktyką w przypadku grania na długoterminowy wzrost jest przeniesienie środków z giełdy na portfel dyskowy. Można go dodatkowo zabezpieczyć hasłem, a nawet zapisać na ukrytej partycji dysku (lub skorzystać z portfeli off-line). Zapobiega to ryzyku utraty środków spowodowanym atakiem hakerów na wybraną przez nas giełdę. Trzymając kryptowaluty na dysku również jesteśmy podatni na potencjalny atak hakerów. Zatem ważnym jest, aby zabezpieczyć nasz portfel hasłem, a komputer – stale aktualizowanym programem antywirusowym. Dodatkowo warto również wydrukować klucz prywatny powiązany z adresem, na którym lokujemy inwestycje.

77 *Analiza fundamentalna*, Narodowy Bank Polski – Portal Edukacji Ekonomicznej, https://www.nbportal.pl/slownik/pozycje-slownika/analiza-fundamentalna [dostęp: 19 lipca 2017 r.].

78 Przykładowy ich spis: *Wydarzenia w historii Bitcoina (do 2017-07-17), subiektywne zestawienie + ICO + VC*, https://docs.google.com/spreadsheets/d/e/2PACX-1vRCddBDpqdYCrnz4_F9F3dCB9swu51xKlKj6ViL5Mt5rW158N3ag5adNV1SxSbNwDIuDrVzr69u2YN_A/pubhtml# [dostęp: 13 listopada 2017 r.].

Jeśli chodzi o kierunek zmiany, to zdecydowana większość inwestorów, niezależnie od wybranego kryterium czasowego, gra na wzrost ceny wybranego waloru względem bazowego, w stosunku do którego jest rozliczana strata lub zysk. Pozycja długa, inaczej zwana też transakcją kupna (Buy), polega na kupnie na przykład bitcoinów za złotówki po aktualnym kursie i oczekiwaniu na wzrost kursu tak, żeby sprzedać zakupione bitcoiny z zyskiem.

Alternatywą do tego sposobu spekulacji jest zajęcie pozycji krótkiej, inaczej zwanej transakcją sprzedaży (Sell). Transakcja ta polega na tym, że bitcoiny są pożyczane od innego użytkownika (możliwość taka istnieje na wybranych giełdach kryptowalut) i sprzedawane po aktualnym kursie. Następnie oczekuje się spadku kursu bitcoina tak, by kupić pożyczoną ilość bitcoinów po kursie niższym od tego, po którym bitcoiny zostały sprzedane i zwrócić pożyczone bitcoiny pożyczkodawcy. W przypadku krótkiej pozycji, oprócz opłat transakcyjnych należnych giełdzie w analizie rentowności należy brać pod uwagę również koszty utrzymywania krótkiej pozycji (koszty pożyczania kryptowaluty).

## 5.4. Inwestowanie w kryptowaluty – obszary ryzyka

Ryzyka związane z inwestowaniem w kryptowaluty można podzielić na dwie kategorie:

1. **Inwestycje krótkoterminowe**, z którymi wiążą się:
    - wysoka zmienność kursów,
    - ciągłość notowań – giełdy działają przez całą dobę,
    - duża ilość transakcji zwiększa łączny koszt prowizji giełdowej,
    - konieczność śledzenia rynku na bieżąco,
    - presja emocjonalna, problem zniecierpliwienia,
    - wysokie spready giełdowe wśród mniej popularnych kryptowalut,
    - użycie dźwigni w przypadku nagłej zmiany kursu może przełożyć się na osiągnięcie maksymalnej straty i utraty całości zainwestowanej kwot,
    - bańki spekulacyjne,
    - konieczność trzymania środków na giełdzie w celu szybkiego reagowania na zmiany – ryzyko utraty środków w wyniku problemów z giełdą.

2. **Inwestycje długoterminowe**, w tym:
    - zamrożenie środków na długi czas,
    - ryzyko ataku na giełdę kryptowalutą i utraty środków, czy defraudację,
    - ryzyko utraty hasła do rzadko używanego portfela na dysku,
    - podatność na wydarzenia ze świata kryptowalut,
    - rosnące koszty kontraktów typu dźwignia,
    - ryzyko przejęcia przez władze,
    - wyjście z systemu ważnych graczy,
    - ryzyko uruchomienia uśpionych środków z bloku genesis i innych wczesnych bloków (w przypadku Bitcoina),

- ryzyko wszelkich problemów z infrastrukturą internetową utrudniających działanie sieci Bitcoin,
- ryzyko zmowy największych węzłów sieci.

## 5.5. Initial Coin Offering

Initial Coin Offering (ICO) lub Initial Token Offering (ITO) jest jednym z popularnych sposobów finansowania projektów związanych z blockchainem i kryptowalutami. W pewnym zakresie można go także traktować jako jedną z form crowdfundingu. Startupy chcące zebrać kapitał na rozwój przeprowadzają quasi-publiczną (bo najczęściej jeszcze nie regulowaną) ofertę emisji swoich tokenów cyfrowych. Działa to na podobnej zasadzie jak crowdfunding. Takie tokeny w przedsprzedaży (pre-ICO) można zazwyczaj kupić po bardzo atrakcyjnej cenie. Następnie można je odsprzedać (niekiedy ze znaczącym zyskiem), bądź zachować do czasu wytworzenia obiecanego inwestorom produktu. ICO cieszy się dużą popularnością ze względu na łatwość pozyskiwania w ten sposób dużych środków (praktycznie z całego świata) oraz bardzo wysokie niekiedy stopy zwrotu.

Wartość pieniędzy inwestowanych w ICO wciąż rośnie, od 2014 roku do 2017 prawie pięćdziesięciokrotnie[79]. Do października 2017 r. największe ICO, zgodnie z danymi portalu CoinDesk.com, zebrało 262 mln USD, a aktualnie dzięki wszystkim ICO zebrano środki o równowartości **3 miliardów dolarów**[80], co przy kapitalizacji rynku kryptowalut na poziomie ok. 200 mld USD zaczyna być znaczącą wartością. W ostatnim czasie wartość wnoszonych w ten sposób do startupów funduszy przekroczyła kwoty przeznaczane bezpośrednio przez fundusze venture capital[81] na rzecz firm internetowych.

Większość ICO odbywa się na Ethereum lub na innych platformach umożliwiających stosowanie tzw. smart kontraktów. Smart kontrakty są umowami napisanymi w języku oprogramowania, automatycznie realizującymi warunki i operacje uzgodnione pomiędzy stronami takiej umowy.

Podstawą decyzji o inwestycji w konkretne ICO powinna być szczegółowa analiza białej księgi (ang. *whitepaper*), czyli dokumentu zawierającego analizę przyszłego produktu lub technologii, koncepcyjną propozycję platformy, którą chce stworzyć zespół realizujący, na którą zbierane są środki. W przypadku inwestycji w określony projekt już po etapie ICO sprawdzić należy mapę drogową projektu (ang. *roadmap*) i zweryfikować, czy zespół realizujący dotrzymuje terminy.

79 M. Druś, *Rekordowe wpływy start-upów z ICO*, „Puls Biznesu", 18 lipca 2017 r., https://www.pb.pl/rekordowe-wplywy-start-upow-z-ico-866648.

80 *Cryptocurrency ICO Stats 2017*, CoinSchedule, https://www.coinschedule.com/stats.php [dostęp: 16 października 2017 r.].

81 *Firmy Blockchain zebrały 2,4 razy więcej środków z ICO niż inwestycje VC*, Cryptonews, 5 maja 2017 r., https://cryptonews.pl/firmy-blockchain-zebraly-24-razy-wiecej-srodkow-ico-niz-inwestycji-vc.

W ICO trzeba inwestować z rozwagą i należy przeanalizować dany projekt, ponieważ niektóre z nich z góry skazane są na niepowodzenie i mogą służyć do wyłudzenia środków. Z drugiej strony czasami zdarza się, że projekty – nawet pomimo dobrego przygotowania i wielu perspektyw rozwoju – mogą paść ofiarą ataku hakerskiego[82]. Za przykład służyć może przypadek ICO – Enigma, podczas którego skradziono pół miliona dolarów[83].

Inwestując środki w ICO warto wziąć również pod uwagę ryzyko regulacji tej metody finansowania. Organy państwowe w różnych krajach na świecie upatrują w ICO podobieństw do tradycyjnych ofert publicznych emisji papierów wartościowych (ang. Initial Public Offering – IPO) – uregulowanych prawnie i stawiających liczne wymogi wobec emitentów, mimo że niektóre ICO nie są wcale powiązane z podziałem zysków firmy. W niektórych państwach, np. Chinach, wprowadzane są zakazy ICO. Decyzje takie mogą mieć niespodziewany i negatywny wpływ na kursy poszczególnych kryptowalut.

82 W. Zhao, *$7 Million Lost in CoinDash ICO Hack*, CoinDesk, 17 lipca 2017 r., https://www.coindesk.com/7-million-ico-hack-results-coindash-refund-offer.

83 F. Memoria, *Hacker Nets over $500,000 after Hacking Enigma before ICO Date*, Cryptocoins News, 21 sierpnia 2017 r., https://www.cryptocoinsnews.com/hacker-nets-over-500000-after-hacking-enigma-before-its-ico-date.


# 6. Prawno-podatkowe aspekty kryptowalut w Polsce

## 6.1. Kwalifikacja walut cyfrowych

W polskiej nauce prawa prywatnego wskazuje się, że zgodnie z art. 44 kodeksu cywilnego waluty cyfrowe stanowią postać **mienia** („Mieniem jest własność i inne prawa majątkowe") oraz – niezależnie od tego – są **innym niż pieniądz miernikiem wartości** w myśl art. 358 § 2 kodeksu cywilnego („Strony mogą zastrzec w umowie, że wysokość świadczenia pieniężnego zostanie ustalona według innego niż pieniądz miernika wartości")[84].

Waluty cyfrowe nie mogą być uważane za rzecz, gdyż nie są przedmiotami materialnymi (art. 45 kodeksu cywilnego). Są **zbywalnym prawem majątkowym**[85]. Jako **prawo podmioto-**

84 K. Zacharzewski, K. Piech (red.), *Przegląd polskiego prawa w kontekście zastosowań technologii rozproszonych rejestrów oraz walut cyfrowych*, Ministerstwo Cyfryzacji – Strumień „Blockchain i Kryptowaluty", 19 stycznia 2017 r., https://www.gov.pl/documents/31305/52168/przeglad_polskiego_prawa_w_kontekscie_zastosowan_technologii_rozproszonych_rejestrow_oraz_walut_cyfrowych.pdf, s. 13.

