BITCOIN

I BLOCKCHAIN

NARODZINY

KRYPTOWALUT

W ofercie Wydawnictwa Łukasz Tomys Publishing dostępne są m.in. następujące e-booki:

- *Elon Musk. Wizjoner z Doliny Krzemowej (lata 1971-2021)* - Renata Pawlak, Kinga Kosecka
- *Mark Zuckerberg i jego imperium. Jak Facebook zmienia Twój świat* - Kinga Kosecka, Renata Pawlak, Ewa Szach, Kinga Sołtysiak
- *Ray Kroc i imperium McDonald's* - Kinga Kosecka, Justyna Jaciuk
- *Skuteczny inwestor. Warren Buffett i Benjamin Graham* - Łukasz Tomys, Mateusz Sawicki, Justyna Jaciuk
- *Steve Wozniak. Geniusz Apple* - Łukasz Tomys, Renata Pawlak
- *Warren Buffett i Philip Fisher. Selekcjonuj jak mistrzowie. Ocena firmy 15 kroków* - Łukasz Tomys, Mateusz Sawicki

Bitcoin i Blockchain. Narodziny kryptowalut.

Autorzy: Mateusz Lubiński, Mateusz Wiatr

Redakcja i korekta: Przemysław Andrzejewski

Wstęp

Nasze czasy zostały okrzyknięte mianem cyfrowej rewolucji. Kryptowaluty i technologia blockchain zmieniają świat, jaki znamy. Od kryptowalut nie da się już uciec. Niektórzy traktują je jako sposób na pomnażanie swoich oszczędności i spekulują. Inni widzą w nich walutę przyszłości i trzymają w swoich portfelach, czekając na znaczny wzrost wartości w czasie. Pojawiają się również głosy wieszczące koniec ery inwestowania w złoto, które ma zostać wyparte przez kryptowaluty. Inwestując w walutę cyfrową można w bardzo krótkim czasie uzyskać wysokie stopy zwrotu, ale także szybko stracić wszystkie ulokowane pieniądze. Zmienność notowań na tym rynku znacznie odbiega bowiem od wahań wycen innych instrumentów finansowych.

Historia zna wiele przypadków kryptomilionerów, którzy dorobili się ogromnych sum w ciągu kilku lat, ale nie zapominajmy również o bankrutach, którzy w mgnieniu oka stracili oszczędności swojego życia. Kryptowaluty mają także swoją mroczną stronę, pełną historii o włamaniach, praniu brudnych pieniędzy, handlu narkotykami czy bronią. Jednak z całą pewnością genezy takiego ich wykorzystania nie należy dopatrywać się w samej technologii, a w ludziach, którzy z niej korzystają.

Mamy nadzieję, że niniejszy tekst pozwoli Ci zrozumieć świat kryptowalut, który być może do tej pory jawił Ci się jako czarna magia, a także, że zauważysz potencjał drzemiący w technologii blockchain. Dzięki tej publikacji poznasz historię kryptowalut. Dowiesz się, jak rozwijały się koncepcje i powstawały rozwiązania, które znalazły zastosowanie w sieci Bitcoin. Ponadto poznasz podstawowe pojęcia ze świata kryptowalut, takie jak tokeny, ICO, łańcuchy bloków, klucze prywatne i publiczne czy zimny portfel. Odkryjesz drogę, którą przeszedł Bitcoin oraz pierwsze altcoiny – czyli kolejne kryptowaluty.

Opowiemy Ci o tym, jak wyglądały początki Ethereum i Dogecoina promowanego przez Elona Muska. Przybliżymy Ci ciekawe postaci, które

miały wpływ na rozwój technologii blockchain. Odsłonimy przed Tobą historię upadku największej giełdy kryptowalut – Mt.Gox. Przytoczymy przykłady pierwszych transakcji, ataków hakerskich i regulacji, jakimi próbuje się objąć kryptowaluty. Podczas czytania zdobędziesz praktyczne informacje na temat kupowania i przechowywania kryptowalut, a także o sposobach wykorzystywanych przez cyberprzestępców chcących okraść nasze konta bankowe i portfele kryptowalut. Dowiesz się więcej o technologii Blockchain oraz w jaki sposób zmienia ona cyfrową rzeczywistość, którą znamy.

Świat kryptowalut jest w ciągłym ruchu, zmienia się, ewoluuje. W krótkim czasie powstały – i powstaną kolejne – innowacyjne rozwiązania oparte na łańcuchu bloków, które ułatwią nasze życie. Za ich pomocą możemy zbierać środki w kampaniach crowdfundingowych, chronić własność intelektualną tokenami NFT czy wykonywać anonimowe transakcje. W podsumowaniu przedstawimy zalety oraz wady, szanse i ryzyka, które stoją przed kryptowalutami i technologią Blockchain.

Rozdział 1. Technologiczne podwaliny

Blind signatures (pol. niewidoczne podpisy) *– to zbiór algorytmów kryptograficznych, które są wykonywane przez trzech użytkowników: odbiorcę, podpisującego i weryfikatora. Technologia ta znajduje zastosowanie m.in. w elektronicznych płatnościach. Wykorzystując ślepe podpisy bank nie jest w stanie śledzić użytkownika elektronicznego banknotu. Algorytmy te wykorzystywane są również w elektronicznych wyborach czy innych technologiach chroniących prywatność użytkowników.*

Pierwsze rozwiązania technologiczne, na których oparta jest architektura kryptowalut sięgają początku lat 80-tych ubiegłego wieku. Fundamenty Bitcoina i całego kryptowalutowego świata czerpią z osiągnięć Davida Chauma, amerykańskiego informatyka i kryptografa, specjalisty anonimowej komunikacji elektronicznej, nazywanego „ojcem cyfrowego pieniądza". David Chaum podczas studiów na Uniwersytecie Kalifornijskim w Berkeley zaproponował rozwiązanie polegające na bezpiecznym, nienamierzalnym podpisie. W artykule naukowym opisywał architekturę tzw. niewidocznego podpisu, czyli blind signature, w ramach którego istnieje klucz publiczny i prywatny. Rozwiązanie to zapewnia prywatność użytkownikom dokonującym transakcji online i gwarantuje jej bezpieczeństwo. Już wtedy Chaum stwierdził, że dane zbierane przez banki i innych pośredników finansowych mogą stanowić zagrożenie dla prywatności użytkowników Internetu i naruszać prawa obywatelskie. Jakże trafnie przewidział gromadzenie danych i zarabianie na internautach przez największych gigantów technologicznych dzisiejszych czasów.

