ISSN 2392-0300 „Civitas et Lex" 2019 / 3(23)
DOI 10.31648/cetl.4416

VARIA

Krzysztof Markowski

KRYPTOWALUTY. POWSTANIE – TYPOLOGIA – CHARAKTERYSTYKA

Wprowadzenie

Ciekawostki technologiczne powinny być śledzone przez ustawodawców, służby i urzędników, zwłaszcza kiedy zaczynają stanowić problem. W przypadku kryptowalut przeszkodą może być mała ilość publikacji w języku polskim i dlatego właśnie powstał ten artykuł. W pracy omówiona zostanie najważniejsza kryptowaluta oraz okoliczności jej powstania, a także kilka innych, które się wyróżniają popularnością.

Autor artykułu sięgnął po anglojęzyczne publikacje, a najważniejszą z nich jest książka napisana przez Andreasa Antonopoulosa. Z jego książki o bitcoinie zostały wybrane najważniejsze elementy, a następnie uproszczone z pomocą innych publikacji. Było to konieczne, ponieważ artykuł ma ograniczoną liczbę stron.

1. Powstanie pierwszej kryptowaluty

Upowszechnienie się kryptowalut może przypominać okres średniowiecza, kiedy władcy mieli możliwość dorobienia nowych monet, co powodowało spadek wartości pieniądza. Takie działanie najbardziej uderzało w kupców, którzy próbując coś zrobić z zaistniałą sytuacją, zaczęli tworzyć organizacje i gildie, aż w końcu stworzyli własną walutę, która była używana w całej Europie. Stworzyli więc mniej zależną walutę, która była naprawdę ich i nie była kontrolowana przez władcę[1].

Choć bitcoin powszechnie uważany jest za pierwszą kryptowalutę, to już wcześniej tworzono coś podobnego, choć bez sukcesów. W 1982 r. David Chaum miał pomysł na anonimowe przelewy, stworzył nawet swój koncept „Blind signatures for untraceable payments", a następnie opublikował go na wydziale informatyki Uniwersytetu Kalifornijskiego. Po kilku latach założył własną

Krzysztof Markowski – Uniwersytet Warmińsko-Mazurski w Olsztynie Filia w Ełku; e-mail: krmr@protonmail.com

[1] K. Kopańko, M. Kozłowski, *Bitcoin. Złoto XXI wieku*, Gliwice 2014, s. 125–126.

działalność. Wykorzystując swoje pomysły, stworzył elektroniczny system DigiCash umożliwiający przelewy między użytkownikami. Użytkownicy uruchomiali na komputerach oficjalny program, doładowywali konta za pomocą przelewów z banków, ale tylko tych, które wspierały ten system. Wysłana prawdziwa waluta po przetworzeniu przez system stawała się w programie „cyberdolarami". Jak zakładano, transakcje były anonimowe. System DigiCash był jednak scentralizowany, przez co podatny na ataki hakerskie. Firma Chauma miała zarabiać na licencjonowaniu technologii, ale już w 1998 r. zbankrutowała[2].

W 2008 r., kiedy trwał wielki kryzys finansowy, prezydent Bush podpisał ustawę o ratowaniu sektora finansowego, zwaną Planem Paulsona. Ustawa, zakładająca przeznaczenie na ten cel 700 mld dolarów pochodzących z podatków, uratowała kilku nieuczciwych bankierów, co nie spodobało się innym. Jednym z niezadowolonych był anonimowy człowiek przedstawiający się w Internecie jako Satoshi Nakamoto. Wykorzystując znaną w tamtych latach wiedzę, opracował wirtualną walutę, którą można przelewać bez pośredników, bez żadnych instytucji mogących sprawować kontrolę, a dodrukowanie pieniędzy było niemożliwe. Historia bitcoina[3] zaczyna się od opublikowania przez Satoshiego Nakamoto pod koniec 2008 r. dokumentu rozesłanego przez Internet zatytułowanego „Bitcoin: A Peer-to-Peer Electronic Cash System". Opisał w nim dokładnie zasady działania wirtualnej waluty zabezpieczonej przez kryptografię, z transakcjami zapisywanymi w blockchainie[4]. 8 stycznia 2009 r. anonimowy Nakamoto opublikował oprogramowanie bitcoina, ale blockchain kryptowaluty zaistniał 3 stycznia 2009 r. i właśnie ta data uznawana jest za narodziny BTC, ponieważ wtedy zatwierdzono pierwszy blok w blockchainie[5].

Blockchain bitcoina, nazywany również łańcuchem bloków, to w pełni rozproszony rejestr podzielony na bloki danych zabezpieczony kryptografią[6].

Należy pamiętać, że bitcoin to nie tylko blockchain, to także zbiór koncepcji, technologii, protokół, algorytm oraz sieć[7]. Całość przypomina internet, choć drugim internetem nie jest. Do przeglądania zwykłego internetu instalujemy przeglądarkę, wybór jest duży, a jeśli ktoś umie programować, może stworzyć własną. Podobnie jest z oprogramowaniem do obsługi kryptowaluty bitcoin – wszystko będzie działać, jeśli będzie zgodne z protokołem, który jest jawny.

---

[2] R. Pitta, *Requiem for a Bright Idea*, 1.11.1999, <https://www.forbes.com/ forbes/1999/1101/6411390a.html#873fdc4715f6>, dostęp: 22.04.2019.

[3] W Polsce przyjął się zapis „bitcoin" małą literą, z innymi kryptowalutami jest już inaczej.

[4] M. Kmita, *10 lat temu wybuchł kryzys finansowy. Wtedy też narodziła się idea Bitcoina*, 17.10.2018, <https://bithub.pl/opinie/10-lat-temu-wybuchl-kryzys-finansowy-wtedy-tez-narodzila-sie-idea-bitcoina/>, dostęp: 19.04.2019.

[5] D. Dziduch, *Bitcoin powstał dokładnie 10 lat temu, w ciągu dekady odmieniając oblicze rynków*, 03.01.2019, <https://www.fxmag.pl/artykul/bitcoin-genesis-block-10-lat>, dostęp: 19.04.2019.

[6] D. Drescher, *Blockchain. Podstawy technologii łańcucha bloków w 25 krokach*, tłum. L. Sielicki, Gliwice 2018, s. 41.

[7] A. M. Antonopoulos, *Bitcoin dla zaawansowanych. Programowanie z użyciem otwartego łańcucha bloków*, tłum. T. Walczak, Gliwice 2018, s. 31.

Bitcoin jest otwartoźródłowy, co oznacza, że każdy może poznać zasady jego działania w najmniejszym szczególe[8].