85 Polemizuje z tym A. Kotucha uważając, że jest to wadliwe rozumowanie, gdyż kryptowaluty ewidentnie występują w stanie faktycznym, a nie w sferze praw. A. Kotucha, *Bitcoin nie jest prawem*, 29 października 2017 r., http://schiffersroczynski.pl/blog/399-bitcoin-nie-jest-prawem

**we względne**, skuteczne tylko *inter partes*, waluty cyfrowe nie mogą być przedmiotem własności; do majątku osoby utytułowanej mogą wchodzić tylko jako wierzytelność. W związku z tym wyrażenie „własność waluty cyfrowej" z technicznoprawnego punktu widzenia jest niepoprawne i może być używane jedynie w języku potocznym[86].

Waluta cyfrowa nie może być uznawana za prawny środek płatniczy, nie jest bowiem emitowana przez organ władzy publicznej. Określanie jej jako waluty cyfrowej, wirtualnej, kryptowaluty, czy jakiejkolwiek innej **waluty** jest akceptowalne jedynie w języku potocznym. Bliższymi wobec walut cyfrowych, w aspekcie jurydycznym, są dary ziemi takie jak np. bursztyn czy złoto, z tym zastrzeżeniem, że po wydobyciu stają się one rzeczą w rozumieniu art. 45 kodeksu cywilnego. Waluta cyfrowa jest zatem pierwotnym miernikiem wartości, który może posiadać atrybut środka umarzania zobowiązań, o ile strony tak postanowią[87].

Oznacza to, że dłużnik może „uwolnić się" od zobowiązania za pomocą waluty cyfrowej tylko wówczas, gdy wierzyciel wyrazi zgodę na przyjęcie świadczenia w takiej postaci. Nikt nie ma obowiązku przyjęcia świadczenia w postaci waluty cyfrowej wbrew własnej woli.

Odwrotnie jest w przypadku prawnych środków płatniczych, którym moc umarzania zobowiązań przyznaje konkretne państwo. Wierzyciel, który podlega jego władzy publicznej jest zobowiązany do przyjęcia od dłużnika środków uznanych za prawne środki płatnicze, a po ich przyjęciu dług dłużnika wygasa (tak samo, jak wierzytelność wierzyciela)[88].

## 6.2. Przeniesienie tytułu do waluty cyfrowej

W związku z tym, że waluta cyfrowa nie może być przedmiotem własności, to czynność prawna, która zobowiązuje do rozporządzenia walutą cyfrową nie niesie za sobą skutku rozporządzającego wyrażonego w treści art. 155 § 1 kodeksu cywilnego. Bardziej odpowiednią podstawą prawną dla rozporządzeń walutami cyfrowymi jest art. 510 § 1 kodeksu cywilnego. Zgodnie z art. 555 kodeksu cywilnego – do sprzedaży praw stosuje się odpowiednio przepisy o sprzedaży rzeczy. Jednakże, aby rozporządzenie walutą cyfrową było skuteczne, dodatkowo konieczne jest dokonanie aktu konwencyjnego w postaci wykorzystania klucza prywatnego. Taki akt jest przykładem ograniczenia skutku rozporządzającego czynności zobowiązującej, zgodnie z treścią art. 510 § 1 kodeksu cywilnego („chyba (…) że strony inaczej postanowiły"). Oznacza to, że bez wykorzystania klucza prywatnego umowa, która zobowiązuje do rozporządzenia walutą cyfrową, nie wywoła automatycznego skutku rozporządzającego[89].

86 K. Zacharzewski, *Bitcoin jako przedmiot stosunków prawa prywatnego*, „Monitor Prawniczy" 2014, nr 21, s. 1132-1139.

87 Ibidem.

88 S. Bala, T. Kopyściański, W. Srokosz, *Kryptowaluty jako elektroniczne instrumenty płatnicze bez emitenta. Aspekty informatyczne, ekonomiczne i prawne*, Uniwersytet Wrocławski, Wrocław 2016, s. 107.

89 Ibidem.

Czynność zobowiązująca + Akt konwencjonalny = Skutek rozporządzający

Umowa sprzedaży bitcoina + wykorzystanie klucza prywatnego = przeniesienie praw do bitcoina

## 6.3. Waluty cyfrowe a prawo zobowiązań

Na gruncie prawa zobowiązań waluty cyfrowe mogą pełnić dwie zasadnicze role:

- przedmiotu świadczenia kupującego (ceny) oraz
- przedmiotu świadczenia sprzedającego (przedmiotu sprzedaży).

Jeżeli w umowie zobowiązującej do rozporządzenia **waluta cyfrowa uznawana jest za zapłatę**, a przedmiotem świadczenia sprzedającego jest inne mienie (np. samochód), trafne wydaje się, w obecnym stanie prawnym, zakwalifikowanie takiej umowy jako **umowy zamiany**. Zgodnie z art. 504 kodeksu cywilnego do umowy zamiany stosuje się odpowiednio przepisy o umowie sprzedaży.

Umową sprzedaży będzie natomiast wyłącznie taka umowa, w której waluta cyfrowa uznawana jest za przedmiot świadczenia sprzedającego, w zamian za który otrzyma on legalnie funkcjonujący pieniądz lub odwrotnie (sprzedaż kantorowa)[90].

## 6.4. VAT oraz podatek dochodowy od osób fizycznych

W wyroku z dnia 22 października 2015 r. Trybunał Sprawiedliwości Unii Europejskiej stwierdził, że „świadczenie usług (…), które polegają na wymianie walut tradycyjnych na jednostki wirtualnej waluty <bitcoin> i odwrotnie (…) stanowi transakcje zwolnione z podatku od wartości dodanej". Zdaniem Trybunału art. 135 ust. 1 lit. e dyrektywy Rady, konstytuujący zwolnienie z podatku VAT transakcji dotyczących „walut, banknotów i monet używanych jako prawny środki płatniczy" ma zastosowanie również do obrotu walutami cyfrowymi. Oznacza to, że nie trzeba płacić VAT-u za czynności związane z wydobyciem i obrotem kryptowalut.

W myśl ustawy o podatku dochodowym od osób fizycznych[91], osoby fizyczne podlegają nieograniczonemu obowiązkowi podatkowemu, tj. jeżeli mieszkają w Polsce to podlegają obowiązkowi podatkowemu od całości swoich dochodów (przychodów) bez względu na miejsce położenia źródła przychodów.

90 K. Zacharzewski, *Praktyczne znaczenie bitcoina na wybranych obszarach prawa prywatnego*, „Monitor Prawniczy" 2015, nr 4, s. 187-195.

91 Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (Dz.U. z 2016 r. poz. 2032).

Wspomniany akt określa, jakiego rodzaju dochody podlegają opodatkowaniu. I tak, **dochodem** ze źródła przychodu jest **nadwyżka sumy przychodów** z tego źródła **nad kosztami** ich uzyskania osiągnięta **w danym roku podatkowym**.

Źródła przychodu wymienione są wyczerpująco w art. 10 ust. 1, a wśród nich wskazane są m.in.: kapitały pieniężne i prawa majątkowe, w tym odpłatne zbycie praw majątkowych. W ustawie zdefiniowane jest również ogólne pojęcie przychodów jakimi są m.in.: otrzymane lub postawione do dyspozycji podatnika w roku kalendarzowym pieniądze i wartości pieniężne oraz wartość otrzymanych świadczeń w naturze i innych nieodpłatnych świadczeń.

Ustawa jedynie przykładowo wskazuje, co może być przychodem z praw majątkowych, jest to więc katalog otwarty, w skład, którego mogą wchodzić jeszcze inne przychody z praw majątkowych, tj. przychód z kryptowalut.

Bitcoin i inne kryptowaluty są zbywalnymi prawami majątkowymi, stanowiącymi składnik mienia[92], co oznacza, że **przychody uzyskane ze sprzedaży kryptowalut podlegają opodatkowaniu**.

Przedstawiony powyżej sposób opodatkowania przychodów ze sprzedaży kryptowalut stanowi aktualne stanowisko prezentowane przez organy skarbowe, wskazywane w interpretacjach indywidualnych[93]. Trzeba jednak pamiętać, że może ulegać ono dość dynamicznym zmianom. W związku z tym uzasadnionym wydaje się śledzenie najnowszych informacji, a w przypadku wątpliwości warto zgłosić się do urzędu skarbowego z wnioskiem o wydanie indywidualnej interpretacji podatkowej.

Przychody ze sprzedaży kryptowalut powinno wpisywać się w zeznaniu podatkowym PIT-36, w części D.1, w rubryce 74, a koszty uzyskania przychodu w rubryce 75[94]. Trzeba **pamiętać o dokumentowaniu transakcji** kupna i sprzedaży walut cyfrowych na giełdach, poprzez np. wykonanie zrzutu ekranu lub wydruk potwierdzający przelew z konta inwestora na konto giełdy[95]. Jeżeli nie będziemy posiadali dowodu na zakup kryptowaluty, nie będziemy mogli wpisać kosztów uzyskania przychodu, co będzie skutkowało tym, że podatek będzie obliczany od całej kwoty przychodu.

92 Ibidem, s. 50.

93 *Interpretacja Indywidualna*, syg.: 2461-IBPB-2-2.4511.12.2017.2.BF, 03.04.2017, http://sip.mf.gov.pl/faces/views/szczegoly/szczegoly-interpretacji-indywidualnej.xhtml?dokumentId=502729&poziomDostepu=PUB&indexAccordionPanel=-1#tresc, [dostęp: 24 sierpnia 2017 r.].

94 *Interpretacja Indywidualna*, syg.: IPPB2/415-842/13-2/MK, 25.02.2014, http://sip.mf.gov.pl/faces/views/szczegoly/szczegoly-interpretacji-indywidualnej.xhtml?dokumentId=382095&poziomDostepu=PUB&indexAccordionPanel=-1#tresc, [dostęp: 25.08.2017].

95 *Interpretacja Indywidualna*, syg.: IPPB1/415-276/14-4/EC, 26.06.2014, http://sip.mf.gov.pl/faces/views/szczegoly/szczegoly-interpretacji-indywidualnej.xhtml?dokumentId=394395&poziomDostepu=PUB&indexAccordionPanel=-1#tresc, [dostęp: 28.08.2017].

Przykładowo, jeżeli zakupimy Bitcoiny za 2000 złotych, po czym sprzedamy je za 3000 złotych to nasz przychód będzie wynosił 1000 złotych. Jednakże jeżeli nie będziemy posiadali żadnego potwierdzenia transakcji kupna Bitcoinów, w świetle prawa nasz przychód po sprzedaży będzie wynosił 3000 złotych i nie będziemy mogli obniżyć podstawy opodatkowania o koszty uzyskania przychodu.