Chcąc wdrożyć swój pomysł w życie, w 1989 roku Chaum założył firmę DigiCash. Jej flagowym produktem był program, który pozwalał użytkownikom na wymianę dolarów na specjalny pieniądz elektroniczny i umożliwiał przeprowadzanie anonimowych transakcji. Model biznesowy

Davida Chauma zakładał, że jego firma będzie zarabiać na licencjonowaniu technologii. W 1994 roku, w Genewie, na zorganizowanej w siedzibie CERN konferencji dotyczącej internetu i rozwiązań www, Chaum przedstawił światu pierwszy elektroniczny system obsługi płatności online – eCash. Stwierdził wówczas: „Możesz zapłacić za dostęp do bazy danych, kupić oprogramowanie lub biuletyn przez e-mail, zagrać w grę komputerową przez internet, otrzymać 5 dolarów od znajomego lub po prostu zamówić pizzę. Możliwości są naprawdę nieograniczone". Brzmi bardzo współcześnie, prawda?

Pomysłem Chauma zainteresowały się wielkie banki oraz koncerny technologiczne, w tym Microsoft. Do 1995 roku jego firma zawarła umowy z Mark Twain Bank w St. Louis. W 1996 roku DigiCash rozpoczął współpracę z Deutsche Bank, Credit Suisse, australijskim Advance Bank i Bankiem Austria. Jednak pod koniec lat 90. przedsiębiorstwo zaczęło mieć problemy ze znalezieniem stabilnego modelu biznesowego. Niektóre źródła, jako jedną z przyczyn takiego stanu rzeczy, wskazują brak zaufania Chauma do swoich pracowników i stawianie na perfekcję kosztem praktyczności produktu. Odmówił również nawiązania współpracy z niektórymi dużymi bankami (jak np. ING) i był nieufny wobec wielkich graczy technologicznych, takich jak Microsoft czy Netscape. Z powodu błędów w oprogramowaniu i nieprzemyślanej strategii biznesowej w 1998 roku firma Davida Chauma zbankrutowała. Pozostałe aktywa DigiCash zostały kupione przez eCash Technologies, spółkę specjalizującą się w cyfrowej walucie, która w 2002 roku została przejęta przez InfoSpace – dostawcę wyników wyszukiwania i monetyzacji typu white label (aby uniknąć niepotrzebnego żargonu technicznego możemy posłużyć się uproszczeniem i opisać InfoSpace jako firmę zarabiającą na reklamach w wyszukiwarkach oraz szeroko pojętym pozycjonowaniu w sieci).

Koncepcja płatności internetowych nie zniknęła wraz z DigiCash. Z uwagi na coraz szybszy rozwój i rozpowszechnianie się internetu pojawiały się kolejne elektroniczne systemy płatności online. Przedstawiona wtedy tzw. pierwsza generacja systemów mikropłatności, umożliwiała zakup alternatywnej gotówki elektronicznej. Twórcy pierwszych systemów płatności internetowych dążyli do tego, aby ich cyfrowy pieniądz był zbliżony do tradycyjnego pieniądza fiducjarnego, czyli waluty opartej na

zaufaniu do emitenta. Zależało im, by nowy cyfrowy pieniądz był szeroko akceptowalny, nie generował dodatkowych opłat transakcyjnych, a ponadto gwarantował anonimowość.

W latach dziewięćdziesiątych komputery z dostępem do Internetu należały do rzadkości. Trzeba zatem wziąć pod uwagę, że tylko nieliczni mogli pozwolić sobie na skorzystanie z takiej formy płatności. Obsługa pierwszych systemów była trudna, nieintuicyjna i wymagała pewnej wiedzy technicznej – użytkownicy musieli nie tylko poradzić sobie z nieporęcznymi interfejsami, ale także posiadać specjalistyczną wiedzę dotyczącą szyfrowania i transmisji danych. Ponadto niektóre systemy wymagały dodatkowego sprzętu – zazwyczaj kart chipowych i czytników do nich. Duże ograniczenia techniczne potencjalnych użytkowników skłoniły twórców kolejnych systemów płatności do porzucenia koncepcji utworzenia nowej waluty cyfrowej. Zamiast tego skupili się na rozwoju architektury samego oprogramowania. Dążyli do zaprojektowania rozwiązań, które będą proste w obsłudze, bardziej wydajne i będą funkcjonować bez konieczności użycia dodatkowych akcesoriów czy instalowania odrębnego programu. Założeniem było uruchomienie systemów transakcyjnych dostępnych dla każdego posiadacza urządzenia z dostępem do Internetu.

Idea stworzenia niezależnego, anonimowego i alternatywnego systemu płatności była promowana przez ruch cypherpunk, do którego należeli m.in. kryptolodzy o wolnościowych poglądach, którzy wyrażali swój sprzeciw wobec amerykańskiej władzy. Początkowo tworzyli nieformalną grupę, która komunikowała się za pośrednictwem różnego rodzaju internetowych list dyskusyjnych, na których poruszali tematy korporacyjnej kontroli informacji oraz braku prywatności. Przy wykorzystaniu kryptografii dążyli do zapewnienia wysokiego poziomu prywatności i niezależności.

W przeciwieństwie do obecnych zdecentralizowanych, opartych o łańcuch bloków kryptowalut, pierwsze stworzone przez cypherpunków systemy płatności internetowych bazowały na jednym głównym serwerze, który obsługiwał transakcje wymiany zwykłej gotówki na ich cyfrową postać. Wczesne formy pieniądza cyfrowego pozostawiały wiele do

życzenia. Nie gwarantowały anonimowości i niezależności transakcji. Generowały wysokie koszty związane z zapewnieniem bezpieczeństwa i nie były ze sobą kompatybilne – nie można było wymienić jednego cyfrowego pieniądza na drugi bez udziału dolara amerykańskiego lub innej państwowej waluty.