Bitcoin jest przełomowy, ponieważ zawiera w sobie nowatorskie zabezpieczenie przed podwójnym wydawaniem środków, które sprawdza się od dziesięciu lat, ponadto jego twórca nie ma większych praw w sieci niż reszta użytkowników. Odróżnia to tę kryptowalutę od wcześniejszych podobnych projektów, których twórcy dbali o to, by mieć dochód choćby z powodu bycia ich twórcami. Rozwiązano tu problem „bizantyjskich generałów", czyli wykrycie elementu, w tym przypadku węzła sieci, czyli jednego użytkownika, który celowo działa błędnie. Mogło to okazać się trudne, ponieważ użytkownicy sieci są sobie równi. Mimo że większość posiadaczy kryptowalut nie słyszała o tym problemie, to należy wiedzieć, że rozwiązanie go okazało się dużym przełomem, który doceniony zostaje po poznaniu szczegółów.

Kryptowaluta bitcoin jest zdecentralizowana, co oznacza, że nie ma jednego podmiotu, który będzie czuwał nad wykonywanymi transakcjami, nikt nie anuluje transakcji ani nie przejmie jakiegoś konta. Użytkownicy sieci łączą się z siecią bez pośredników. Każdy użytkownik sieci ma równe prawa, a blockchain istnieje w dziesiątkach tysięcy kopii. Awaria tysięcy komputerów odpowiedzialnych za zatwierdzanie transakcji nie spowoduje problemów, natomiast winne awarii zwykłego banku może być jedno urządzenie, pełniące ważną rolę[9].

Transakcje w złotówkach polegają na przekazaniu pieniędzy drugiej osobie, natomiast transakcje w BTC tak naprawdę są przekazaniem praw do monet, następuje to poprzez wpis w łańcuchu bloków, czym zajmują się „górnicy".

Waluty narodowej możemy używać za pomocą karty debetowej, a zasadniczym systemem jest bankowy system wraz z ludźmi sprawującymi kontrolę nad transakcjami. W przypadku kryptowaluty jest inaczej: przelewy dokonywane są tylko za pomocą oprogramowania nazywanego portfelami bądź „klientami", a za bezpieczeństwo transakcji odpowiada protokół sieci bitcoin.

Pomysł na rejestr rozproszony, czyli na bazę danych w wielu kopiach, istniał już przed pierwszą kryptowalutą, lecz było to pojęcie ogólne. Dopiero Nakamoto dopracował ten pomysł i zastosował go w blockchainie kryptowaluty; było to pierwsze bardziej znane zastosowanie takiego rejestru.

Blockchain bitcoina, wciąż będący rejestrem rozproszonym, zawiera informacje o transferach bitcoinów. Nazywany jest również łańcuchem bloków, ponieważ informacje te zapisywane są w blokach o ograniczonej pojemności, które po około 10 min. są zatwierdzane[10]. Informacje o transakcjach umieszczane są w łańcuchu boków przez „górników" wykorzystujących moc obliczeniową swoich urządzeń. Każdy blok jest powiązany w poprzednim, dzięki czemu łańcuch bloków jest integralny.

Jedną z technologii chroniących łańcuch bloków jest funkcja haszująca. Jest to jednokierunkowy skrót wyliczony dla tekstu bądź pliku, który pozwala szybko

[8] V. Dhillon, D. Metcalf, M. Hooper, *Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You*, 2017, s. 3.

[9] S. Raval, *Decentralized Applications*, Sebastopol 2016, s. 3.

[10] G. Karame, E. Audroulaki, *Bitcoin and Blockchain Security*, Norwood 2016, s. 44.

sprawdzić, czy coś się nie zmieniło[11]. Taka funkcja ma określoną liczbę znaków, które wyglądają na znaki losowe, lecz zawsze pokazuje identyczną wartość dla identycznych danych. Obliczona funkcja dla tekstu składającego się z jednego znaku, jak i dla zawartości książki będzie miała taką samą długość. Korzystając z internetowego generatora SHA256, można obliczyć hash dla wyrazów „Filia w Ełku", wynik to:

E8973B52F5EFBE61ACACCBE1C2D90C9DDDD540A545137295E4F38F-73C52E84B4

Ale po dodaniu kropki na końcu zdania wynik jest już zupełnie inny i jest to:

DE345AE523DA5C9B121556FB6F35F9F97AFD630BC5A35C4A0FAFB-165B693ECFD

Funkcja haszująca bywa wykorzystywana przez producentów oprogramowania, podają oni funkcję skrótu dla pliku instalacyjnego, aby osoba pobierająca program mogła sprawdzić jego autentyczność przed instalowaniem. W taki sposób funkcję haszującą wykorzystują przykładowo twórcy programu Veracrypt do szyfrowania danych[12]. W bitcoinie każdy nowy blok musi być zatwierdzony przez nadanie hashu. Nie jest to natychmiastowe, ponieważ sieć kryptowaluty zaakceptuje tylko taki wynik, który spełnia wymagania wyliczone przez algorytm; w przypadku BTC jest to ilość zer na początku. Sprawia to, że bloki nie są zatwierdzane natychmiast i to właśnie nazywane jest „trudnością kopania". Aby to zrozumieć, załóżmy, że posiadamy pewien blockchain i chcemy zatwierdzić nowy blok, który będzie zawierał tekst: „Filia w Ełku.". Sieć wymaga trzech zer na początku funkcji haszującej SHA256, abyśmy mogli dodać taką informację, a z poprzednich obliczeń wiemy, że trzy pierwsze znaki funkcji to „DE3", hash jest niezmienny i dla danego zdania będzie taki sam. W jakiś sposób musimy spełnić postawione nam wymagania, więc zaczynamy coś dopisywać do naszego zdania, postanawiamy po kropce wpisywać kolejno cyfry, za każdym razem sprawdzamy wynik z generatora i już po trzech próbach osiągamy jedno zero na początku. Wynik dla „Filia w Ełku.3" to:

0CFD22706E3B5DCFE4D744408A47400D56A546C092E8A2A80B9422B2E-DA9E451

Udało nam się osiągnąć jedno zero już po kilku sekundach prób, ale wciąż nie spełniamy wymagań. Okazuje się, że spełniamy je po wykonaniu ponad trzystu prób. Wynik dla „Filia w Ełku.343" to:

000B8CC863F2C21522C3CE756EF7EE7A83BF878F5FB24836FB5B8E-2A9EB0C48F

[11] A. Judmayer, N. Stifter, K. Krombholz, E. Weippl, *Blocks and Chains Introduction to Bitcoin, Cryptocurrencies, and their Consensus Mechanisms*, San Rafael 2017, s. 9.

[12] *Veracrypt*, <https://www.veracrypt.fr/en/Downloads.html>, dostęp: 01.06.2019.