Przychody z kryptowalut opodatkowane według skali określonej w art. 27 ustawy o podatku dochodowym od osób fizycznych, w zależności od sumy przychodów danego podatnika, w konkretnym roku podatkowym. W 2017 roku pierwszy próg podatkowy wynosi 18% – w przypadku sumy dochodów brutto do 85 528 złotych, a drugi próg podatkowy – 32%, w przypadku sumy dochodów brutto przekraczającej tę kwotę.

Rozliczenie dotyczy całego roku podatkowego, jeżeli więc w jego trakcie kilkukrotnie zakupimy i sprzedamy kryptowaluty, należy doliczyć do siebie przychody z każdorazowej zamiany kryptowalut na złotówki oraz odliczyć od tego udokumentowane koszty przychodu.

## 6.5. Skala oraz rodzaje przestępstw popełnianych przy użyciu kryptowalut

Z funkcjonowaniem walut cyfrowych wiąże się kilka zagadnień, które stanowić mogą potencjalne zagrożenie. Należą do nich m.in.:

- decentralizacja baz danych, na których oparte są kryptowaluty;
- łatwość dostępu oraz brak wymaganych dokumentów potwierdzających tożsamość użytkownika, wpływają na zwiększoną anonimowość zawieranych transakcji;
- brak jednego zdefiniowanego oraz zaufanego emitenta;
- brak instytucji nadzorczych;
- brak tożsamości prawnej (jedynie nieliczne państwa, takie jak Japonia, Chiny czy Stany Zjednoczone uregulowały prawnie waluty cyfrowe);
- brak dostatecznej wiedzy oraz świadomości społecznej dotyczącej kryptowalut.

Wszystkie wyżej wymienione czynniki wpływają na to, iż waluty cyfrowe mogą być potencjalnie interesującym narzędziem do przeprowadzenia lub częściowego pośredniczenia w przestępstwach.

Przestępstwa z użyciem kryptowalut można usystematyzować według 5 kategorii:

- przestępstwa „klasyczne” – dotyczą one użycia walut cyfrowym w celu anonimowego zakupu nielegalnych towarów oraz usług, w tzw. Darknet (Deep Web);
- przestępstwa „dużego kalibru” – w tą kategorię wchodzą najcięższe przestępstwa, stanowiące największe zagrożenie, takie jak finansowanie terroryzmu czy pranie pieniędzy;
- przestępstwa teleinformatyczne – odnoszą się one do nielegalnego oddziaływania na

dane cyfrowe. W skład tych działań wchodzą między innymi ataki hakerskie na giełdy kryptowalutowe;
- innowacyjne formy przestępczości – przykładem są przestępstwa oparte na tak zwanych smart kontraktach (samo wykonujące się cyfrowe umowy);
- przestępstwa częściowo spowodowane przez błąd ludzki – odnoszą się do wykorzystania przez przestępców luki w działaniu systemu spowodowanej przez błąd ludzki (niedostateczne zabezpieczenie haseł oraz poufnych danych, błędy w funkcjonowaniu systemu)[96].

W badaniach przeprowadzonych przez firmę Chainalysis[97] (wiodącego dostawcę oprogramowania zapobiegającego praniu pieniędzy, chroniącego połączenie finansów z zdecentralizowanym Internetem) szacuje się, że ponad 30 000 osób padło ofiarą cyberprzestępczości związanej z kryptowalutą Ethereum, tracąc średnio 7 500 USD każda. Z analizy wynika również, że ponad połowa z poszkodowanych (tj. 16 900 osób) straciła swoje pieniądze w wyniku phishingu – czyli metody oszustwa, polegającej na tym, że przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji. 11 000 z poszkodowanych padło ofiarą programów mających na celu wykorzystanie błędów w oprogramowaniu, 2 100 poniosło stratę z powodu włamania hakera, a jedynie 260 osób straciło swoje środki w związku z piramidami finansowymi[98].

Według raportu Rady Unii Europejskiej w sprawie oceny ryzyka prania pieniędzy i finansowania terroryzmu wpływającego na rynek wewnętrzny, największymi zagrożeniami wiążącymi się z walutami cyfrowymi są odpowiednio finansowanie działalności terrorystycznej oraz wprowadzanie do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł. W raporcie zwrócono uwagę, iż użycie kryptowalut w celu skutecznego przeprowadzenia przestępstwa wymaga od przestępcy wyspecjalizowanej wiedzy w dziedzinie technologii informacyjnej oraz technicznej wiedzy dotyczącej zarządzania walutami cyfrowymi. Są one niezbędne w celu zanonimizowania swojej tożsamości, która uniemożliwi wyśledzenie sprawcy przestępstwa. W raporcie zaznaczono również, iż pomimo istniejącego zagrożenia ze strony kryptowalut, to z powodów barier technologicznych, którą stawiają przed przestępcami waluty cyfrowe, są one rozwiązaniem rzadziej wybieranym[99]. Wynika z tego, że przestępcy częściej wolą wybrać łatwiejsze, wymagające mniejszej wiedzy technicznej oraz sprawdzone rozwiązania w celu przeprowadzenia udanego przestępstwa, niż te związane z kryptowalutami.

96 P. Opitek, *Przestępczość z wykorzystaniem kryptowalut oraz ich status w postępowaniu karnym*, referat wygłoszony na międzynarodowej konferencji naukowej „Techniczne aspekty przestępczości teleinformatycznej", Instytut Kościuszki, Szczytno, 14 czerwca 2017 r.

97 Chainalysis, www.chainalysis.com [dostęp: 4 września 2017 r.].

98 L. Chen, Y. Nakamura, *Cryptocurrency Cyber Crime Has Cost Victims Millions This Year*, Bloomberg, www.bloomberg.com/news/articles/2017-08-24/cyber-criminals-extracting-a-heavy-toll-from-ethereum-advocates [dostęp: 4 września 2017 r.].

99 *Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and ○relating to cross-border situations*, Council of the European Union, 4 lipca 2017 r., http://europeanmemoranda.cabinetoffice.gov.uk/files/2017/07/10977-17-ADD-2.pdf, s. 87.

Podsumowując, istotnym działaniem, które powinno być podjęte w celu bezpiecznego rozwoju walut cyfrowych w Polsce i na świecie oraz w celu ochrony użytkowników legalnie korzystających z walut cyfrowych jest skuteczne szkolenie sędziów, prokuratorów i funkcjonariuszy organów dochodzeniowo-śledczych w praktycznych kwestiach funkcjonowania kryptowalut oraz blockchaina. Dostateczna wiedza na ten temat pozwoli na właściwe kwalifikowanie przestępstw popełnianych na tym polu, skuteczne zabezpieczanie śladów i dowodów przestępstwa[100]. Także agenda Interpolu – Cyber Research Lab, podjęła działania zmierzające do poznania mechanizmów funkcjonowania czarnego internetowego rynku[101]. Stworzyła ona własną, prywatną sieć Darknet, własną kryptowalutę oraz symulowany rynek (marketplace), aby móc używać jej do szkoleń policjantów, w celu sprawnego prowadzenia dochodzeń[102].

100 Ibidem, s. 49.

101 Przykładem działania w tym kierunku jest już czwarta edycja konferencji zorganizowanej przez Europol dotycząca walut cyfrowych. Głównym celem konferencji było dalsze umocnienie walki z nadużyciami wirtualnych walut na potrzeby transakcji kryminalnych i prania brudnych pieniędzy. Por. *Europol hosted 4th conference on virtual currencies*, 5 lipca 2017 r., www.europol.europa.eu/newsroom/news/europol-hosted-4th-conference-virtual-currencies.

102 *INTERPOL backs World Economic Forum cybercrime project*, Interpol, 22 stycznia 2016 r., https://www.interpol.int/News-and-media/News/2016/N2016-010.


# 7. Zalety i wady walut cyfrowych

Płatności dokonywane przy użyciu kryptowalut posiadają wiele zalet, których próżno by szukać u płatności pieniędzmi konwencjonalnymi. Podstawową jest wolność związana z użytkowaniem kryptowalut. Gwarantują one możliwość względnie szybkiej zapłaty kwoty w każde miejsce na świecie (z dostępem do Internetu) 24/7 – bez dni wolnych oraz bez limitów. Umożliwiają więc one większą kontrolę nad swoimi środkami niż np. tradycyjne przelewy czy usługi międzynarodowych transferów pieniężnych. W porównaniu do tradycyjnego przelewu bankowego, w kryptowalutach pojęcie zaufanej trzeciej strony jest ograniczone (częściowo stały się nią giełdy kryptowalutowe, które w większości nie są zdecentralizowane, co wystawia użytkowników na ryzyka). Nie jest potrzebny więc udział instytucji bankowych, które tradycyjnie pełnią funkcję kontrolera. Społeczność danej kryptowaluty sprawuje nad nią nadzór, przy czym zasady rządzące systemem zapisane są w kodzie komputerowym, który staje się „prawem" (*code is law*). Możliwe są jego zmiany, jednak niekiedy jest to bardzo trudne – im system jest większy i bardziej zróżnicowane są interesy poszczególnych grup jego interesariuszy, tym trudniej o konsensus. Dobrze to widać na przykładzie zmian w Bitcoinie.

W związku z brakiem pośredników (banków) można liczyć w większości przypadków na znacznie niższe opłaty transakcyjne, na które składają się przynajmniej opłaty do sieci (jeśli korzystamy z kantorów czy giełd – trzeba uwzględnić także z ich prowizje). W przypadku Bitcoina, trzeba się liczyć ze względnie wysokimi kosztami działania sieci (zużyta energia elektryczna) oraz stale rosnącym popytem na bitcoina, przez co są obecnie wysokie koszty transakcyjne,

szczególnie gdy chcemy nadać wyższy priorytet zatwierdzania naszej transakcji przez sieć[103]. W Bitcoinie trwają prace nad wprowadzeniem możliwości bezpłatnych i niemal natychmiastowych przekazów bitcoinów w ramach podsieci ufających sobie kontrahentów (którzy otworzą pomiędzy sobą kanały płatności), które możliwe będą dzięki implementacji tzw. Lightning Network[104]. Jest to jednak perspektywa miesięcy, a może nawet lat.

Kwestia bezpieczeństwa, która wiąże się z kryptowalutami jest kolejną cechą, która przyciąga nowych użytkowników. Zabezpieczenia stosowane przez kryptowaluty są na dzień dzisiejszy praktycznie niemożliwe do złamania[105], wymagałoby to bowiem gigantycznej mocy obliczeniowej, nieosiągalnej nawet przez najpotężniejsze superkomputery. Nie oznacza to, że nie można obejść zabezpieczeń podmiotów pośredniczących w handlu kryptowalutami – niektóre włamania na giełdy kończyły się znaczącymi stratami, np. Bitfinex w sierpniu 2016 r. utracił 120 tys. bitcoinów.