Początku rozwoju koncepcji kryptowalut jako zdecentralizowanego i anonimowego elektronicznego środka płatności należy szukać pod koniec lat dziewięćdziesiątych ubiegłego wieku. W 1998 roku Wei Dai, informatyk i absolwent Uniwersytetu Waszyngtońskiego, a także członek wspomnianego ruchu cypherpunk, przedstawił ideę anonimowej cyfrowej waluty o nazwie b-money. Twierdził, że „podstawą społeczności, która ceni prywatność, powinno być posiadanie środka wymiany (pieniądza), który cechuje anonimowość i efektywność w egzekwowaniu zawieranych umów". Jego pomysł zakładał istnienie sieci (łańcucha bloków), w której anonimowi użytkownicy będą mogli przelewać między sobą środki i egzekwować umowy bez pomocy z zewnątrz.

Projekt b-money nie został nigdy oficjalnie uruchomiony, jednak założenia i koncepcje opracowane przez Wei Daia stanowiły istotny wkład do pracy Satoshiego Nakamoto, legendarnego i tajemniczego twórcy Bitcoina, o którym wspomnimy w dalszej części książki. Koncepcja zakładała, że transakcje przeprowadzane za pomocą b-money będą weryfikowane przez społeczność w publicznie dostępnym rejestrze historycznych transakcji. Dai zapisał się na kartach historii kryptowalut – do dziś pozostaje jedną z najistotniejszych postaci w tej branży. W hołdzie za wkład wniesiony w rozwój technologii założyciele kryptowaluty Ethereum nazwali jego imieniem swoją najmniejszą jednostkę rozliczeniową – „wei".

Ważnym fundamentem technologicznym, bez którego nie moglibyśmy rozmawiać o kryptowalutach, jest koncepcja „smart contracts". Zgodnie z definicją „zwykłego" kontraktu, jest to umowa pomiędzy dwojgiem lub więcej stronami. Przykładami dobrze znanych nam kontraktów są: umowa o pracę, umowa kredytowa, akt małżeństwa czy umowa najmu lokalu. W tego typu kontraktach często widnieje paragraf – „Wszelkie spory i niejasności wynikłe z realizacji niniejszej umowy będzie

rozstrzygać sąd właściwy dla…”. Egzekwowanie i rozwiązywanie sporów w obecnie dominujących na świecie kontraktach wymaga istnienia strony trzeciej – regulatora, który włączy się do umowy, gdy kontrakt nie będzie przestrzegany, a jedna ze stron zostanie poszkodowana. Zgodnie z obowiązującym systemem prawnym regulator podejmuje odpowiednie działania, aby rozwiązać wszelkie spory i dopilnować prawidłowego wywiązania się z umowy.

To właśnie potrzeba regulacji jest największą różnicą pomiędzy standardowym a inteligentnym kontraktem. Dlaczego? Smart contract to samowykonalna umowa. Warunki między stronami są zapisywane bezpośrednio w wierszach kodu, który najczęściej przyjmuje formę bloków logicznych. Jeżeli warunek zostanie spełniony, program wykonuje lub odblokowuje możliwość procesowania odpowiedniej dla warunku czynności i przejścia do kolejnego punktu w umowie. Działa jak swoisty protokół bezpieczeństwa, który dba o prawidłowy przebieg umowy.

Dla zobrazowania posłużmy się przykładem inteligentnego kontraktu z popularnym automatem z przekąskami. Strona kupująca podejmuje działanie i wrzuca monety – wykonuje tym samym część kontraktu. Następnie maszyna weryfikuje wykonanie tego punktu umowy i odpowiada swoim działaniem zapisanym w kontrakcie – wydaje zakupione towary. To oczywiście najprostszy przykład, przytoczony w celu pokazania zasady działania inteligentnego kontraktu. W rzeczywistości w tego rodzaju maszynach nie implementuje się mechanizmu „smart contracts”, natomiast kontrakty takie możemy coraz częściej zawierać w sieci.

W dzisiejszych czasach, kiedy każdy z nas nosi w kieszeni komputer, internet jest właściwie wszędzie, a kryptowaluty stały się codziennością, inteligentne kontrakty pozwalają na znacznie bardziej skomplikowane działania. Umożliwiają przeprowadzanie zaufanych transakcji i umów pomiędzy różnymi, często anonimowymi stronami bez potrzeby posiadania centralnego organu, systemu prawnego lub zewnętrznego mechanizmu egzekwowania.

W rewolucji związanej z blockchainem i inteligentnymi kontraktami nie chodzi jednak o całkowite wyparcie regulatora. Trudno sobie wyobrazić, żeby w niedalekiej przyszłości system prawny mógł obyć się

bez organów urzędu jako gwaranta sprawiedliwości i bezpieczeństwa. Faktem natomiast jest, że ze względu na sposób swojej konstrukcji smart contract uniemożliwia łamanie zapisów umowy i automatyzuje cały proces jej przestrzegania, a to ogromny krok naprzód, który przyczynia się do wciąż rosnącego zainteresowania i chęci rozwoju tej technologii.

Jakie są realne przykłady jej użycia i jak prezentuje się smart contract w całej okazałości? Przyjrzyjmy się zbiórce crowdfundingowej. Jedna ze stron oferuje udziały w przedsięwzięciu. Dotacje są realizowane przez odpowiednio zaprogramowany, niezmienialny kod. Osoba zbierająca pieniądze nie otrzyma środków, dopóki nie zabezpieczy inwestorów udziałami oraz nie wypełni odpowiednich punktów kontraktu. Co więcej, w przypadku niepowodzenia lub próby oszustwa wszystkie pieniądze zostaną zwrócone biorącym udział w zbiórce, bo są przetrzymywane na osobnym koncie, do którego dostęp ma tylko smart contract, i nie przeleje ich do zbierającego, dopóki ten nie wywiąże się z umowy.

Tego typu działania wykluczają ryzyko defraudacji do minimum. Nawet wysłanie paczki może być lepsze dzięki inteligentnej umowie! Kurier podaje swój adres portfela Ethereum. Tworzycie umowę w Ethereum Blockchain i wpłacasz na nią środki za dostarczenie paczki, załóżmy, że chodzi o wartość jednego Ethereum. Kurier sprawdza, czy umowa rzeczywiście opiewa na jeden Ether (ETH) i wyrusza w drogę dostarczyć twoją przesyłkę. Gdy paczka dotrze do odbiorcy, a ten potwierdzi jej prawidłowość, smart contract wysyła 1 ETH na internetowy portfel kuriera. Umowa zrealizowana. Żadnych reklamacji i niepotrzebnych sporów.