Mamy trzy zera, spełniamy wymagania, rozsyłamy informację do sieci, a ta akceptuje nasz blok. Nasze zdanie o filii dodawane jest w pozostałych blockchainach, o ile ktoś inny nas nie ubiegł i nie zamieścił informacji wybranej przez siebie. Dopisane „343" jest w tym przykładzie „zmienną". Poszukiwaniem odpowiedniej spełniającej wymagania sieci kryptowaluty zajmują się „górnicy", nazywani tak, ponieważ wykonują żmudną pracę kopiąc, aż w końcu coś znajdą. W podanym przykładzie wymagano od nas trzech zer, ponieważ algorytm na podstawie historycznych danych uznał, że znalezienie trzech zer na początku funkcji zajmie dziesięć minut wszystkim innym górnikom pracującym jednocześnie.

W przypadku kryptowaluty BTC liczba wymaganych zer określana jest przez algorytm sieci co 2016 bloków i jeśli poprzednie bloki zostały zatwierdzone średnio poniżej 10 minut, trudność rośnie[13]. Nie jest tak, że każdy blok zostaje zatwierdzony zawsze dokładnie w 10 minut.

Informacjami zawartymi w zatwierdzonych blokach kryptowaluty są: hash obecnego bloku, transakcje między użytkownikami sieci wraz z nagrodą dla górnika, ale dodatkowo każdy blok posiada jeszcze hash bloku poprzedniego, dzięki czemu blockchain jest integralny, a próba zmiany transakcji z przeszłości oznacza również konieczność przeliczenia wszystkich następnych bloków.

Kolejnym zabezpieczeniem kryptowaluty jest technologia „Proof of Work", czyli dowód pracy, a mówiąc jeszcze prościej, chodzi o to, aby blok był zatwierdzony z taką trudnością, z wykorzystaniem takiej mocy obliczeniowej, aby oszustwo było bardzo ograniczone. Blok udaje się zatwierdzić co 10 minut zazwyczaj wtedy, kiedy o wygraną konkurują wszyscy górnicy razem wzięci; jednemu, w pojedynkę, mogłoby to zająć lata. Po poprawnym dodaniu bloku zaczynają się zmagania o nowy. Mogłoby się zdarzyć, że pozostanie jeden górnik, który się nie podda i będzie próbował zatwierdzić swoją wersję poprzedniego bloku, mimo że mający taki sam numer jest już zatwierdzony w sieci. Gdyby mu się udało, powstałyby dwa bloki o takim samym numerze. Mogłoby się wydawać, że w takiej sytuacji powstałaby możliwość podwójnego wydania środków z adresu, do którego ma dostęp zły górnik, ponieważ w dwóch blokach o tym samym numerze górnik mógłby zamieścić transakcję wysłania tego samego bitcoina na dwa różne adresy. Tymczasem przez sieć brany jest pod uwagę tylko pierwszy zatwierdzony blok, zły górnik musiałby poczekać, aż ktoś zatwierdzi nowy blok, a następnie samemu zatwierdzić dwa, w tym jeden o oznaczeniu takim samym jak ten zatwierdzony przez kogoś innego, doprowadziłoby to do zapomnienia przez sieć bloku innego górnika. Jednak taka próba ataku jest bardzo trudna, ponieważ moc obliczeniowa górników już w 2013 r., kiedy bitcoin był mało znany, 256-krotnie przewyższała możliwości 500 najwydajniejszych superkomputerów świata[14],

[13] J. Wilmoth, *Bitcoin Mining Industry 'Under Considerable Stress,' 1.3 Million Devices Switched Off* [tłumaczenie własne: Problemy kryptowalutowego górnictwa], 11.12.2018, <https://www.ccn.com/bitcoin-mining-industry-under-considerable-stress-1-3-million-devices-switched-off>, dostęp: 20.04.2019.

[14] R. Cohen, *Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers* [tłumaczenie własne: Globalna moc obliczeniowa bitcoin 256-krotnie przekracza moc 500 superkomputerów razem], Combined!, 28.11.2013, <https://www.forbes.com/sites/reuven-

a w 2018 r. rosła o ponad 100% w zaledwie cztery miesiące[15]. Przez „superkomputery" można rozumieć urządzenia wielkości dużych pomieszczeń o mocy wielokrotnie przewyższającej najwydajniejsze komputery, a rozbudowa jednego z bardziej znanych kosztowała aż 97 mln USD[16]. Wracając do górnika, który chciałby podwójnie wydać swoje monety. Aby przeprowadzić taki atak, potrzebowałby mocy obliczeniowej przewyższającej resztę sieci, co nazywane jest „atakiem 51%"[17]. Jednak zatwierdzenie jednej wadliwej wersji bloku to mało, ponieważ każda transakcja zyskuje kolejne potwierdzenia, a każde z nich oznacza, że uwierzytelniono już kolejny blok. Transakcja z trzema potwierdzeniami jest uznawana za autentyczną, a górnicy nie będą tworzyć nowego bloku powiązanego z oszukanym. Zły górnik musiałby dać radę zatwierdzić kilka bloków z rzędu, wyprzedzając resztę sieci, która zatwierdziła wcześniej inny. Taki atak istnieje w teorii, ponieważ moc sieci bitcoin jest zbyt duża, aby to się udało. Posiadając taką ogromną moc, po prostu bardziej opłaca się zarabiać na kopaniu kryptowalut.

W przypadku bitcoina nagroda za zatwierdzenie jednego bloku kryptowaluty wynosi obecnie 12,5 BTC (są to nowo powstałe monety), a oprócz nagrody przewidzianej wcześniej przez algorytm, górnik dolicza jeszcze opłaty transakcyjne. Przykładowo, nagroda za blok 570605 wynosi w zaokrągleniu 13,8 BTC. Górnik do swojej wersji bloku, który udało mu się zatwierdzić, dodaje jedną szczególną transakcję bez nadawcy, ale z odbiorcą, na samym szczycie listy jest to przekaz tych monet na jego adres[18]. Wielu próbuje zatwierdzić swoją wersję bloku, ale tylko jednemu udaje się średnio co 10 minut[19]. Można pomyśleć, że praca innych idzie na marne, ale to jest cena za bezpieczeństwo kryptowaluty bitcoin.

W początkach bitcoina do zatwierdzania bloków górnicy wykorzystywali procesory, dążąc do przeliczania jak największej liczby hashy na sekundę. Do tego zadania przydatniejsze okazały się karty graficzne, ponieważ lepiej radziły sobie z dużą liczbą małych obliczeń. „Górnictwo kryptowalutowe" rozwijało się wolno, ponieważ BTC był początkowo tylko ciekawostką, monety nie miały wartości, w 2010 r. rozdawane były za darmo[20]. Dużym postępem były urządzenia ASIC[21], których celem było przeliczanie jak największej liczby hashy przy jak najmniejszym poborze prądu. Podczas gdy konkurencja rosła, górnicy

cohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/#14f75bc16e5e>, dostęp: 20.04.2019.