Bezpieczeństwo podnosi również fakt oparcia bitcoina i większości innych kryptowalut na tak zwanym oprogramowaniu *open source*, czyli takim, które ma publicznie dostępny kod źródłowy. Charakteryzuje się to tym, że każdy może sprawdzić zasady działania i naprawić jego ewentualne błędy w nowej wersji, która będzie musiała być przyjęta przez większość użytkowników.

Oparcie kryptowalut na blockchainie gwarantuje ich transparentność, ponieważ w przypadku większości ich rodzajów informacje dotyczące przeszłych transakcji są publicznie dostępne w czasie rzeczywistym. Konsekwencją oparcia kryptowalut na blockchainie (a nie na innej technologii rozproszonych rejestrów) jest nieodwracalność operacji (płatności) przeprowadzonych przy pomocy tych walut (raz zapisany blok w blockchainie już tam pozostaje na zawsze w niezmienionej formie). Dlatego nie można liczyć na zwrot przelewu przesłanego na błędnie podany adres, o ile osoba, której wysłaliśmy pieniądze, sama ich nam nie odeśle. Z punktu widzenia sklepów, handlowców wprowadzenie możliwości płatności kryptowalutami nie wiąże się z większymi problemami (o ile przestrzegają przepisów prawa podatkowego). Uzgodnioną przez obie strony transakcji walutę cyfrową otrzymują szybko, bezpośrednio na swoje „konto", bez możliwości zwrotu. Jeśli nie chcą otrzymać danej waluty, mogą skorzystać z usług pośrednika, który wymieni je np. na złotówki (InPay) czy dolary (BitPay).

Anonimowość kryptowalut jest kwestią, która często wywołuje spory. Przez niektórych może być bowiem uznawana za zaletę, a przez innych jako wadę. Brak przejrzystej informacji dotyczącej użytkowników może rodzić różne wątpliwości związane z kwestiami podatkowymi, legalnością pochodzenia pieniędzy lub celowym ukrycia tożsamości. Wątpliwości budzi także sama właściwość

103 W październiku 2017 r. przy opłacie ok 0,36 groszy (10 satoshi) za przeciętną transakcję (226 bajtów) zatwierdzenie transakcji może trwać nawet 13 godzin; chcąc mieć zagwarantowane zatwierdzenie w ciągu 25 minut, opłata dla sieci za transakcję wyniesie ok 5,4 zł (150 satoshi), co i tak nie jest wygórowaną wartością w porównaniu z opłatami za transfery międzynarodowe czy usługi typu PayPal (związane z przewalutowaniem). Por. *Predicting bitcoin fees for transactions*, Bitcoinfees, https://bitcoinfees.21.co [dostęp: 13 listopada 2017 r.].

104 Zob. *Lightning Network*, https://lightning.network [dostęp: 17 października 2017 r.].

105 Por. Large Bitcoin Collider, https://lbc.cryptoguru.org [dostęp: 17 października 2017 r.].

anonimowości, stąd mówi się o pseudonimowości[106]. Jest to jedną z przyczyn, dla których przestępcy nie są głównymi użytkownikami sieci Bitcoin, jak się część opinii publicznej uważa.

Ze względu na to, że historia kryptowalut jest stosunkowo krótka trzeba liczyć się z niskim stopniem ich akceptacji. Pomimo, iż ostatnio odnotowuje się znaczny wzrost zainteresowania nimi oraz akceptacji przez znaczące przedsiębiorstwa (Microsoft[107], PayPal[108], Dell[109], Steam/Valve[110], magazyn Time[111], Mozilla[112], Wikipedia[113], Wordpress[114]), to wciąż świadomość ich jest nieporównywalnie niższa niż innych środków wymiany, takich, jak chociażby pieniądz bezgotówkowy. Również skomplikowany mechanizm działania przyczynia się do niechęci ludzi do kryptowalut. Dodatkowo z powodu tego, że waluty cyfrowe są wciąż w fazie rozwoju, trzeba się liczyć z możliwymi zawirowaniami na ich rynku, takimi jak spora niestabilność cen. Niektóre, przeważnie nowe kryptowaluty mogą z dnia na dzień zyskiwać nawet 500% (lub stracić 50%) swojej wartości. Większe z nich, np. bitcoin, charakteryzują się rosnącą stabilnością w dłuższym okresie.

Jedną z wad kryptowalut jest fakt, że używanie ich jako zapłaty w handlu detalicznym i usługach nie jest powszechne (tak jak trudno jest dokonać płatności w Polsce używając dolara, czy mniej popularnej waluty innego kraju). Jednakże, ilość miejsc, w których akceptuje się kryptowaluty stale rośnie. W samej Warszawie jest 26 punktów stacjonarnych, w których możemy uiścić należność przy pomocy bitcoina. Na mapie coinmap.org możemy zobaczyć wszystkie tego typu miejsca na świecie. W październiku 2017 r. mapa wskazywała ponad 10 000 punktów akceptujących bitcoiny na całym globie[115].

106 Analiza anonimowości systemu była przedmiotem jednym z pierwszych publikacji naukowych dotyczących Bitcoina (2011 r.). Informacje o wszystkich transakcjach w sieci w zestawieniu z dodatkowymi informacjami zewnętrznymi oraz przy wykorzystaniu zaawansowanych technik analitycznych częściowo umożliwiają identyfikację osób. Por. F. Reid, M. Harrigan, *An Analysis of Anonymity in the Bitcoin System*, Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third International Conference on Social Computing (SocialCom), 7 maja 2012 r., https://arxiv.org/pdf/1107.4524.pdf [dostęp: 13 listopada 2017 r.].

107 C. Chen, *Microsoft Now Accepts Bitcoin Through BitPay*, CryptoCoins News, https://www.cryptocoinsnews.com/microsoft-now-accepts-bitcoin-bitpay [dostęp: 17 października 2017 r.].

108 N. Sardesai, *PayPal Partners with BitPay, Coinbase, and GoCoin*, CryptoCoins News, https://www.cryptocoinsnews.com/paypal-partners-with-bitpay-coinbase-and-gocoin [dostęp: 17 października 2017 r.].

109 M. Flacy, Dell, *Newegg start accepting Bitcoin as payment*, Digital Trends, https://www.digitaltrends.com/web/dell-newegg-start-accepting-bitcoin-payment/#!bv9oFm [dostęp: 17 października 2017 r.].

110 M. Parker, *Steam accepts bitcoin with BitPay*, BraveNewCoin, https://bravenewcoin.com/news/steam-accepts-bitcoin-with-bitpay [dostęp: 17 października 2017 r.].

111 P. Rizzo, *Time Inc Becomes First Major Magazine Publisher to Accept Bitcoin*, CoinDesk, https://www.coindesk.com/time-inc-becomes-first-major-magazine-publisher-accept-bitcoin [dostęp: 17 października 2017 r.].

112 G. MacDougall, *Mozilla Now Accepts Bitcoin*, Mozilla,org, https://blog.mozilla.org/blog/2014/11/20/mozilla-now-accepts-bitcoin [dostęp: 17 października 2017 r.].

113 L. Gruwell, *Wikimedia Foundation Now Accepts Bitcoin*, Wikimedia.org, https://blog.wikimedia.org/2014/07/30/wikimedia-foundation-now-accepts-bitcoin [dostęp: 17 października 2017 r.].

114 A. Skelton, *Pay Another Way: Bitcoin*, https://en.blog.wordpress.com/2012/11/15/pay-another-way-bitcoin, [dostęp: 17 października 2017 r.].

115 http://www.coinmap.org/#/world/21.53484700/-27.94921875/3, [dostęp: 17 października 2017 r.].

Więcej możliwości uzyskujemy działając przez Internet. Bitcoinem możemy opłacić rachunki, doładować telefon czy zapłacić za dowolne zakupy w sklepie internetowym[116]. Aby zapłacić bitcoinem stacjonarnie należy posiadać na swoim telefonie portfel mobilny z zdeponowanymi na nim środkami. Następnie zeskanować kod QR, który udostępni nam pracownik miejsca, w którym dokonujemy zakupu towaru lub usługi. Pierwszą informację o dokonaniu transakcji otrzymujemy w ciągu kilku sekund.

Jednak od pewnego czasu nie jest to atrakcyjna forma m.in. ze względu na rosnące koszty transakcyjne w Bitcoinie, a także wysokie koszty alternatywne związane z rosnącym kursem tej kryptowaluty (co zniechęca do wydawania go a zachęca – do trzymania).

„Potwierdzenia to nic innego jak 'akceptacja' całej sieci, że płatność jest poprawna. (...) w przypadku Bitcoina nie ma banku, który sprawdziłby poprawność transakcji. To sieć weryfikuje czy osoba wysyłająca bitcoiny rzeczywiście była w ich posiadaniu i czy na przykład nie spróbowała wysłać tych samych bitcoinów do dwóch osób jednocześnie. Oczekiwanie na dwa potwierdzenia trwa średnio 20 minut"[117]. Właśnie długość czasu oczekiwania na potwierdzenie jest jednym z minusów płatności bitcoinami w punktach stacjonarnych. Być może zmieni się to po wprowadzeniu Lightning Network, a może do celów płatności detalicznych zacznie być wykorzystywana inna kryptowaluta? Musimy jeszcze poczekać na upowszechnienie się tych rozwiązań.

Ważną wadą kryptowalut, a jednocześnie istotnym, jeśli nie kluczowym czynnikiem, który ogranicza rozwój kryptowalut oraz ich codziennego praktycznego wykorzystania jest problem regulacji. Kryptowaluty jako zjawisko bezprecedensowe. Środek płatniczy, który nie jest podobny do żadnego innego wcześniej znanego od momentu, gdy zaczął zyskiwać na popularności budził grozę i powodował zamieszanie, zarówno wśród przedsiębiorców (szczególnie księgowych) oraz urzędników. Urzędnicy pierwotnie uznali (w Polsce), że bitcoin jest towarem, a „płatność" nim oznacza wymianę towar za towar, czyli barter. Przed wyrokiem Trybunału Sprawiedliwości UE z 22 października 2015 r. uznawano, że sprzedaż bitcoinów jest opodatkowana podatkiem VAT. Obecnie obowiązuje w UE interpretacja, iż bitcoin powinien być traktowany jako alternatywny środek płatniczy i zwolniony z podatku VAT. Jednak w Polsce, pomijając wspomniany wcześniej komunikat NBP i KNF z lipca 2017 r., obrót ani księgowanie bitcoina nie są uregulowane (choć nie jest to zakazane).