Kolejnym dobrym przykładem zastosowania koncepcji smart contract jest umowa ubezpieczeniowa. Po stłuczce z udziałem np. dwóch kierowców, odpowiednie służby wskazują jedną ze stron winną spowodowania wypadku, która musi pokryć koszty powstałe na skutek wyrządzenia szkody ze swojego ubezpieczenia. Rozwiązywanie tego rodzaju sporu jest często bardzo powolne i żmudne. Z pomocą inteligentnych kontraktów może się to stać znacznie szybsze. Trudno to zrobić samodzielnie, ale jeśli inteligentna umowa jest skonfigurowana z odpowiednią polityką, dokumentami i sposobami przechwytywania danych, może zostać wykonana sama wkrótce po wypadku.

To, co dzisiaj zajmuje nawet kilka miesięcy, może przy pomocy dobrej inteligentnej umowy zostać rozwiązane w ciągu zaledwie jednego dnia. Prace nad takimi rozwiązaniami już trwają i całkiem niedługo ich rezultaty mogą stać się naszą codziennością. Wykorzystując inteligentne kontrakty do automatyzacji pewnych zadań, zarówno w usługach, jak i handlu, jesteśmy w stanie zwiększyć płynność i opłacalność tych sektorów gospodarki.

Warto również wspomnieć o zdecentralizowanej organizacji autonomicznej, czyli DAO. Jest to złożona forma inteligentnego kontraktu, której kod zawiera regulamin zdecentralizowanej organizacji. DAO to autonomiczna jednostka, która nie posiada centralnego organu i jest zarządzana przez kod komputerowy. Taka organizacja może analizować zewnętrzne informacje i wykonywać wcześniej zaplanowane polecenia autonomicznie – bez jakiejkolwiek ingerencji człowieka. Jej działanie jest podobne do korporacji lub kraju, z tą różnicą, że nie występuje tutaj hierarchia czy szczeble zarządu. Nie istnieje także żaden podmiot, który miałby uprawnienia do podejmowania i egzekwowania decyzji. Nie ma odpowiednika zarządu przedsiębiorstwa czy rządu krajowego, Sejmu czy Senatu. Każda propozycja może zostać przegłosowana przez większość społeczności. DAO to system, który pozwala osobom i instytucjom na współpracę bez konieczności poznawania się, zaufania czy podpisywania umowy.

Złożone wersje DAO mogą znaleźć zastosowanie między innymi w systemach zarządzania tokenami, platformach social media, ale także w koordynowaniu urządzeń podłączonych do Internetu, czyli w ramach Internetu Rzeczy (Internet of Things, IOT). DAO może dotyczyć także autonomicznych usług, na przykład obsługi przejazdów, czyli ridesharingu – gdzie system autonomicznie przeprowadzałby transakcje z klientami, rozliczał się z nimi, opłacał podatki, ale także mógłby planować przeglądy u mechanika.

Przenieśmy się nieco w przyszłość, w której czwarta rewolucja przemysłowa już się dokonała. Większość maszyn działa w standardzie IOT, a sieć 5G jest dominującym standardem komunikacji, umożliwiającym milionom urządzeń na porozumiewanie się między sobą w ułamkach

sekund. Większość czynności manualnych wykonują za nas roboty i autonomiczne pojazdy. Firma A, producent półprzewodników, tworzy inteligentną umowę z określonymi z góry warunkami, które należy spełnić. Firma B, zainteresowana kupnem półprzewodników potrzebnych jej do produkcji np. autonomicznych kosiarek akceptuje umowę i staje się stroną kupującą. Osoba odpowiedzialna za złożenie zamówienia przesyła dane adresowe potrzebne do transportu, wpłaca określoną ilość wirtualnej waluty na portfel inteligentnego kontraktu i po spełnieniu tych warunków kod programu zapewni realizację umowy. Stanie się to z pominięciem całego działu sprzedaży Firmy A i osób koordynujących wysyłanie zamówienia. Automatyczny magazyn w dokach otworzy się, kontener zostanie przetransportowany na statek, a zamówione produkty wyruszą w drogę do nabywcy. Bez udziału człowieka jako kontrolera. Szybciej i przy mniejszych kosztach. Po otrzymaniu potwierdzenia o odbiorze, zapewne z autonomicznej ciężarówki, środki pieniężne zostaną wysłane do firmy A i kontrakt zakończy się. To wszystko brzmi dość futurystycznie, jednak patrząc na tempo rozwoju technologii, być może nie jest to wcale aż tak odległa przyszłość. Wróćmy do historii powstania kryptowalut.

Twórcą wspomnianej koncepcji „smart contracts” jest Nick Szabo – Amerykanin węgierskiego pochodzenia, genialny informatyk i kryptograf, który pod koniec lat dziewięćdziesiątych wystartował z projektem wirtualnej waluty o nazwie BitGold. Jak sam przyznaje, motywacją do stworzenia BitGolda była chęć zaradzenia nieefektywnościom obecnego systemu finansowego.

We współczesnych systemach gospodarczych gwarantem wartości pieniądza jest jego emitent, czyli bank centralny. Regulując ilość pieniądza na rynku programami luzowania ilościowego i stopami procentowymi władze monetarne wpływają na wartość pieniędzy. Oficjalnym celem takiej polityki jest z reguły zapisane w statutach owych banków utrzymanie koniunktury i stabilności gospodarki.

Według Szabo, aby transakcje w tradycyjnym systemie finansowym mogły się odbyć, strony muszą się wykazać dużym zaufaniem. Wartość waluty jest więc ściśle związana z zaufaniem do jej emitenta. Problem polega na tym, że wartość naszych pieniędzy zależy obecnie od zaufania

banków centralnych. Jak pokazało wiele epizodów inflacji i hiperinflacji w XX i XXI wieku, nie jest to idealny stan rzeczy. Szabo swoją koncepcją nawiązuje do systemów walutowych sprzed epoki fiducjarnej, kiedy wartość pieniądza była oparta na parytecie złota. Paradoksalnie BitGold nigdy nie miał być pieniądzem elektronicznym, jak Bitcoin.