[15] B. Bambrough, *Bitcoin's Computing Power Growth Is Outpacing The Bitcoin Price* [tłumaczenie własne: Moc obliczeniowa bitcoin przewyższa jej cenę], 11.06.2018, <https://www.forbes.com/sites/billybambrough/2018/07/11/bitcoins-computing-power-growth-is-outpacing-the-bitcoin-price/>, dostęp: 20.04.2018.

[16] D Poeter, *Cray's Titan Supercomputer for ORNL Could Be World's Fastest* [tłumaczenie własne: Superkomputer Titan najszybszy], 11.11.2011, <https://www.pcmag.com/news/288991/crays-titan-supercomputer-for-ornl-could-be-worlds-fastest>, dostęp: 22.04.2019.

[17] P. Franco, *Understanding Bitcoin Cryptography, Engineering and Economics*, Nowy Jork 2015, s. 17.

[18] *Bchain.com. Eksplorator bloków*, <https://bchain.info/BTC/block/570605>, dostęp: 22.04.2019.

[19] M. Szymankiewicz, *Bitcoin. Wirtualna waluta internetu*, Gliwice 2014, s. 40.

[20] *Web.archiwe.org*. Internetowa kopia strony freebitcoins.appspot.com działającej w 2010 roku, <https://web.archive.org/web/20100703032414/http://freebitcoins.appspot.com>, dostęp: 22.04.2019.

[21] P. Franco, *Understanding Bitcoin Cryptography*…, s. 147.

zaczęli współpracować, mieli wprawdzie mniejsze zyski, ale regularne. Tworzyli oni pule wydobywcze, w których współpraca polegała na dzieleniu się zadaniami, następnie wygrany przewodniczący dzielił się wygraną ze wspólnikami[22].

Aby zrozumieć, jak działają transakcje BTC, najlepiej założyć, że jest to przekazywanie praw do monet, a nie wysyłanie ich jako załącznika w wiadomości. W dużym skrócie – jest to tworzenie informacji o posiadaniu monet i informowanie sieci, na jaki adres mają być przekazane. Następnie taka informacja rozgłaszana jest w sieci, jest przez nią weryfikowana, na końcu trafia do łańcucha bloków. Lecz zanim powstanie transakcja, należy stworzyć swój adres, najczęściej dzieje się to automatycznie przy pierwszym otworzeniu aplikacji do obsługi BTC – portfela. Dokładniej – na początku tworzony jest losowy klucz prywatny, a na podstawie niego klucz publiczny, działa to na zasadzie kryptografii klucza publicznego[23]. Można uznać, że klucz prywatny to hasło do konta bankowego, a klucz publiczny to numer konta, z tym że drugie wynika z pierwszego, nigdy odwrotnie. Oba adresy są wykorzystywane do kryptograficznych podpisów. Klucz prywatny służy do podpisywania informacji o transakcji, a dzięki zastosowaniu kryptografii asymetrycznej węzły sieci widzą, że podpisano transakcję, ale ciąg znaków użyty do tego jest niewidoczny. Sieć może tylko za pomocą klucza publicznego dostać potwierdzenie, czy podpis jest prawidłowy, czy nie. Zdobycie klucza prywatnego, nawet kiedy widzi się podpisaną informację, nie jest możliwe. Wiedząc, jak działają podpisy cyfrowe, wiemy, że podstawowym zadaniem portfeli kryptowalut BTC jest bezpieczne ukrywanie klucza prywatnego oraz podpisywanie transakcji i wysyłanie ich do sieci. Dlatego po uruchomieniu takiego oprogramowania użytkownik ustawia hasło, aby zaszyfrować w pliku klucz prywatny, a następnie za każdym razem odszyfrowywać. Istnieją jednak rozwiązania bezpieczniejsze, są to tzw. portfele sprzętowe, zasada działania których jest dość prosta. Są to urządzenia z wyświetlaczami, z co najmniej dwoma przyciskami i możliwością podłączenia do komputera. Po pierwszym uruchomieniu generowany jest klucz prywatny, który pozostanie na tym urządzeniu. To, że można urządzenie podłączyć do komputera, nie oznacza, że istnieje możliwość skopiowania tajnego klucza do podpisu. Przez komputer na takie urządzenie wysłany jest adres, na jaki ma zostać wykonany przelew i dopiero na tym urządzeniu transakcja jest przetwarzana, czyli podpisana tajnym kluczem. Jest to obecnie najbezpieczniejsze rozwiązanie na trzymanie kryptowalut. Portfele sprzętowe mają przyciski, aby potwierdzić transakcję, wyświetlają przy tym jeszcze raz adres adresata. Ponadto, po uruchomieniu takiego urządzenia należy wpisać kilkucyfrowy pin. Po wpisaniu złego pinu, urządzenie może usunąć tajny klucz.

Portfele do BTC można podzielić na dwa rodzaje: na pełne oraz lekkie. Pełne wymagają pobrania pełnego łańcucha bloków, którego rozmiar na dzisiaj przekracza 200 GB[24] i dopiero po pobraniu można wykonywać transakcje.

---

[22] S. Bentyn, M. Grzybkowski, *Kryptowaluty,* Poznań 2018 s. 52–54.

[23] D. Homa, *Sekrety Bitcoina i innych kryptowalut. Jak zmienić wirtualne pieniądze w realne zyski*, Gliwice 2015, s. 27.

[24] *Blockchain.com. Eksplorator bloków*, <https://www.blockchain.com/pl/charts/blocks-size>, dostęp: 22.04.2019.

Z kolei portfele lekkie, jak wskazuje nazwa, nie wymagają pobierania pełnego blockchaina, zamiast tego takie portfele komunikują się z pełnymi węzłami, czyli z portfelem pełnym – Bitcoin Core. Pełnych węzłów działa obecnie 9491[25]. Ważną zaletą pełnego portfela jest to, że każdy nowo uruchomiony umacnia sieć[26].

Warto wyjaśnić, jak dokładniej wyglądają informacje o transakcji. Nie jest to takie oczywiste, choć znajomość zagadnienia nie jest wymagana, aby korzystać z kryptowaluty. Informację o transakcji można podzielić na dwie części: wejścia i wyjścia. „Wejście" to udowodnienie, że nadawca posiada daną ilość monet, aby transakcja została wykonana. W tym miejscu znajdują się skróty wcześniejszych transakcji na adresie obecnego nadawcy. Przykładowo, jeśli teraz chce wysłać 80 BTC, a wcześniej dostawał same przelewy po 1 BTC, to informacji zaliczanych jako „wejścia" będzie kilkadziesiąt. Z „Wyjściami" również nie jest prosto, jakby się mogło wydawać. Oczywiście, w tym miejscu jest adres odbiorcy, ale również adres nadawcy, aby zwrócono resztę monet. Chodzi o sytuację, gdy nadawca dostał wcześniej dwa razy po 30 BTC, a wysłać dalej chce tylko 50 BTC. W takiej sytuacji jednym „wyjściem" będzie adres odbiorcy, na który trafi 50 BTC, drugim będzie adres nadawcy, czyli 10 BTC pomniejszone o opłatę transakcyjną. Adresat tej opłaty nie jest wskazany, ponieważ nie wiadomo, któremu górnikowi uda się zatwierdzić blok.