Wadą można też nazwać uzależnienie od infrastruktury internetowej. Władze nie zawsze są w stanie przechwycić informacje przepływające w Internecie, jednak mają wpływ na ogólniejszą strukturę, w ramach której działa system – na Internet, a Bitcoin jest systemem

116 *Opłacaj rachunki i płać bitcoinami niemal, gdzie chcesz w polskim internecie. Ruszyła nowa usługa inpay.pl*, Bitcoin.pl, 12 sierpnia 2017 r., http://bitcoin.pl/wiadomosci/biznes/987-oplacaj-rachunki-i-plac-bitcoinami-gdzie-chcesz-ruszyla-nowa-usluga-inpay-pl [dostęp: 24 sierpnia 2017 r.].

117 *Ile trwa płatność Bitcoin?*, Bitbe.co, http://bitbe.co/bitcoin [dostęp: 19 lipca 2017 r.].

informatycznym, osadzonym w Internecie. Pozostają zależni od jego struktury i polityki dostawców internetowych[118].

Ponadto, jako że kryptowaluty do realnego zaistnienia wymagają zaangażowania podmiotów gospodarki realnej – musiały one do nich „wyjść" i zaoferować wymienialność na istniejące waluty. Problem polega na tym, że liczba połączeń gospodarki Bitcoina z gospodarkami realnymi jest ograniczona. Są one relatywnie łatwe do zidentyfikowania i możliwe do kontrolowania. Jako przedsięwzięcia w gospodarce realnej obracające oficjalnymi środkami pieniężnymi podlegają określonym prawom, nawet jeśli kwestie transferów pieniężnych nie zawsze są dobrze uregulowane[119].

Interwencje wpływające na kurs wciąż są możliwe przy niewielkich kapitałach (np. w ramach jednej, mniejszej giełdy), będących w zakresie nawet osób prywatnych.

Rynek kryptowalut wciąż jest w fazie rozwoju i codziennie powstają nowe waluty posiadające swoje charakterystyczne, wyróżniające je spośród innych cechy. Kryptowaluty będące już na rynku od lat stale ulegają zmianom, które usprawniają ich funkcjonowanie. Podobnie nieustannie zmieniają się uwarunkowania prawne prowadzenia działalności związanej z nimi. Mimo, że w tym momencie polskie władze są sceptycznie nastawione do usankcjonowania obrotu kryptowalutami, wciąż jest szansa, że to się zmieni.

118 G. Sobiecki, *Bitcoin: Globalna Alternatywna Waluta*, monografia pokonferencyjna XIII Międzynarodowa Konferencja Naukowa „Kryzys finansowy – przebieg i skutki społeczno-gospodarcze w Europie Środkowej i Wschodniej", 21-23 maja 2012 r., https://www.researchgate.net/publication/271474055_Bitcoin_globalna_alternatywna_waluta, [dostęp: 17 października 2017 r.].

119 Ibidem.

# 8. Jak zachować bezpieczeństwo kryptowalut?

Brak zaufanej trzeciej strony w relacjach pomiędzy użytkownikami kryptowalut jest niezaprzeczalnie przejawem wolności, jednakże stanowić może pewne niebezpieczeństwo dla niedoświadczonych użytkowników. Od nich samych zależy bowiem bezpieczeństwo dokonywanych transakcji. Sami muszą zatroszczyć się o to, aby przez błąd czy zaufanie nieodpowiedniej giełdzie nie utracić swoich środków. Gdy dokonujemy tradycyjnego przelewu bankowego przez Internet i pomylimy się w numerze konta adresata, kwocie przelewu – nie jest to wina banku, lecz nasza. Bank może nam jednak pomóc w naprawieniu naszego błędu. W przypadku kryptowalut, odpowiedzialność na posiadaczu środków jest jeszcze większa, bo nie ma tej „trzeciej strony" – banku, który mógłby pomóc w rozwiązaniu problemu. Istnieją jednak wolnorynkowe rozwiązania typu *escrow*, które umożliwiają – jeśli strony transakcji się zgodzą – uczestniczenie w transakcji pośrednika[120]. Zostały opracowane[121] lecz jeszcze nie wdrożone (są w fazie „final"[122], tj. przed implementacją i aktywowaniem) zmiany w samym protokole, umożliwiające warunkową akceptację i odroczenie akceptacji transakcji. Nieco inaczej jest w Ethereum – tam inteligentne umowy (ang. *smart contracts*) mogą pełnić tę rolę. Jest to

120 *Bitcointalk Escrows - Trade Safely!*, https://bitcointalk.org/index.php?topic=855778.0, [dostęp: 17 października 2017 r.].

121 Chodzi tu o BIP (Bitcoin Improvement Proposals) o numerach 65 i 112. Por. *BIP112 czyli escrow w praktyce i nie tylko*, Bitcoin.pl, 18 lutego 2016 r., http://bitcoin.pl/wiadomosci/techniczne/1145-bip112-czyli-escrow-w-praktyce-i-nie-tylko.

122 *Bitcoin Improvement Proposals*, Bitcoin.it, https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals, [dostęp: 17 października 2017 r.].

zresztą jedno z najczęściej wykorzystywanych zastosowań sieci Ethereum (używane w procesie ICO). Nie jest to jednak rozwiązanie wolne od wad, gdyż zdarzają się błędy w kodach takich umów i są one niekiedy bardzo kosztowne. Innym rozwiązaniem jest zbudowanie blockchaina od początku przewidującego rozwiązanie ww. problemów. Pracuje nad tym np. zespół EOS.

Jak wspomniano w rozdziale poświęconym portfelom, każdy z nich posiada inny stopień bezpieczeństwa. Trzeba dostosować ich wybór do swoich potrzeb, do tego jakie środki chcemy przechowywać na danym portfelu. Ważne jest również, jak wspomniano powyżej, jakie kryptowaluty chcemy przechowywać.

Kryptowaluty mimo tego, że są znacznie bezpieczniejsze od tradycyjnej bankowości elektronicznej (jeśli są dobrze zabezpieczane), tak jak każde inne aktywo są narażone na kradzież. Dlatego warto dbać o ich bezpieczeństwo.

Poniżej pokrótce przedstawione zostaną podstawowe zasady korzystania z portfeli i serwisów transakcyjnych.

- W przypadku przechowywania kryptowaluty na komputerze należy zainstalować program antywirusowy, skanować nim komputer regularnie oraz przeprowadzać aktualizacje oprogramowania. Jest to podstawowa zasada zwiększania bezpieczeństwa (również na telefonie).
- Używając aplikacji portfela należy ją zaszyfrować. Taka możliwość jest dostępna w każdej aplikacji. Hasło powinno być unikalne oraz posiadać znaki, cyfry i duże litery.
- Kopie portfela z kluczami prywatnymi należy trzymać w bezpiecznym miejscu, takim jak płyta DVD albo pendrive.
- Logowanie się z bezpiecznych sieci Wi-Fi jest również elementarną zasadą bezpieczeństwa naszych środków.
- Należy robić kopie zapasowe (ang. *backup*) portfela i trzymać je poza urządzeniem.

Trzymanie środków w serwisach transakcyjnych jest praktyczne i wygodne. Jednak przy takim przetrzymywaniu środków nasze bezpieczeństwo zależy od osób trzecich. Warto korzystać z serwisów, które cieszą się zaufaniem oraz unikać przechowywania w nich dużych kwot.

- Korzystanie w serwisach transakcyjnych z dodatkowej weryfikacji np. za pomocą telefonu, znacząco zwiększa nasze bezpieczeństwo.
- Należy logować się w domenach, w których transmisja jest szyfrowana za pomocą SSL.
- Warto sprawdzić nazwę domeny, gdyż strona, na którą się wejdzie może wyglądać łudząco podobnie do tej, do której rzeczywiście chcemy się zalogować. Są przestępcy, którzy specjalizują się w kopiowaniu stron (np. prowadzących ICO) i stawianiu ich na domenach, które w nazwie nieznacznie (np. jedną literą) różnią się od oryginału.
- Należy posiadać różne hasła do serwisów transakcyjnych.
- Nigdy nie powinno się zapisywać hasła do serwisów w przeglądarce oraz powinno się wylogowywać z niej po zakończeniu pracy.
- Do różnych kryptowalut są dedykowane portfele (niektóre z nich obsługują więcej kryptowalut). Przelanie środków na portfel innej waluty powoduje ich utracenie.

Kupno i sprzedaż kryptowalut poza internetowymi giełdami wymiany:

- Odradza się handlu bitcoinami w Internecie poza sprawdzonymi giełdami wymiany.
- Nie należy dokonywać transakcji z kimś, kto z własnej inicjatywy podejmuje próbę kontaktu i oferuje cenę znacząco odbiegającą od rynkowej. Nawet jeżeli wymiana dojdzie do skutku może ona być powiązana z zainfekowaniem komputera lub z przekazaniem „brudnych" pieniędzy.
- Decydując się jednak na wymianę pozagiełdową należy sprawdzić reputację sprzedawcy / nabywcy (nie na jego własnej stronie internetowej, ale u osób trzecich). Przy ocenie reputacji warto zwrócić uwagę na datę zarejestrowania użytkownika na danym forum, liczbę postów oraz ewentualne komentarze dotyczące już dokonanych transakcji.

# 9. Podsumowanie

Kryptowaluty są nowym zjawiskiem w sferze finansów. Są one w dużej mierze podobne do pieniędzy, których używamy na co dzień w formie elektronicznej[123]. W niektórych krajach główna z kryptowalut – bitcoin – została uznana za pełnoprawny środek płatniczy. W innych krajach władze podchodzą do nich w sposób bardziej sceptyczny. Niektóre z kryptowalut, np. bitcoin – spełniają już podstawowe funkcje pieniądza (trwałość, poręczność, oryginalność, podzielność, miernik wartości, środek wymiany, funkcja tezauryzacyjna).

Od strony prawnej kryptowaluty są traktowane jako inny niż pieniądz miernik wartości. Należy pamiętać, iż przychody uzyskane ze sprzedaży kryptowalut podlegają opodatkowaniu.

W związku z ich dynamicznie rosnącą popularnością może wystąpić zjawisko bańki spekulacyjnej, która powoduje – zwłaszcza wśród regulatorów rynku finansowego – być może nadmierne obawy, zwłaszcza biorąc pod uwagę konsekwencje rozwoju technologii w tzw. długim okresie.

Kryptowaluty mylnie porównywane są z piramidami finansowymi. Miano to należałoby używać w stosunku do pseudo-kryptowalut, czyli takich, które jedynie podszywają się pod kryptowaluty wykorzystując ich popularność (i rosnącą wartość), podczas gdy stworzone zostały w celu wyłudzenia pieniędzy od inwestorów. Prawdziwe kryptowaluty oparte są na otwartym kodzie źródłowym z jasno określonymi algorytmami i zasadami funkcjonowania oraz bez centralnego emitenta, który zarabiałby na ich sprzedaży. Jest w wśród nich prawdziwa demokracja, bo opierają się na systemach zdecentralizowanych, rozproszonych.