Koncepcja została stworzona jako waluta rezerwowa do przechowywania wartości, aby wspierać inną formę waluty elektronicznej. Zasada działania miała być adekwatna do tej, która przyświecała dolarowi mającemu pokrycie w złocie. Oparcie go o kruszec wymuszało stałą podaż i wartość. Widząc jednak niedoskonałości parytetu kruszcowego, szczególnie te związane z jego kosztami wytworzenia, wydobycia czy magazynowania, Szabo w ramach alternatywy do przechowywania wartości zaproponował wartości cyfrowe. Chodziło mu o zdecentralizowaną sieć, którą można „bezpiecznie przechowywać, przenosić" i – dokładnie tak jak w przypadku złota – która będzie miała skończoną ilość bitów, o jakie będzie mógł być oparty inny pieniądz.

BitGold miał wykorzystywać różne elementy kryptografii i kopania, aby osiągnąć decentralizację. Obejmują one bloki ze znacznikami czasu, przechowujący je rejestr tytułów i generowanie nowych bloków przy użyciu dowodu pracy – tzw. proof of work. W praktyce oznacza to, że każdy użytkownik podłączony do sieci udostępnia swoją zdolność obliczeniową, przeważnie komputer, w celu rozwiązania łamigłówki kryptograficznej. Wszystkie rozwiązane łamigłówki są przesyłane przez sieć peer-to-peer, a następnie przypisywane do klucza publicznego rozwiązania łamigłówki. Szczegóły dotyczące transakcji przechowywane są w rejestrze tytułów. Każde następne rozwiązanie staje się częścią kolejnej łamigłówki, tworząc łańcuch, który łączy najnowsze rozwiązanie łamigłówki z wynikiem następnej łamigłówki, tym samym walidując bloki transakcji. W ten sposób BitGold miał działać jak rezerwy fizyczne kruszców w erze przed walutą fiducjarną.

Bez obaw, jeśli nie wszystko jest na tym etapie jasne, będziemy jeszcze omawiać ten mechanizm bardziej szczegółowo przy okazji sieci blockchain. Na razie najistotniejsze jest zrozumienie, że zamiast jednego scentralizowanego gwarantu zaufania (banku centralnego), każdy

użytkownik wykonując swój dowód pracy (czyli udostępniając moc obliczeniową swojej maszyny) staje się częścią każdej transakcji i tworzy historię sieci, zapewniając bezpieczeństwo i eliminując ryzyko fałszerstwa. Kradzież czy „nadmierny dodruk” są praktycznie niemożliwe. To rozwiązanie znalazło zastosowanie w blockchainie i jest powszechnie wykorzystywane w świecie kryptowalut.

Chociaż projekt BitGold nigdy nie został wdrożony, jest postrzegany jako bezpośredni prekursor architektury Bitcoina. Przemyślenia Nicka Szabo stworzyły fundamenty do rozwoju całej koncepcji zdecentralizowanych walut wirtualnych.

Rozdział 2. Czym jest Bitcoin?

Algorytm publicznego oraz prywatnego klucza *– stosuje się go do szyfrowania danych w internecie. Klucz publiczny używany jest do zaszyfrowania informacji, klucz prywatny do jej odczytu. Klucz publiczny jest udostępniony każdemu, kto zechce zaszyfrować wiadomość. Ponieważ klucz prywatny jest w wyłącznym posiadaniu adresata informacji, tylko on może ją odczytać.*

Nie ma jednej złotej formuły, która w pełni oddałaby naturę Bitcoina. Bitcoin nie zna granic – jest wszędzie tam, gdzie jest dostęp do Internetu. Jest globalny. Pozostaje poza wpływem regionalnej gospodarki i nie uznaje pośredników. I chociaż nie jest emitowany przez żadną centralną instytucję, taką jak rządy czy banki centralne, to stanowi podstawę całego systemu pieniądza cyfrowego. Jest zbiorem koncepcji i technologii, ale przede wszystkim kryptowalutą, czyli walutą internetową.

Użytkownicy sieci Bitcoin komunikują się bezpośrednio między sobą za pomocą specjalnego protokołu. Zawierają kontrakty, przesyłają jednostki, modyfikują bloki. Dzięki kryptowalutom mogą przeprowadzać transakcje z każdego miejsca na ziemi, bez względu na język, kulturę czy walutę, którą posiadamy w portfelu.

Podaż Bitcoina jest z góry ograniczona i wynosi 21 milionów jednostek. Dzięki temu jest odporny na inflację. Na początku kwietnia 2022 roku, czyli w momencie pisania tej publikacji, w obiegu znajdowało się 19 milionów Bitcoinów, czyli około 90% możliwej podaży. Jeden Bitcoin może być podzielony na mniejsze jednostki, do ośmiu miejsc po przecinku. Dzięki temu rozwiązaniu, niezależnie od jego przyszłej ceny (oczywiście przy założeniu, że wartość Bitcoina będzie wyższa od zera), wciąż będzie można nim płacić wszędzie tam, gdzie są akceptowane kryptowaluty. Trzeba zauważyć, że tych miejsc jest już całkiem sporo. Płatności w walutach internetowych przyjmują już tacy giganci jak Microsoft,

Starbucks czy Amazon, jednak jest to wciąż kropla w morzu internetowych transakcji. Wydaje się, że wbrew przekonaniom twórców kryptowaluty, stały się one bardziej środkiem inwestycyjnym niż płatniczym. Większość użytkowników traktuje Bitcoina i inne kryptowaluty jako inwestycję alternatywną, a nie jako formę płatności czy substytut tradycyjnych walut.

Bitcoin to także sieć – występuje w postaci zdecentralizowanego łańcucha bloków (tzw. blockchain), który opiera się na modelu komunikacji peer-to-peer, czyli takiej, która składa się z grupy urządzeń (węzłów), które zbiorowo przechowują i udostępniają pliki. W tego rodzaju sieci komunikacja odbywa się bez centralnej administracji lub serwera, co oznacza, że wszystkie węzły mają jednakową moc sprawczą i wykonują te same zadania.