Bitcoinów będzie nie więcej niż 21 mln, takie ograniczenie jest umieszczone w protokole sieci. Od początku istnienia BTC z każdym powstałym blokiem powstawało 50 BTC trafiających na adres górnika, lecz po około czterech latach nagroda ta maleje o połowę; takie wydarzenie nazywane jest „halvingiem"[27]. Jedną monetę można podzielić do ośmiu miejsc po przecinku, ponieważ 1 BTC to 100 000 000 sat[28]. Najmniejsza cząstka 1 sat, czyli „jeden grosz bitcoinowy", jest warta mało, bo tylko 0,0002 PLN podczas pisania artykułu[29]. Nagroda za zatwierdzenie bloku będzie maleć aż do 2140 r., wtedy górnicy będą zarabiać tylko na opłatach transakcyjnych. Jednak monet w obiegu w praktyce będzie mniej, ponieważ w 2018 r. szacowano, że od początku istnienia kryptowaluty zgubiono 4 mln BTC. „Zgubienie" w tym przypadku oznacza, że stracono klucz prywatny, bez którego nie można ruszyć monet. Zdarzało się to często, kiedy BTC nie miał wartości[30]. Ciekawostką jest, że nagroda za pierwszy blok transakcyjny została przyznana, ale trafiła na adres, z którego nie można ich przelać dalej; jest to tzw. hołd dla Satoshiego.

[25] *Bitnodes. Statystyki pełnych węzłów*, <https://bitnodes.earn.com/>, dostęp: 22.04.2019.
[26] C. Barski, C. Wilmer, *Bitcoin for the Befuddled*, San Francisco 2015, s. 193.
[27] B. Badr, R. Horrocks, X. Wu, *Blockchain By Example*, 2018, s. 103.
[28] R. Caetano, *Learning Bitcoin*, 2015, s. 9.
[29] *Kryptonotowania. Przelicznik ceny kryptowaluty*, <https://www.kryptonotowania.pl/kalkulator>, dostęp: 22.04.2019.
[30] J. Young, *6 Million Bitcoin is Lost or Stolen, Should the Real Value of BTC Higher?* [tłumaczenie własne: 6 milionów bitcoinów zgubiono lub ukradziono], 04.07.2018, <https://www.ccn.com/6-million-bitcoin-is-lost-or-stolen-should-the-real-value-of-btc-higher>, dostęp: 23.04.2019.

2. Powstanie następnych kryptowalut – altcoiny

„Altcoin" jest skrótem od „alternative coin", oznacza wszystkie kryptowaluty niebędące BTC. Nie istnieje żaden oficjalny spis wszystkich altcoinów, lecz są strony internetowe grupujące bardziej znane kryptowaluty w jednym miejscu wraz z cenami i dziennym obrotem na giełdach kryptowalutowych. Najpopularniejszą stroną jest coinmarketcap.com i na dzisiaj lista zawiera 2136 kryptowalut[31]. Duża część kryptowalut opiera się na kodzie źródłowym bitcoina ze zmianami, inne mają kod napisany od początku, a jeszcze inne są tylko tokenami.

Transakcje w przypadku kryptowalut – tak jak przy bitcoinie – często są zatwierdzane przez górników. Istnieją jednak alternatywy, kiedy zamiast górników pojawiają się „walidatorzy", występują oni w protokole „proof-of-stake". W takim systemie użytkownicy nagradzani za zatwierdzanie transakcji muszą posiadać również monety – im więcej, tym większa szansa na nagrodę[32]. W przypadku BTC górnicy nie muszą spełniać takiego wymagania.

Niektórzy używają określeń „kryptowaluty" i „tokeny" zamiennie, jest to jednak błąd, ponieważ to drugie słowo oznacza „nibykryptowalutę". Kryptowaluty mają własne blockchainy, tokeny natomiast korzystają z blockchainów innych kryptowalut. Istnieją kryptowaluty, które dają możliwość tworzenia tokenów na swoim blockchainie. Taką funkcję oferuje np. kryptowaluta Ethereum, gdzie za drobną opłatą w walucie ETH można stworzyć w jej blockchainie, na swoim adresie, wybraną przez nas liczbę tokenów. Tokeny tego typu nie mają wartości, a za wysyłanie ich na inne adresy w blockchainie płacimy wciąż w ETH. Warto dodać, że takie tokeny nie wymagają specjalnych adresów i mogą być wysyłane na adresy do odbioru ETH. Jednak portfele do obsługi kryptowaluty ETH po otrzymaniu takich tokenów mogą ich nie rozpoznać, czasami jest bowiem widoczna tylko informacja, że otrzymaliśmy przelew i nie jest to kryptowalutą ETH, lecz czymś innym. W takiej sytuacji należy skonfigurować portfel według instrukcji emitenta tokena. Niektóre eksploratory blockchaina ETH rozpoznają bardziej znane tokeny, przykładem jest https://ethplorer.io/.

Kryptowaluta Etherem została stworzona przez rosyjskiego programistę Vitalika Buterina i różni się od BTC tym, że jest od niego bardziej rozbudowana, ma wbudowany język programowania[33], dzięki któremu można tworzyć „smart contracts" w blockchainie ETH. Najprostszym przykładem jest zaprogramowanie płatności cyklicznej, a innym zapisanie w blockchainie, że ma zostać wykonana transakcja, kiedy jakiś wybrany adres w sieci wykaże się aktywnością. Oczywiście, istnieją dużo bardziej skomplikowane pomysły na wykorzystanie „smart contracts". Adres publiczny Ethereum różni się tym, że na początku ma „0x", podczas gdy w bitcoinie niezmienny początek to liczba 1 lub 3.

---

[31] Strona internetowa z listą najpopularniejszych krypto walut: *Coinmarketcap*, <https://coinmarketcap.com/all/views/all/>, dostęp: 22.04.2019.

[32] S. Raval, *Decentralized Applications*, s. 11.

[33] C. Dannen, *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginner*, Barkeley 2017, s. 2.