Integralną częścią kryptowalut jest technologia łańcucha bloków, tj. blockchain. Zapewnia ona transparentność, bezpieczeństwo oraz niepodważalność transakcji na niej opartych. Blockchain pełni funkcję księgi rozrachunkowej z tą różnicą, że aby sfałszować dane sprzed np. kilku miesięcy konieczne będzie sfałszowanie wszystkich bloków transakcji, które od tamtego czasu powstały. W przypadku największych blockchainów (np. bitcoinowego) zadanie to jest praktycznie niemożliwe.

Niniejsze opracowanie zawiera szereg porad o charakterze praktycznym. Ze względu na to, że bardzo duża część użytkowników technologii blockchain to osoby zajmujące się inwestowaniem w kryptowaluty, stąd autorzy opisali podstawy również tego zagadnienia.

Inwestowanie (każde, nie tylko w kryptowaluty) powinno być poprzedzone edukacją. Generalna zasada – nie inwestuje się w rzeczy, których się nie rozumie – obowiązuje szczególnie w zakresie walut cyfrowych, które są trudne do pojęcia.

123 G. Sobiecki (2011), *Czy bitcoiny mają wartość*, wpis na blogu Katedry Zarządzania Wartością SGH, 1 września 2011 r., http://www.valuecomesfirst.pl/bitcoiny/; G. Sobiecki (2014), *Walut światy równoległe*, „Kwartalnik Nauk o Przedsiębiorstwie" 4 / 2014, s. 5-17, https://www.researchgate.net/profile/Grzegorz_Sobiecki/publication/271473114_Walut_swiaty_rownolegle/links/54c8bad60cf289f0ced0c2e4/Walut-swiaty-rownolegle.pdf.

Inwestowanie w kryptowaluty można podzielić na krótkoterminowe oraz długoterminowe. Pierwsze oparte jest na wysokiej zmienności kursów oraz wymaga dużego zaangażowania inwestora (codzienne śledzenie kursów oraz wydarzeń). Inwestowanie długoterminowe wiąże się z zamrożeniem środków na długi okres (w slangu społeczności kryptowalutowej mówi się o tej strategii – „hodl", od słowa „hold" – trzymaj).

Początek inwestowania w kryptowaluty polega na ich nabyciu – najczęściej i najbezpieczniej za pomocą zaufanych giełd. Aktualnie przy rejestracji na giełdach wymagana jest weryfikacja użytkownika w celu zabezpieczenia przed działalnością przestępczą.

Szczególna uwaga powinna być skierowana na zabezpieczenie kont oraz portfeli. Kryptowaluty nie powinny być przez dłuższy czas trzymane na giełdach, a jeśli już – zaleca się wykorzystanie m.in. weryfikacji dwuczynnikowej (2FA). Bezpieczniejsze jest wykorzystanie portfeli sprzętowych i trzymanie kluczy prywatnych na urządzeniach nie podłączonych do Internetu.

Poza inwestowaniem w same kryptowaluty możliwa jest inwestycja w ICO, które jest formą crowdfundingu opartą na blockchainie lub polega na sprzedaży tokenów (*utility tokens*). Zjawisko to nie zostało szerzej rozwinięte w opracowaniu – inwestowanie w ICO wymaga jeszcze większej ostrożności i wiedzy technicznej.

Rosnąca popularność kryptowalut spowodowała również rozwój przestępstw kryptowalutowych. Dlatego należy zachować szczególną ostrożność podczas inwestowania i stosować do wspomnianych w poradniku zasad. Nie wyczerpują one kompletu potrzebnej użytkownikom walut cyfrowych i inwestorów wiedzy. Postęp techniczny jest na tyle duży, że warto być na bieżąco z różnymi źródłami informacji: czytać, uczyć się, brać udział w seminariach, meetupach i konferencjach.

Do zobaczenia!

# 10. Bibliografia


Adamowicz A., Zacharski M., *Analiza wybranych giełd kryptowalutowych w Polsce*, Uczelnia Łazarskiego – Centrum Technologii Blockchain, http://www.lazarski.pl/pl/wydzialy-i-jednostki/instytuty/wydzial-ekonomii-i-zarzadzania/centrum-technologii-blockchain/analiza-wybranych-gield-kryptowalutowych-w-polsce, [dostęp: 24 sierpnia 2017 r.].

Amos H., *Russia Is Becoming a Cryptocurrency Haven*, The Moscow Times, 9 lipca 2017 r., https://themoscowtimes.com/articles/russia-is-becoming-a-cryptocurrency-haven-58175, [dostęp: 13 listopada 2017 r.].

*Analiza fundamentalna*, Narodowy Bank Polski – Portal Edukacji Ekonomicznej, https://www.nbportal.pl/slownik/pozycje-slownika/analiza-fundamentalna, [dostęp: 19 lipca 2017 r.].

*Analiza Techniczna*, Edukacja Giełdowa, https://www.edukacjagieldowa.pl/gieldowe-abc/analiza-techniczna, [dostęp: 19 lipca 2017 r.].

Azarko U., Yakauleu U., *Przegląd kilku wybranych giełd kryptowalutowych*, Uczelnia Łazarskiego – Centrum Technologii Blockchain, http://www.lazarski.pl/pl/wydzialy-i-jednostki/instytuty/wydzial-ekonomii-i-zarzadzania/centrum-technologii-blockchain/przeglad-kilku-wybranych-gield-kryptowalutowych, [dostęp: 24 sierpnia 2017 r.].

Bala S., Kopyściański T., W. Srokosz, *Kryptowaluty jako elektroniczne instrumenty płatnicze bez emitenta*. *Aspekty informatyczne, ekonomiczne i prawne*, Uniwersytet Wrocławski, Wrocław 2016, s. 107.

Bielecki r., *Analiza wybranych giełd kryptowalutowych na świecie*, Uczelnia Łazarskiego – Centrum Technologii Blockchain, http://www.lazarski.pl/pl/wydzialy-i-jednostki/instytuty/wydzial-ekonomii-i-zarzadzania/centrum-technologii-blockchain/analiza-wybranych-gield-kryptowalutowych-na-swiecie, [dostęp: 24 sierpnia 2017 r.].

BIP (Bitcoin Improvement Proposals) o numerach 65 i 112. Por. *BIP112 czyli escrow w praktyce i nie tylko*, Bitcoin.pl, 18 lutego 2016 r., http://bitcoin.pl/wiadomosci/techniczne/1145-bip112-czyli-escrow-w-praktyce-i-nie-tylko, [dostęp: 13 listopada 2017 r.].

*Bitcoin Improvement Proposals*, Bitcoin.it, https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals, [dostęp: 17 października 2017 r.].

*Bitcoin Transactions Aren't as Anonymous as Everyone Hoped*, MIT Technology Review, 23 sierpnia 2017 r., https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped, [dostęp: 13 listopada 2017 r.].

Bubiel A., *Bitcoin – determinanty i skutki jego akceptacji przez przedsiębiorstwa*, rozprawa doktorska, Kolegium Nauk o Przedsiębiorstwie Szkoły Głównej Handlowej w Warszawie, Warszawa 2017. Rozprawa ta (zawierająca ww. dowód na to, że bitcoin nie jest piramidą finansową) 25 października 2017 r. została obroniona z wyróżnieniem.

Buterin V., *The Meaning of Decentralization*, Medium, 6 lutego 2017 r., https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274, [dostęp: 24.08.2017].

*Cechy pieniądza*, Narodowy Bank Polski – Portal Wiedzy Ekonomicznej, https://www.nbportal.pl/wiedza/prezentacje/nowe-prezentacje/cechy-pieniadza, [dostęp: 17 lipca 2017 r.].

Chainalysis, www.chainalysis.com, [dostęp: 4 września 2017 r.].

Chen C., *Microsoft Now Accepts Bitcoin Through BitPay*, CryptoCoins News, https://www.cryptocoinsnews.com/microsoft-now-accepts-bitcoin-bitpay, [dostęp: 17 października 2017 r.].

Chen L., Nakamura Y., *Cryptocurrency Cyber Crime Has Cost Victims Millions This Year*, Bloomberg, www.bloomberg.com/news/articles/2017-08-24/cyber-criminals-extracting-a-heavy-toll-from-ethereum-advocates, [dostęp: 4 września 2017 r.].

Cohen R., *Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined!*, Forbes, 28 listopada 2013 r., https://www.forbes.com/sites/reuvencohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/#28f8da4d6e5e, [dostęp: 13 listopada 2017 r.].

*Cryptocurrency ICO Stats 2017*, CoinSchedule, https://www.coinschedule.com/stats.php, [dostęp: 16 października 2017 r.].

Cryptocurrency statistics, https://bitinfocharts.com, [dostęp: 12 listopada 2017 r.].

del Castillo M., *Vladimir Putin and Vitalik Buterin Discuss Ethereum 'Opportunities'*, CoinDesk, 5 czerwca 2017 r., http://www.coindesk.com/vladimir-putin-vitalik-buterin-discuss-ethereum-opportunities-recent-forum, [dostęp: 13 listopada 2017 r.].

Druś M., *Rekordowe wpływy start-upów z ICO*, „Puls Biznesu", 18 lipca 2017 r., https://www.pb.pl/rekordowe-wplywy-start-upow-z-ico-866648, [dostęp: 13 listopada 2017 r.].

Dudek P. M., *Waluta bitcoin – glosa do wyroku Trybunału Sprawiedliwości z 22.10.2015 r. w sprawie C-264/14 Skatteverket przeciwko Davidowi Hedqvistowi*, „Europejski Przegląd Sądowy", czerwiec 2016 r., s. 43.

Dziembowski S., Faust S., Kolmogorov V., Pietrzak K., *Proofs of space*

Gennaro, M. Robshaw (eds.), *Advances in Cryptology – CRYPTO 2015*, Springer, Heidelberg 2015, str. 585-605.

Dziubak P., *KNF i NBP są zbyt konserwatywne w sprawie kryptowalut. Posłanka PO staje w obronie bitcoina*, Cashless.pl, 12 lipca 2017 r., https://www.cashless.pl/temat-dnia/2825-poslanka-nykiel-nbp-i-knf-sa-zbyt-konserwatywne-w-sprawie-kryptowalut, [dostęp: 13 listopada 2017 r.].

*Economic majority*, Wikipedia, https://en.bitcoin.it/wiki/Economic_majority; https://en.bitcoin.it/wiki/Bitcoin_is_not_ruled_by_miners, [dostęp:16.10.2017].

*Europol hosted 4th conference on virtual currencies*, 5 lipca 2017 r., www.europol.europa.eu/newsroom/news/europol-hosted-4th-conference-virtual-currencies, [dostęp: 13 listopada 2017 r.].