Zasadnicza różnica między obydwoma systemami polega na tym, że w typowej architekturze Client-Server istnieje dedykowany serwer i konkretni klienci. Oznacza to, że wpisując np. www.facebook.pl w swojej przeglądarce, działasz jako klient, pobierasz dane z osobnego serwera i wchodzisz w interakcje z treścią, utrzymywaną i administrowaną przez inną instytucję. W peer-to-peer dane są utrzymywane przez rozproszoną sieć użytkowników, gdzie każdy węzeł, czyli każde urządzenie podpięte do Internetu, może działać zarówno jako serwer, jak i klient. Sieć jest zdecentralizowana, tzn. że nikt nie ma nad nią naczelnej władzy. Nie ma nadrzędnego właściciela czy administratora, który zarządza systemem i decyduje, ile kryptowaluty ma być w obiegu. Struktura Bitcoina uniemożliwia emisję dodatkowych jednostek, ich blokowanie lub fałszowanie.

Obecnie powszechnym rozwiązaniem w systemach transakcji jest zaufany organ centralny, który sprawdza każdą transakcję pod kątem podwójnego wydatkowania, czyli czy jedna ze stron nie wydała monety podwójnie. Jego wadą jest to, że system pieniężny zależny jest od centralnej instytucji, przez którą musi przejść każda transakcja, tak jak w systemie bankowym. Bank blokuje środki na koncie i nie pozwala, aby były wydane podwójnie. W świecie kryptowalut nie ma odpowiednika banku centralnego czy rady polityki pieniężnej. W przypadku tego systemu nie ma takiej konieczności – transakcje są ogłaszane i dostępne publicznie. Sieć

gwarantuje anonimowość każdego użytkownika, a przy okazji zapewnia transparentność – wszystkie działania są w pełni jawne, jednak przy zachowaniu anonimowości stron.

Idea rozproszonego rejestru, czyli bazy zawierającej historyczne transakcje była znana od lat, jednak to Satoshi Nakamoto jako pierwszy zastosował to rozwiązanie w kryptowalucie Bitcoin. Każdy uczestnik zgadza się na jeden chronologicznie uporządkowany zapis transakcji i każdy może sprawdzić pomiędzy jakimi kontami doszło do wymiany oraz na jaką kwotę opiewała transakcja. Co jest istotne – nie ma tutaj żadnej tajemnicy funkcjonowania systemu – Bitcoin jest otwartoźródłowy, czyli open source i każdy może poznać zasady jego działania. Oczywiście niezbędna jest wiedza z zakresu informatyki i kryptografii, jednak w przeciwieństwie do tradycyjnego modelu bankowości, nie ma tutaj skomplikowanych schematów i zależności czy tajemnic w zakresie funkcjonowania.

Bitcoinowa społeczność może mieć również wpływ na zmiany w protokole kryptowaluty – są one bowiem przeprowadzane demokratycznie – decyduje większość. Każdy może zgłosić swój pomysł na ulepszenie sieci Bitcoina! Wystarczy wpisać w wyszukiwarkę Bitcoin Improvement Proposal i na odpowiedniej stronie podzielić się swoimi przemyśleniami.

Bitcoina i inne kryptowaluty można kupić na giełdzie lub w kantorze kryptowalut. Kursy zależą przede wszystkim od popytu i podaży. Większość z nich cechuje płynny kurs wymiany. W wyniku spekulacji inwestorów często zdarza się, że występują nawet kilkuprocentowe różnice kursowe tych samych kryptowalut na poszczególnych giełdach. Tak samo jak w przypadku tradycyjnych giełd papierów wartościowych, opłaty za transakcje, wypłaty czy depozyty, mogą się różnić pomiędzy pośrednikami. Każda giełda kryptowalutowa ma swój własny cennik na stronie internetowej. Wszystkie legalnie działające giełdy wymagają weryfikacji użytkowników. Konieczne jest więc wysłanie skanu dowodu osobistego lub innego dokumentu, potwierdzającego tożsamość oraz rachunków lub wyciągów z banku. Niektóre giełdy kryptowalutowe mogą poprosić Cię o zrobienie sobie zdjęcia z dokumentem lub przeprowadzenie krótkiej wideorozmowy w celu weryfikacji tożsamości.

Przy wyborze giełdy kryptowalutowej istotna jest także jej reputacja, bowiem w historii wielokrotnie dochodziło do włamań i kradzieży Bitcoinów przez cyberprzestępców. Ostatecznie cenę ponosili oczywiście klienci, dlatego tak ważne jest, aby uważnie dobierać platformy tradingowe.

Kolejnym miejscem, gdzie możemy kupić kryptowaluty są kantory. Ich funkcjonowanie jest podobne do klasycznych kantorów internetowych. Wystarczy założyć konto i zasilić je dowolną sumą pieniędzy, a następnie dokonać płatności za wybraną kryptowalutę.

Bitcoina można kupić także za fizyczną gotówkę. W wielu centrach handlowych możemy spotkać się z maszynami z szyldem „Bitomat". Jest to nic innego, jak bankomat do Bitcoinów. Maszyny znajdują się w największych polskich miastach. Ich zaletą – w przeciwieństwie do giełdy – jest fakt, że oferują niemal całkowitą anonimowość. Jeśli zależy nam na jej zachowaniu musimy jednak liczyć się z dodatkowymi kosztami. Kurs wymiany w bitomacie nie będzie tak korzystny jak na giełdzie czy w kantorze. Bitomaty pobierają również większą prowizję.

Bitcoina można także pozyskać we własnym zakresie. Powstają one bowiem w procesie tzw. kopania (od ang. słowa mining). Jest to analogia do wydobywania paliw kopalnych, tylko że w przypadku kryptowalut proces ten odbywa się za pomocą sprzętu rozwiązującego skomplikowane obliczenia. To cyfrowi górnicy odpowiadają za utrzymanie sieci Bitcoin, a ich wirtualnym kilofem jest komputer.

Kopacze udostępniają wysoką moc obliczeniową swoich maszyn, dzięki czemu mogą zachodzić transakcje w sieci Bitcoin. W zamian za wkład wniesiony w utrzymanie sieci (ang. proof of work – dowód pracy), kryptogórnicy wykopują nowe Bitcoiny, które wynagradzają im trud wniesiony w funkcjonowanie społeczności. Sprowadza się to do rozwiązywania matematycznych problemów, dotyczących przetwarzania transakcji z wykorzystaniem Bitcoinów.