Ethereum pozwala na łatwe tworzenie tokenów, ale niesie to ze sobą pewne problemy. W internecie wiele jest dobrze reklamowanych projektów przyszłych kryptowalut, które według ich twórców wprowadzą innowację, często zapowiadają blockchain nowej generacji[34], transakcje z prędkością światła i podobne rzeczy, których nie posiada bitcoin. Lecz zanim innowatorzy stworzą kryptowalutę na swoim blockchainie, najpierw tworzą tokeny na blockchainie Ethereum i je sprzedają. Najczęściej wygląda to tak, że oczekując na otrzymanie prawdziwej kryptowaluty Ethereum, odsyłają tokeny na ten sam adres, z którego dostali zapłatę, obiecując, że po ukończeniu prac nad swoją rewolucyjną kryptowalutą uruchomią autorski blockchain i wtedy będzie miała miejsce migracja, czyli tokeny znajdujące się w blockchainie ETH będą wymieniane na obiecane wcześniej kryptowaluty już na nowym blockchainie. Taka forma zbierania kapitału określana jest jako ICO[35]. Projekty te często są prowadzone przez osoby anonimowe i reklamowane w przemyślany sposób. Podczas sprzedaży tokenów ludzie odpowiedzialni za projekt oferują również możliwość zdobycia ich małej ilości za darmo, ale należy wykonać kilka działań w celach reklamowych. Zadaniem jest zwykle udostępnienie na portalach społecznościowych informacji o sprzedaży tokenów projektu oraz śledzenie oficjalnego profilu na twitter.com w celu poprawienia statystyk. Ponadto, za zachęcenie innej osoby do reklamowania projektu jest szansa zdobycia jeszcze większej ilości tokenów. Kilka takich działań nic nie kosztuje, a tego typu forma reklamy sprawdza się znakomicie. Liczba tokenów do zdobycia jest zazwyczaj ograniczona i rozdawana dużo później, po zakończeniu ICO. Reklamujący, jak i kupujący takie tokeny oczekują, że będą jak pierwsi posiadacze bitcoinów, którzy sprzedali je później z dużym zyskiem. Prawda jest jednak taka, że Nakamoto nie potrzebował zbiórek, aby stworzyć swojego bitcoina, natomiast twórcy owych „innowacyjnych" projektów często są anonimowi nie dlatego, że chcą być jak Satoshi, ale żeby łatwo zniknąć wraz z zebranymi funduszami, a projekt trafia na deadcoins.com. Szacuje się, że 80% takich ICO to oszustwa[36], a sam twórca kryptowaluty Ethereum, który anonimowy nie jest, twierdzi że 90% takich projektów upadnie[37].

Nie wszystkie tokeny mają związek z oszustwem. Znane osobistości tworzą własne i sprzedają je; takie nazywane są „tokenami personalnymi"[38]. Przypominają autografy, które w przyszłości mogą nabrać wartości. Innym ciekawym tokenem jest Binance Coin, który był sprzedawany w trakcie ICO. Środki zebrane podczas ICO zostały przeznaczone na stworzenie giełdy kryptowalut. Giełda osiągnęła sukces, a sam sprzedawany wcześniej token ma zastosowanie. Użytkownicy giełd kryptowalut podczas wymian kryptowalut na inne muszą

[34] Multiversum, https://www.multiversum.io/

[35] B. Dhillon, D. Metcalf, M. Hooper, *Blockchain Enabled Applications*..., s. 185–186.

[36] A. Alexandre, *New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams* [tłumaczenie własne: Według badań, 80% ICO to oszustwa], 17.07.2018, <https://cointelegraph.com/news/new-study-says-80-perc ent-of-icos-conducted-in-2017-were-scams>, dostęp: 26.04.2019.

[37] E. Peters, *90% of ICOs Will Fail – Vitalik Buterin* [tłumaczenie własne: 90% ICO upadnie – Vitalik Buterin], 01.01.2017, <http://www.thecryptowire.com/2017/12/01/90-of-icos-will-fail-vitalik-buterin/>, dostęp: 26.04.2019.

[38] S. Bentyn, M. Grzybkowski, *Kryptowaluty*, s. 69.

również wnieść opłaty, najczęściej w BTC, ale na giełdzie Binance pozwolono płacić tokenem, dzięki któremu powstała owa giełda. Jest to jeden z nielicznych tokenów, który ma zastosowanie, co sprawiło, że jego cena jest bardziej stabilna. Tego właśnie brakuje innymi tokenom. Obecnie token Binance Coin istnieje w blockchainie ETH, ale w przyszłości przejdzie na swój własny, na którym będzie działać jednocześnie zdecentralizowana giełda kryptowalut[39], zdecentralizowana podobnie jak kryptowaluty.

Istnieją kryptowaluty, które są prężnie reklamowane, a ich twórcy deklarują, że produkt ów zdetronizuje bitcoina. Mówi się o blockchainach nowej generacji, a nawet o alternatywie dla tej technologii. Pomysłów jest wiele, jednak od dziesięciu lat nic się nie zmienia. Pojawiły się także kryptowalaty, których twórcy niczego nie obiecywali, a ich produkt przyjął się. Taką przykładową kryptowaluta jest Dogecoin, która w logo ma psa znanego z internetowych śmiesznych obrazków. Dogecoin oparty jest na jawnym kodzie kryptowaluty bitcoin, ale z małymi zmianami. Najważniejszą różnicą jest to, że waluta nie ma w algorytmie ustawionego limitu monet, który w bitcoinie wynosi 21 mln. Nowe monety Dogecoin będą powstawały w nieskończoność. Bloki w tej walucie są zatwierdzane średnio w jedną minutę, a jej kod nie jest poprawiany od lat, choć prawdopodobnie można by coś poprawić. Dogecoin często jest wykorzystywany do zbierania funduszy na cele charytatywne, przykładem jest zbiórka na studnie w Kenii[40].

Kryptowalutą, która ma najwięcej wrogów, jest Bitcoin Cash. Nikt nie może zakazać używania nazwy bitcoin, również logo nie jest zastrzeżone i każdy może sprzedawać koszulki z logo kryptowaluty. Twórcy Bitcoin Cash reklamują swój projekt jako lepszy bitcoin, niestety w zły sposób. Kupili prawa do domeny bitcoin.com, a nieostrożni ludzie mogą uznać, że to oficjalna strona internetowa bitcoina od Satoshiego Nakamoto. Na stronie tej są odnośniki do zakupu kryptowaluty bitcoin, ale dopiero po kliknięciu w nie okazuje się, że nie chodzi o prawdziwego bitcoina. Niestety, Bitcoin Cash jest popularny.