Financial Services Agency, 24 marca 2017 r., http://www.fsa.go.jp/news/28/ginkou/20170324-1.html, [dostęp: 13 listopada 2017 r.].

*Firmy Blockchain zebrały 2,4 razy więcej środków z ICO niż inwestycje VC*, Cryptonews, 5 maja 2017 r., https://cryptonews.pl/firmy-blockchain-zebraly-24-razy-wiecej-srodkow-ico-niz-inwestycji-vc, [dostęp: 13 listopada 2017 r.].

Flacy M., Dell, *Newegg start accepting Bitcoin as payment*, Digital Trends, https://www.digitaltrends.com/web/dell-newegg-start-accepting-bitcoin-payment/#!bv9oFm, [dostęp: 17 października 2017 r.].

Galeon D. J., *Dubai just got its first official cryptocurrency*, Business Insider, 2 października 2017 r., http://www.businessinsider.com/dubai-official-cryptocurrency-blockchain-emcash-2017-10?IR=T, [dostęp: 13 listopada 2017 r.].

Gileman G., Rauchs M., *Global cryptocurrency benchmarking study*, Cambridge University, 2017, s. 93.

Gruwell L., *Wikimedia Foundation Now Accepts Bitcoin*, Wikimedia.org, https://blog.wikimedia.org/2014/07/30/wikimedia-foundation-now-accepts-bitcoin, [dostęp: 17 października 2017 r.].

Heller D., Directorate-General for Internal Policies. Policy Department A. Economic and Scientific Policy, *The Implications of Digital Currencies for Monetary Policy. Monetary Dialogue*, Maj 2017, http://www.europarl.europa.eu/cmsdata/118907/PIIE_FINAL%20upload.pdf, s. 9, [dostęp: 13 listopada 2017 r.].

Helms K., *Europol Discusses Bitcoin as Store of Value and Payment Method With the Industry*, Bitcoin.com, 6 lipca 2017 r., https://news.bitcoin.com/europol-bitcoin-store-of-value-legitimate-payment-method, [dostęp: 13 listopada 2017 r.].

Hertig A., *Calm Before the Fork? Segwit2x Goes Silent as Bitcoin Split Looms*, CoinDesk, https://www.coindesk.com/calm-fork-segwit2x-goes-silent-bitcoin-spilt-looms, [dostęp: 16 października 2017 r.].

Homa D., *Sekrety Bitcoina i innych kryptowalut*, Helion, Gliwice 2015, s. 165.;

http://www.coinmap.org/#/world/21.53484700/-27.94921875/3, [dostęp: 17 października 2017 r.].

https://www.cashless.pl/felietony/2831-prezes-nbp-chyba-woli-gotowke-bank-centralny-wystapil-z-organizacji-promujacej-rozwoj-obrotu-bezgotowkowego-w-polsce, [dostęp: 13 listopada 2017 r.].

*Ile trwa płatność Bitcoin?*, Bitbe.co, http://bitbe.co/bitcoin, [dostęp: 19 lipca 2017 r.].

*INTERPOL backs World Economic Forum cybercrime project*, Interpol, 22 stycznia 2016 r., https://www.interpol.int/News-and-media/News/2016/N2016-010, [dostęp: 13 listopada 2017 r.].

Interpretacja Indywidualna, syg.: 2461-IBPB-2-2.4511.12.2017.2.BF, 03.04.2017, http://sip.mf.gov.pl/faces/views/szczegoly/szczegoly-interpretacji-indywidualnej.xhtml?dokumentId=502729&poziomDostepu=PUB&indexAccordionPanel=-1#tresc, [dostęp: 24 sierpnia 2017 r.].

Interpretacja Indywidualna, syg.: IPPB1/415-276/14-4/EC, 26.06.2014, http://sip.mf.gov.pl/faces/views/szczegoly/szczegoly-interpretacji-indywidualnej.xhtml?dokumentId=394395&poziomDostepu=PUB&indexAccordionPanel=-1#tresc, [dostęp: 28 sierpnia 2017 r.].

Interpretacja Indywidualna, syg.: IPPB2/415-842/13-2/MK, 25.02.2014, http://sip.mf.gov.pl/faces/views/szczegoly/szczegoly-interpretacji-indywidualnej.xhtml?dokumentId=382095&poziomDostepu=PUB&indexAccordionPanel=-1#tresc, [dostęp: 25 sierpnia 2017 r.].

JaiChai, *Is Cryptocurrency Real Money? Brief Discussion on Major Issues Surrounding Debate*, Cointelegraph, 22 sierpnia 2017 r., https://cointelegraph.com/news/is-cryptocurrency-real-money-brief-discussion-on-major-issues-surrounding-debate, [dostęp: 13 listopada 2017 r.].

Kiesnowski K., *The Top 10 US Companies by Market Capitalization*, CNBC.com, updated: 27 October 2017, https://www.cnbc.com/2017/03/08/the-top-10-us-companies-by-market-capitalization.html, [dostęp: 13 listopada 2017 r.].

Komisja Gospodarcza i Monetarna, *Sprawozdanie w sprawie wirtualnych walut*, 3 maja 2016 r., http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2016-0168+0+DOC+XML+V0//PL, [dostęp: 13 listopada 2017 r.].

*Komunikat Narodowego Banku Polskiego i Komisji Nadzoru Finansowego w sprawie „walut" wirtualnych*, Narodowy Bank Polski, 7 lipca 2017 r., http://www.nbp.pl/home.aspx?f=/aktualnosci/wiadomosci_2017/ww-pl.html, [dostęp: 13 listopada 2017 r.].

Kotucha A., *Bitcoin nie jest prawem*, 29 października 2017 r., http://schiffersroczynski.pl/blog/399-bitcoin-nie-jest-prawem, [dostęp: 13 listopada 2017 r.].

Kowalewski P., *Pieniądz i jego znaczenia*, Narodowy Bank Polski – Portal Wiedzy Ekonomicznej, https://www.nbportal.pl/wiedza/artykuly/pieniadz/pieniadz-i-jego-znaczenia, [dostęp: 17 lipca 2017 r.].

Kwiatek W., Fragment wykładu: *Czym się różnią kryptowaluty od pseudowalut*, https://www.wykop.pl/link/3951739/fragment-wykladu-wojciecha-kwiatka-czym-sie-roznia-kryptowaluty-od-pseudowalut, [dostęp: 16 października 2017 r.].

Large Bitcoin Collider, https://lbc.cryptoguru.org, [dostęp: 17 października 2017 r.].

Lendzion-Stachera E., *Rozłamy w sieciach blockchain*, Uczelnia Łazarskiego, https://www.lazarski.pl/pl/wydzialy-i-jednostki/instytuty/wydzial-ekonomii-i-zarzadzania/centrum-technologii-blockchain/rozlamy-w-sieciach-blockchain, [dostęp: 24 sierpnia 2017 r.].

*Lightning Network*, https://lightning.network, [dostęp: 17 października 2017 r.].

*Bitcointalk Escrows - Trade Safely!*, https://bitcointalk.org/index.php?topic=855778.0, [dostęp: 17 października 2017 r.]."

Lujan S., *Is Bitcoin as Risk as Google and IBM Aim for 50-Qubit Quantum Computers?*, Bitcoin.com, 30 kwietnia 2017 r., https://news.bitcoin.com/is-bitcoin-at-risk-as-google-and-ibm-aim-for-50-qubit-quantum-computers, [dostęp: 24 sierpnia 2017 r.].

MacDougall G., *Mozilla Now Accepts Bitcoin*, Mozilla,org, https://blog.mozilla.org/blog/2014/11/20/mozilla-now-accepts-bitcoin, [dostęp: 17 października 2017 r.].

*Matematyka kryjąca się za Bitcoin*, Krypto Polonia, 25 marca 2015 r., http://kryptopolonia.info/matematyka-kryjaca-sie-za-bitcoin, [dostęp: 12 listopada 2017 r.].

Meiklejohn S., M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. Voelker, S. Savage, *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, University of California – San Diego, https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf, [dostęp: 12 listopada 2017 r.].

Memoria F., *Hacker Nets over $500,000 after Hacking Enigma before ICO Date*, Cryptocoins News, 21 sierpnia 2017 r., https://www.cryptocoinsnews.com/hacker-nets-over-500000-after-hacking-enigma-before-its-ico-date, [dostęp: 13 listopada 2017 r.].

Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin.org, https://bitcoin.org/bitcoin.pdf, [dostęp: 13 listopada 2017 r.].

Olszański M., Piech K. (red.), *E-biznes – innowacje w usługach. Teoria, praktyka, przykłady*, PARP, Warszawa 2012 (też: https://www.parp.gov.pl/images/PARP_publications/pdf/20506.pdf).

Opitek P., *Przestępczość z wykorzystaniem kryptowalut oraz ich status w postępowaniu karnym*, referat wygłoszony na międzynarodowej konferencji naukowej „Techniczne aspekty przestępczości teleinformatycznej", Instytut Kościuszki, Szczytno, 14 czerwca2017 r.

*Opłacaj rachunki i płać bitcoinami niemal, gdzie chcesz w polskim internecie. Ruszyła nowa usługa inpay.pl*, Bitcoin.pl, 12 sierpnia 2017 r., http://bitcoin.pl/wiadomosci/biznes/987-oplacaj-rachunki-i-plac-bitcoinami-gdzie-chcesz-ruszyla-nowa-usluga-inpay-pl, [dostęp: 24 sierpnia 2017 r.].

Parker L., *Bitcoin regulation overhaul in Japan*, 1 April 2017, Brave New Coin – Digital Currency Insights, https://bravenewcoin.com/news/bitcoin-regulation-overhaul-in-japan, [dostęp: 13 listopada 2017 r.].

Parker M., *Steam accepts bitcoin with BitPay*, BraveNewCoin, https://bravenewcoin.com/news/steam-accepts-bitcoin-with-bitpay, [dostęp: 17 października 2017 r.].

Piech K. (red.), *Leksykon pojęć na temat technologii blockchain i kryptowalut*, Strumień „Blockchain i kryptowaluty", Ministerstwo Cyfryzacji, 8 listopada 2016 r., https://www.gov.pl/documents/31305/0/leksykon_pojec_na_temat_technologii_blockchain_i_kryptowalut.pdf, [dostęp: 13 listopada 2017 r.].

Piech K., *O upadkach giełd bitcoinowych – ciąg dalszy*, http://piech.blog.pl/2016/10/25/o-upadkach-gield-bitcoinowych-ciag-dalszy, [dostęp: 24 sierpnia 2017 r.].

*Pieniądz fiducjarny*, Narodowy Bank Polski, https://www.nbportal.pl/slownik/pozycje-slownika/pieniadz-fiducjarny, [dostęp: 17 lipca 2017 r.].