Górnicy kryptowalut – a raczej ich komputery – pełnią także funkcję audytora. Sprawdzają transakcje i zapobiegają powstawaniu problemu podwójnego wydatkowania środków. Wszystkie nowe transakcje

trafiają do węzłów sieci kryptowaluty i są przechowywane w puli niezweryfikowanych transakcji. Górnicy tworzą nowy blok, gdzie weryfikowana jest ich poprawność. Po osiągnięciu limitu pamięci bloku, wszystkie zweryfikowane transakcje dokonane w sieci są w nim zamykane, a następnie wysyłane do księgi z transakcjami, czyli rozproszonej historii wszystkiego, co działo się w sieci Bitcoin. Właśnie to rozwiązanie gwarantuje bezpieczeństwo.

Wszyscy uczestnicy sieci Bitcoin są jednocześnie powiernikami jej historii. Gdyby pojawił się fałszerz z innymi danymi, zostanie on automatycznie odrzucony przez większość. Złamanie tego zabezpieczenia jest właściwie niemożliwe.

Jak już było wspomniane – za swoją pracę, czyli udostępnienie mocy obliczeniowej swoich urządzeń, sieć nagradza górników nowymi jednostkami kryptowalut. Zgodnie z konstrukcją Bitcoina ta nagroda będzie się zmniejszać. Co jakiś czas w sieci dochodzi do zjawiska tzw. halvingu, czyli zredukowania emisji nowych Bitcoinów. Dzieje się to automatycznie co 210 000 wydobytych bloków, redukując emisję o połowę. Ostatni halving był trzecim z kolei i miał miejsce 11 maja 2020 roku. Skutkował zmniejszeniem nagrody za rozwiązanie bloku z 12,5 do 6,25 Bitcoina. To rozwiązanie ma zabezpieczyć Bitcoina przed inflacją, ale bezpośrednio wpływa także na jego wycenę. Wraz ze spadkiem nowej podaży następuje także spadek opłacalności wydobywania Bitcoina. Ograniczenie podaży powoduje, że w sieci jest coraz mniej kryptowaluty „do wydobycia”, a co za tym idzie, koparka potrzebuje zużyć więcej energii, zanim otrzyma nagrodę. Proces kopania jest całkowicie losowy. Górnicy nie mają żadnej gwarancji, że akurat ich obliczenia doprowadzą do powstania nowego bloku w sieci. Przyszli beneficjenci liczą więc na prawdopodobieństwo wykopania kryptowaluty. Udostępniając moc obliczeniową nie podpisują żadnej umowy i nie dostają stałego wynagrodzenia. Ryzyko to jest wpisane w zawód kryptogórnika i każdy podejmujący się pracy w tej branży musi się z nim liczyć.

Przez rosnące koszty wydobycia niektórzy górnicy nie sprzedają swoich kryptowalut zaraz po ich otrzymaniu. Licząc na wzrost kursu

Bitcoina w długim terminie, zaczynają je akumulować i trzymać w swoich portfelach, odraczając realizację zysków.

Kurs Bitcoina podczas dwóch poprzednich halvingów gwałtownie wzrastał – po zmniejszeniu nowej emisji jego wycena poszybowała odpowiednio o 8300% i 300%. Pierwszy halving miał miejsce w listopadzie 2012 roku. Zgodnie z założeniem doszło do obniżenia nagrody o połowę z 50 do 25 Bitcoinów – w tym czasie jeden Bitcoin był wyceniany na 12,5 dolara. Kolejny przewidziany jest na 2024 rok. Nagroda spadnie wówczas z 6,25 do 3,125 Bitcoina. Szacuje się, że ostatni halving będzie miał miejsce dopiero po 2140 roku.

Wraz z wydobywaniem nowych Bitcoinów wzrasta także poziom skomplikowania zadań do rozwiązania. Na początku, aby zostać górnikiem wystarczył komputer domowy z dobrą kartą graficzną, jednak wraz z rozwojem sieci Bitcoin i pojawieniem się nowych górników, konieczny był zakup lepszej karty graficznej. Kopiący kryptowaluty powinni posiadać mining rig, czyli specjalny system komputerowy dedykowany do wydobywania kryptowalut. Wyróżnia on dwie metody wydobywania Bitcoinów: CPU i GPU Mining.

Pierwsza metoda opiera się na mocy procesora i ze względu na rozrost sieci przestała być już opłacalna – domowe komputery posiadają zbyt małą moc obliczeniową, żeby konkurować z profesjonalnymi kopalniami.

Metoda GPU Mining polega na zastosowaniu kart graficznych do wykopywania Bitcoina i to właśnie z tej metody korzysta najwięcej górników. Profesjonaliści zaczęli inwestować w koparki, czyli specjalnie skonfigurowany sprzęt, składający się z kart graficznych, które służą wyłącznie do wydobywania Bitcoinów i innych kryptowalut. Zysk kryptogórnika jest pomniejszany o koszty zużytej energii elektrycznej i utrzymania koparki.

Bitcoiny i wszystkie inne kryptowaluty przechowywane są w portfelach kryptowalut. Nie są one podobne do zwykłych skórzanych portfeli, które znamy z życia codziennego – jest to specjalne oprogramowanie lub urządzenie fizyczne, które przechowuje adresy i

klucze prywatne. Portfele służą do przesyłania, otrzymywania i przechowywania kryptowalut. Pełnią istotną rolę skarbca e-waluty. Od jego wyboru zależy poziom bezpieczeństwa oraz jakość i komfort obsługi transakcji. Przenoszenie środków pieniężnych między portfelami jest łatwe i tanie, dlatego można rozważyć wypróbowanie kilku e-portfeli i znalezienie idealnego, który najlepiej odpowiada naszym potrzebom.

Niektórzy użytkownicy korzystają z giełd i platform, trzymając na nich swoje środki. Takie rozwiązanie nie jest w pełni bezpieczne. Niesie ze sobą ryzyko związane z przekazaniem klucza prywatnego portfela osobom trzecim, które zajmują się administrowaniem platformy lub giełdy kryptowalut. W przeszłości dochodziło do wielu włamań i wykradania kluczy, co skutkowało utratą setek milionów dolarów przechowywanych w formie kryptowalut. Podobne ataki mają i zapewne wciąż będą miały miejsce, dlatego najlepiej w ogóle nie korzystać z takiego rozwiązania, a wszystkie swoje kryptowaluty trzymać w specjalnie przeznaczonych do tego portfelach.