3. Kryptowaluty zapewniające anonimowość

Kiedy kryptowaluta bitcoin miała już wartość i używano jej do płatności, powstał czarnorynkowy serwis Silk Road. Portal założony przez Williama Ulbrichta służył do handlowania narkotykami i innymi zakazanymi produktami, można tam było również wynająć hakerów. Bitcoin był stosowany do płatności, ponieważ był lepszym rozwiązaniem niż internetowe przelewy. BTC naprawdę jest jednak „pseudoanonimowy", blockchain jest jawny, ruchy monet bitcoina można śledzić od czasu ich wykopania[41]. Służby sprawdzając adres BTC, mogą powiązać go z adresem giełdy kryptowalut, a jeśli ta znajduje się w Unii Europejskiej, sprawa

[39] D. Wiktor, *Binance odchodzi od Ethereum na rzecz Binance Chain*, 18.04.2019, <https://alternatywa.net.pl/binance-chain-ethereum-bnb-erc20/>, dostęp: 25.04.2019.

[40] T. Waryszak, *Jak zarabiać na kryptowalutach*, Gliwice 2018, s. 48.

[41] M. Swan, *Blockchain. Blueprint for a New Economy*, Sebastopol 2015, s. 36.

jest ułatwiona, możliwe jest zdobycie adresu poczty internetowej, adresu IP komputera, a niektóre giełdy wymagają nawet weryfikacji za pomocą dokumentów. Mimo że człowiek sprawdzany przez służby mógł unikać największych giełd, to osoba, od której dostał przelew, ostrożna być nie musiała. Ulbricht w końcu został namierzony, a FBI prześledziło tysiące adresów, które miały związek z Silk Road. W 2014 r., aby złagodzić wyrok, Ulbricht przyznał się do prowadzenia tego portalu. Tuż przed przybyciem służb mógł zebrać dużą liczbę BTC na jednym koncie i jeśli dobrze zabezpieczył klucz prywatny, nikt tego konta nie przejmie. Właśnie taki adres, powiązany z portalem, znaleziono po zatrzymaniu, zawierał ponad 100 tys. BTC. Liczba monet wzrosła tuż przez zamknięciem właściciela[42].

Prawdą jest, że jeśli przestępcy używają kryptowalut, to wybór pada na BTC bardzo rzadko, ponieważ istnieje kryptowaluta, która nadaje się do tego lepiej, mianowicie anonimowa Monero (choć potwierdzone jest również, że terroryści i tak preferują gotówkę[43]). Monero w języku esperanto oznacza monetę[44]. Owa kryptowaluta ma swój blockchain, ale pozwala ukryć adres odbiorcy, nadawcę oraz kwotę. Osoby nieznające kryptowalut często mają styczność z Monero, nawet o tym nie wiedząc. Na stronach internetowych dodawane są ukryte koparki tej kryptowaluty, ponieważ dobrze wydobywa się ją korzystając z procesora, do którego ma dostęp przeglądarka internetowa[45]. Nieświadome kopanie tej kryptowaluty na stronie poznaje się po wyższym wykorzystaniu procesora. W kryptowalucie bitcoin informacje są jawne i powiązane ze sobą, dzięki czemu waluta jest bezpieczna. W przypadku Monero, gdzie informacje są ukrywane, nie można mieć pewności, że sieć działa dobrze. Prawdopodobnie Monero prędzej czy później zostanie zakazany, co spowoduje zmniejszenie rynku zbytu i spadek wartości. Na razie jednak prywatność jest w cenie.

Mniej anonimową kryptowalutą jest w pewnym sensie Zcash. To użytkownik decyduje, czy transakcja ma być anonimowa, z tej funkcjonalności korzysta 25% wysyłających tę kryptowalutę. Zdaniem Edwarda Snowdena, byłego pracownika CIA, Zcash jest najlepszy wśród prywatnych kryptowalut[46], choć za numer jeden wśród anonimowych kryptowalut powszechnie uznawane jest Monero.

---

[42] K. Kopańko, M. Kozłowski, *Bitcoin…*, s. 22–24.

[43] D. Dziduch, *Bitcoin nie taki straszny. Terroryści wciąż wolą gotówkę od kryptowalut*, 2.04.2019, <https://www.fxmag.pl/artykul/nie-taki-bitcoin-straszny-terrorysci-wola-gotowke-od-kryptowalut-wg-raportu>, dostęp: 01.06.2019.

[44] *Internetowy słownik esperanto-polski*, <https://pl.glosbe.com/eo/pl/monero>, dostęp: 22.04.2019.

[45] P. Maziarz, *Kopanie kryptowalut na CPU – Threadripper wymiata w Monero*, 1.02.2018, <http://www.benchmark.pl/aktualnosci/kopanie-kryptowalut-na-procesorach-wydajnosc-i-zyski.html>, dostęp: 28.04.2019.

[46] D. Dziduch, *Snowden: Bitcoin nie przetrwa, ale kryptowaluty zostaną z nami na dłużej*, 26.11.2018, <https://www.fxmag.pl/artykul/snowden-bitcoin-nie-przetrwa-ale-kryptowaluty-zostana-z-nami-na-dluzej>, dostęp: 28.04.2019.

Podsumowanie

Rynek bitcoinowy może wydawać się trudny do zrozumienia. Nawet mimo wyjaśnienia, dlaczego środki na adresie bitcoinowym są bezpieczne, człowiekowi trudno zaufać technologii niekontrolowanej przez żadne podmioty. Z drugiej strony warto przypomnieć, że chociaż bitcoin działa niezawodnie od dziesięciu lat, nie oznacza to, że będzie tak przez kolejne lata. Mogą bowiem nadejść czasy, gdy do walki z kryptowalutami zostaną wykorzystane komputery kwantowe. Nawet jednak gdyby kryptowaluty upadły, pozostawią po sobie opracowane zabezpieczenia. Najważniejszy jest rejestr rozproszony, który dzięki kryptowalutom został dopracowany i może mieć różne zastosowania.

BIBLIOGRAFIA

Literatura

Antonopoulos M., *Bitcoin dla zaawansowanych. Programowanie z użyciem otwartego łańcucha bloków*, Gliwice 2018.

Badr B., Horrocks R., Wu X., *Blockchain By Example*, 2018.

Barski C., Wilmer C., *Bitcoin for the Befuddled*, San Francisco 2015.

Bentyn S., Grzybkowski M., *Kryptowaluty,* Poznań 2018.

Caetano R., *Learning Bitcoin*, 2015.

Dannen C., *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginner*, Barkeley 2017.

Dhillon V., Metcalf D., Hooper M., *Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You*, 2017.

Drescher D., *Blockchain. Podstawy technologii łańcucha bloków w 25 krokach*, Gliwice 2018.

Franco P., *Understanding Bitcoin Cryptography, Engineering and Economics*, 2015.

Homa D., *Sekrety Bitcoina i innych kryptowalut. Jak zmienić wirtualne pieniądze w realne zyski*, Gliwice 2015.

Judmayer A, Stifter N, Krombholz K, Weippl E., *Blocks and Chains Introduction to Bitcoin, Cryptocurrencies, and their Consensus Mechanisms*, San Rafael 2017.