*Predicting bitcoin fees for transactions*, Bitcoinfees, https://bitcoinfees.21.co, [dostęp: 13 listopada 2017 r.].

*Problem bizantyjskich generałów*, Wikipedia, https://pl.wikipedia.org/wiki/Problem_bizantyjskich_genera%C5%82%C3%B3w, [dostęp 19 lipca 2017 r.].

Reid F., Harrigan M., *An Analysis of Anonymity in the Bitcoin System*, Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third International Conference on Social Computing (SocialCom), 7 maja 2012 r., https://arxiv.org/pdf/1107.4524.pdf, [dostęp: 13 listopada 2017 r.].

Reiff N., *Criminals Are Too Stupid to Use Cryptocurrency: EU Report*, Investopedia, 12 lipca 2017 r., http://www.investopedia.com/news/criminals-are-too-stupid-use-cryptocurrency-eu-report, [dostęp: 13 listopada 2017 r.].

*Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations*, Council of the European Union, 4 lipca 2017 r., http://europeanmemoranda.cabinetoffice.gov.uk/files/2017/07/10977-17-ADD-2.pdf, s. 87, [dostęp: 13 listopada 2017 r.].

Rizzo P., *Federal Agents Face Arrest for Alleged Silk Road Bitcoin Theft*, CoinDesk, 30 marca 2015 r., https://www.coindesk.com/federal-agents-face-arrest-for-alleged-silk-road-bitcoin-theft, [dostęp: 13 listopada 2017 r.].

Rizzo P., *Time Inc Becomes First Major Magazine Publisher to Accept Bitcoin*, CoinDesk, https://www.coindesk.com/time-inc-becomes-first-major-magazine-publisher-accept-bitcoin, [dostęp: 17 października 2017 r.].

Rosenblatt S., Cipriani J., *Two-factor authentication: What you need to know (FAQ)*, CNET, 15 czerwca 2015 r., https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq, [dostęp: 13 listopada 2017 r.].

Sanak B., Kurowski T., *Konsensus w sieci blockchain - czym jest i jak go osiągnąć?*, FXMag, 11 sierpnia 2017 r., https://www.fxmag.pl/artykul/konsensus-w-sieci-blockchain-czym-jest-i-jak-go-osign, [dostęp: 13 listopada 2017 r.].

Sardesai N., *PayPal Partners with BitPay, Coinbase, and GoCoin*, CryptoCoins News, https://www.cryptocoinsnews.com/paypal-partners-with-bitpay-coinbase-and-gocoin, [dostęp: 17 października 2017 r.].

Schwab K., *The Fourth Industrial Revolution*, World Economic Forum, 2016.

Secretary-General of the European Commission, "Commission Staff Working Document" Accompanying the document: Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundeirng and terrorist financing affecting the internal market and relating to cross-border situations, Bruksela, 4 lipca 2017 r., http://europeanmemoranda.cabinetoffice.gov.uk/files/2017/07/10977-17-ADD-2.pdf, [dostęp: 13 listopada 2017 r.].

Skelton A., *Pay Another Way: Bitcoin*, https://en.blog.wordpress.com/2012/11/15/pay-another-way-bitcoin, [dostęp: 17 października 2017 r.].

Smith K., *History of the Dot-Com Bubble Burst and How to Avoid Another*, Money Crashers, https://www.moneycrashers.com/dot-com-bubble-burst, [dostęp:30.10.2017].

Sobiecki G. (2011), *Czy bitcoiny mają wartość*, wpis na blogu Katedry Zarządzania Wartością SGH, 1 września 2011 r., http://www.valuecomesfirst.pl/bitcoiny/.

Sobiecki G. (2014), *Walut światy równoległe*, „Kwartalnik Nauk o Przedsiębiorstwie" 4 / 2014, s. 5-17, [dostęp: 13 listopada 2017 r.]."

Sobiecki G., *Bitcoin: Globalna Alternatywna Waluta*, monografia pokonferencyjna XIII Międzynarodowa Konferencja Naukowa „Kryzys finansowy – przebieg i skutki społeczno-gospodarcze w Europie Środkowej i Wschodniej", 21-23 maja 2012 r., https://www.researchgate.net/publication/271474055_Bitcoin_globalna_alternatywna_waluta, [dostęp: 17 października 2017 r.].

Staśkiewicz T., *Polscy programiści jednymi z najlepszych na świecie. Jest nawet kategoria, w której wygrywamy*, INNPoland, 31 sierpnia 2016 r., http://innpoland.pl/129313,polscy-programisci-docenieni-w-rankingu-hackerrank-jest-kategoria-w-ktorej-jestesmy-najlepsi-na-swiecie; J. Kuźniak, *Polscy programiści coraz częściej zostawiają w tyle dotychczasowych liderów*, Forsal.pl, 14 grudnia 2013 r., http://forsal.pl/artykuly/764634,polscy-programisci-coraz-czesciej-zostawiaja-w-tyle-dotychczasowych-liderow.html, [dostęp: 13 listopada 2017 r.].

*Strumień Blockchain/DLT i Waluty Cyfrowe*, Ministerstwo Cyfryzacji, https://www.gov.pl/cyfryzacja/strumien-blockchain/dlt-i-waluty-cyfrowe, [dostęp: 9 listopada 2017 r.].

Sygnatariusze „Kanonu dobrych praktyk podmiotów rynku kryptowalutowego w Polsce", Ministerstwo Cyfryzacji – Strumień „Blockchain / DLT i Waluty Cyfrowe", https://www.gov.pl/documents/31305/0/signatories_2.11.2017.pdf, [dostęp: 12 listopada 2017 r.].

Tether, https://tether.to, [dostęp: 13 października 2017 r.].

Tyra J. M., *Triple Entry Bookkeeping With Bitcoin*, "Bitcoin Magazine", 10 lutego 2014 r., https://bitcoinmagazine.com/articles/triple-entry-bookkeeping-bitcoin-1392069656.

Uryniuk J., *Prezes NBP chyba woli gotówkę. Bank centralny wystąpił z organizacji promującej rozwój obrotu bezgotówkowego w Polsce*, Cashless.pl, 16 lipca 2017 r.,

*Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, Dz.U. 2000 Nr 116 poz. 1216.

Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (Dz.U. z 2016 r. poz. 2032).

Ward T., *China Becomes First Country in the World to Test a National Cryptocurrency*, Futurism, 23 czerwca 2017 r., https://futurism.com/china-becomes-first-countrchina-becomes-first-country-in-the-world-to-test-a-national-cryptocurrencyy-to-test-national-cryptocurrency.

Wilk J., *Prezes NBP chętnie wprowadziłby zakaz dla kryptowalut*, FXMag, 9 listopada 2017 r., https://www.fxmag.pl/artykul/prezes-nbp-chetnie-wprowadzilby-zakaz-dla-kryptowalut, [dostęp: 13 listopada 2017 r.].

www.coinmarketcap.com.

*Wydarzenia w historii Bitcoina (do 2017-07-17), subiektywne zestawienie + ICO + VC*, https://docs.google.com/spreadsheets/d/e/2PACX-1vRCddBDpqdYCrnz4_F9F3dCB9su51xKlKj6ViL5Mt5rW158N3ag5adNV1SxSbNwDIuDrVzr69u2YN_A/pubhtml#, [dostęp: 13 listopada 2017 r.].

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 22 października 2015 r. w sprawie wspólnego systemu podatku od wartości dodanej (VAT), dotyczący odpłatnego świadczenia usług – Transakcje wymiany wirtualnej waluty „bitcoin" na waluty tradycyjne, w sprawie Skatteverket przeciwko Davidowi Hedqvistowi, http://curia.europa.eu/juris/document/document.jsf?text=&docid=170305&pageIndex=0&doclang=PL&mode=req&dir=&occ=first&part=1&cid=757455, [dostęp: 13 listopada 2017 r.].

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 22 października 2015 r. C-264/14.

Zacharzewski K., *Bitcoin jako przedmiot stosunków prawa prywatnego*, „Monitor Prawniczy" 2014, nr 21, s. 1132-1139.

Zacharzewski K., *Nie taki bitcoin straszny*, „Rzeczpospolita", 14 lipca 2017, http://archiwum.rp.pl/artykul/1347938-Nie-taki-bitcoin-straszny.html, [dostęp: 13 listopada 2017 r.].

Zacharzewski K., Piech K. (red.), *Przegląd polskiego prawa w kontekście zastosowań technologii rozproszonych rejestrów oraz walut cyfrowych*, Ministerstwo Cyfryzacji – Strumień „Blockchain i Kryptowaluty", 19 stycznia 2017 r., https://www.gov.pl/documents/31305/52168/przeglad_polskiego_prawa_w_kontekscie_zastosowan_technologii_rozproszonych_rejestrow_oraz_walut_cyfrowych.pdf/, s. 12, [dostęp: 13 listopada 2017 r.].

Zacharzewski K., Piech K. (red.), *Przegląd polskiego prawa w kontekście zastosowań technologii rozproszonych rejestrów oraz walut cyfrowych*, Ministerstwo Cyfryzacji – Strumień „Blockchain i Kryptowaluty", 19 stycznia 2017 r., https://www.gov.pl/documents/31305/52168/przeglad_polskiego_prawa_w_kontekscie_zastosowan_technologii_rozproszonych_rejestrow_oraz_walut_cyfrowych.pdf, s. 13, [dostęp: 13 listopada 2017 r.].

Zacharzewski K., Piech K., Wilczyński L. (red.), *Kanon dobrych praktyk podmiotów rynku kryptowalutowego w Polsce*, Ministerstwo Cyfryzacji – Strumień „Blockchain / DLT i Waluty Cyfrowe", 10 kwietnia 2017 r., https://www.gov.pl/documents/31305/0/kanon_justowany.pdf, [dostęp: 13 listopada 2017 r.].

Zacharzewski K., *Praktyczne znaczenie bitcoina na wybranych obszarach prawa prywatnego*, „Monitor Prawniczy" 2015, nr 4, s. 187-195.

Zhao W., *$7 Million Lost in CoinDash ICO Hack*, CoinDesk, 17 lipca 2017 r., https://www.coindesk.com/7-million-ico-hack-results-coindash-refund-offer.

# 11. Spis wykresów

# 12. Patroni i sponsorzy

**Sponsor:**

POLSKIE STOWARZYSZENIE BITCOIN

**Patroni Honorowi:**

UNIWERSYTET MIKOŁAJA KOPERNIKA W TORUNIU
Wydział Prawa i Administracji

UCZELNIA ŁAZARSKIEGO ŁAZARSKI WARSZAWA
CENTRUM TECHNOLOGII BLOCKCHAIN

CYFROWA EKONOMIA BLOCKCHAIN I KRYPTOWALUTY

AKCELERATOR .tech

Bitcoin.pl