Karame G., Audroulaki E., *Bitcoin and Blockchain Security*, Norwood 2016.

Kopańko K., Kozłowski M., *Bitcoin. Złoto XXI wieku*, Gliwice 2014.

Raval S., *Decentralized Applications*, Sebastopol 2016.

Swan M., *Blockchain. Blueprint for a New Economy*, Sebastopol 2015.

Szymankiewicz M., *Bitcoin. Wirtualna waluta internetu*, Gliwice 2014.

Waryszak T., *Jak zarabiać na kryptowalutach*, Gliwice 2018.

Źródła internetowe

Alexandre A., *New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams* [tłumaczenie własne: Według badań, 80% ICO to oszustwa], 17.07.2018, <https://cointelegraph.com/news/new-study-says-80-perc ent-of-icos-conducted-in-2017-were-scams>, dostęp: 26.04.2019.

Bambrough B., *Bitcoin's Computing Power Growth Is Outpacing The Bitcoin Price* [tłumaczenie własne: Moc obliczeniowa bitcoin przewyższa jej cenę], 11.06.2018, <https://www.forbes.com/sites/billybambrough/2018/07/11/bitcoins-computing-power-growth-is-outpacing-the-bitcoin--price/>, dostęp: 20.04.2018.

Bchain.com. Eksplorator bloków, <https://bchain.info/BTC/block/570605>, dostęp: 22.04.2019.

Bitnodes. Statystyki pełnych węzłów, <https://bitnodes.earn.com/>, dostęp: 22.04.2019.

Blockchain.com. Eksplorator bloków, <https://www.blockchain.com/pl/charts/blocks-size>, dostęp: 22.04.2019.

Cohen R., *Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers* [tłumaczenie własne: Globalna moc obliczeniowa bitcoin 256 krotnie przekracza moc 500

superkomputerów razem], Combined!, 28.11.2013, <https://www.forbes.com/sites/reuvencohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/#14f75bc16e5e>, dostęp: 20.04.2019.
Coinmarketcap, Strona internetowa z listą najpopularniejszych kryptowalut, <https://coinmarketcap.com/all/views/all/>, dostęp: 22.04.2019.
Dziduch D, *Snowden: Bitcoin nie przetrwa, ale kryptowaluty zostaną z nami na dłużej*, 26.11.2018, <https://www.fxmag.pl/artykul/snowden-bitcoin-nie-przetrwa-ale-kryptowaluty-zostana-z--nami-na-dluzej>, dostęp: 28.04.2019.
Dziduch D., *Bitcoin nie taki straszny. Terroryści wciąż wolą gotówkę od kryptowalut*, 2.04.2019, <https://www.fxmag.pl/artykul/nie-taki-bitcoin-straszny-terrorysci-wola-gotowke-od-kryptowalut-wg-raportu>, dostęp: 01.06.2019.
Dziduch D., *Bitcoin powstał dokładnie 10 lat temu, w ciągu dekady odmieniając oblicze rynków*, 03.01.2019, <https://www.fxmag.pl/artykul/bitcoin-genesis-block-10-lat>, dostęp: 19.04.2019.
Internetowy słownik esperanto-polski, <https://pl.glosbe.com/eo/pl/monero>, dostęp: 22.04.2019.
Kmita M., *10 lat temu wybuchł kryzys finansowy. Wtedy też narodziła się idea Bitcoina*, 17.10.2018, <https://bithub.pl/opinie/10-lat-temu-wybuchl-kryzys-finansowy-wtedy-tez-narodzila-sie-idea-bitcoina/>, dostęp: 19.04.2019.
Kryptonotowania. Przelicznik ceny kryptowaluty, <https://www.kryptonotowania.pl/kalkulator>, dostęp: 22.04.2019.
Maziarz P., *Kopanie kryptowalut na CPU – Threadripper wymiata w Monero*, 01.02.2018, <http://www.benchmark.pl/aktualnosci/kopanie-kryptowalut-na-procesorach-wydajnosc-i-zyski.html>, dostęp:28.04.2019.
Multiversum, https://www.multiversum.io/
Peters E., *90% of ICOs Will Fail – Vitalik Buterin* [tłumaczenie własne: 90% ICO upadnie – Vitalik Buterin], 01.01.2017, <http://www.thecryptowire.com/2017/12/01/90-of-icos-will-fail-vitalik-buterin/>, dostęp: 26.04.2019.
Pitta R., *Requiem for a Bright Idea*, 01.11.1999, <https://www.forbes.com/ forbes/1999/1101/6411 390a.html#873fdc4715f6>, dostęp: 22.04.2019.
Poeter D., *Cray's Titan Supercomputer for ORNL Could Be World's Fastest* [tłumaczenie własne: Superkomputer Titan najszybszy], 11.11.2011, <https://www.pcmag.com/news/288991/crays--titan-supercomputer-for-ornl-could-be-worlds-fastest>, dostęp: 22.04.2019.
Veracrypt, <https://www.veracrypt.fr/en/Downloads.html>, dostęp: 01.06.2019.
Web.archiwe.org. Internetowa kopia strony freebitcoins.appspot.com działającej w 2010 r., dostępna na: <https://web.archive.org/web/20100703032414/http://freebitcoins.appspot.com>, dostęp: 22.04.2019.
Wiktor D., *Binance odchodzi od Ethereum na rzecz Binance Chain*, 18.04.2019, <https://alternatywa.net.pl/binance-chain-ethereum-bnb-erc20/>, dostęp: 25.04.2019.
Wilmoth J., *Bitcoin Mining Industry 'Under Considerable Stress,' 1.3 Million Devices Switched Off* [tłumaczenie własne: Problemy kryptowalutowego górnictwa], 11.12.2018, <https://www.ccn.com/bitcoin-mining-industry-under-considerable-stress-1-3-million-devices-switched-off>, dostęp: 20.04.2019.
Young J., *6 Million Bitcoin is Lost or Stolen, Should the Real Value of BTC Higher?* [tłumaczenie własne: 6 milionów bitcoinów zgubiono lub ukradziono], 04.07.2018, <https://www.ccn.com/6-million-bitcoin-is-lost-or-stolen-should-the-real-value-of-btc-higher>, dostęp: 23.04.2019.

DEVELOPMENT AND GROWTH OF CRYPTOCURRENCIES IN THE WORLD

SUMMARY

The presented article is devoted to cryptocurrencies. In this work simple language is used so that people who have not heard of cryptocurrencies could understand how they work. Some things have been simplified here so that the article would not be too long. Author explains why bitcoin cryptocurrency is special and why it turned out to be a revolution among online currencies. The author has attempted to show how important is cryptography security.

KEY WORDS: bitcoin, ethereum, cryptocurrency, blockchain, cryptography