Żeby zrozumieć ideę portfeli kryptowalut, należy wcześniej zapoznać się z pojęciami klucza prywatnego i klucza publicznego. Są to ciągi liter i liczb wykorzystywanych w szyfrowaniu transakcji.

Klucz publiczny możemy porównać do numeru konta bankowego – można go ujawnić, twoje środki nie będą po tym zagrożone. Jeżeli twój znajomy chce ci przesłać Bitcoiny, musi znać twój klucz publiczny. Co ciekawe i znacząco odróżniające portfel kryptowalutowy od zwykłego konta bankowego – jego stan jest jawny i każdy, kto zna klucz publiczny, będzie mógł sprawdzić, ile kryptowaluty posiada dany portfel. Nie każdy będzie jednak miał możliwość zidentyfikowania ciebie jako posiadacza tego konkretnego portfela. Nadal pozostajesz anonimowy, ponieważ publicznie nie jesteś powiązany ze swoim portfelem. Dopóki nie ujawnisz, że dany ciąg znaków identyfikujący portfel należy do Ciebie, nikt nie będzie o tym wiedział.

Jeśli zaś chodzi o klucz prywatny, to można porównać go do hasła, za pomocą którego logujesz się do swojego konta bankowego. Przy użyciu klucza prywatnego podpisujesz i zatwierdzasz każdą transakcję w sieci. To

dowód na to, że jesteś właścicielem kryptowalut i masz pełne prawa do dysponowania nimi.

Zastanawiasz się pewnie, co się stanie, jeżeli zgubisz klucz prywatny? Wtedy nieodwracalnie utracisz dostęp do swojego klucza publicznego i nie będziesz mógł zarządzać swoimi Bitcoinami. W świecie kryptowalut nie istnieje odpowiednik infolinii, na której da się odzyskać hasło do konta bankowego, dlatego musisz go bardzo pilnować. Utrata dostępu do klucza prywatnego jest równoznaczna z utratą zgromadzonych kryptowalut. Istotne jest więc przechowywanie klucza prywatnego w bezpiecznym miejscu.

Na rynku kryptowalut można wyróżnić dwie grupy portfeli. Pierwsza z nich dotyczy hot wallet – gorącego portfela, czyli specjalnego oprogramowania, które można zainstalować na komputerze lub smartfonie. Zaletą takiego programu jest możliwość zarządzania swoimi środkami właściwie w każdym momencie. Z drugiej strony, w dobie mobilnego internetu, urządzenia te cały czas pozostają podłączone do sieci, przez co narażone są na hakowanie kluczy prywatnych przez cyberprzestępców. Pojawia się też ryzyko utraty (np. kradzieży lub zgubienia) urządzenia z zainstalowaną aplikacją. Do swojego portfela można zalogować się także za pomocą przeglądarki internetowej – jest to rozwiązanie zbliżone do tego, które znamy z internetowego konta bankowego, gdzie występuje administrator strony, zarządzający dostępem do portfela. W takim przypadku operator serwisu ma dostęp do naszych kluczy prywatnych, co również wiąże się z ryzykiem utraty środków przez ataki hakerów. Należy także uważać na aplikacje, które mogą udawać program do obsługi portfela kryptowalut. Hakerzy tworzą perfekcyjne kopie stron do logowania. Od oryginału ich adresy URL odróżnia najczęściej zmiana jednej litery lub kolejności ich występowania w szyku. Wykorzystując ludzką nieuważność cyberprzestępcy zdobywają dane potrzebne do zalogowania. Użytkownik wypełnia formularz, klika przycisk „zaloguj” i w tym momencie jego nazwa oraz hasło są przesyłane na hakerski serwer – jest to tzw. atak phishingowy.

Druga grupa portfeli, czyli cold wallets (w tłum. zimne portfele) to głównie akcesoria sprzętowe takie jak karty, pendrive’y czy kości pamięci,

na których w formie bitów i bajtów zapisane są wszystkie zgromadzone środki. Dopóki taki portfel jest odłączony od komputera z dostępem do Internetu, dopóty pozostaje on niewrażliwy na jakiekolwiek formy cyberataków. Portfele zimne uznawane są za najbezpieczniejszą formę przechowywania kryptowalut. Po podłączeniu do komputera i autoryzacji, która zazwyczaj polega na podaniu kodu PIN, będziemy mieli dostęp do naszych środków. Warto w tym momencie podkreślić, że zawsze trzeba kłaść nacisk na maksymalne skupienie podczas wykonywania transakcji, zarówno tych „zwykłych" – bankowych, jak również tych z wykorzystaniem kryptowalut. Nie trzeba wyjaśniać, co wydarzy się, jeśli pomylimy numer konta w przypadku standardowego przelewu. Wspomnieć jednak należy, że w świecie kryptowalut istnieje złośliwe oprogramowanie, które może podmienić adres portfela docelowego, dlatego przed wysłaniem Bitcoinów do znajomego warto kilkakrotnie sprawdzić, czy jego adres (tzn. klucz publiczny) jest poprawny.

Ryzyko utraty środków zapisanych w portfelu cold wallet związane jest głównie z właścicielem i ogranicza się do utraty bądź zniszczenia nośnika. Jeżeli zgubimy takie urządzenie, to jeszcze nic nie jest stracone. Możemy odzyskać dostęp do klucza prywatnego i naszych kryptowalut, jeżeli zapamiętaliśmy lub zapisaliśmy ciąg słów, który generowany jest podczas pierwszego uruchamiania.

Kolejnym sposobem na przechowywanie kryptowalut jest zwykła kartka papieru. Wystarczy wydrukować na domowej drukarce klucz prywatny i klucz publiczny, które wyglądają jak długi losowy ciąg znaków. Jest to jeden z najlepszych i najbezpieczniejszych sposobów na przechowywanie kryptowalut – jedyne o czym musimy pamiętać to to, gdzie odłożyliśmy kartkę z wydrukowanymi kluczami. Należy wziąć pod uwagę, że papier to delikatny materiał. Istnieje ryzyko zalania go kawą, a tusz wystawiony na działanie promieni słonecznych może wyblaknąć. Korzystanie z tego rozwiązania nie jest może zbyt wygodne i nie nadaje się do wykonywania codziennych płatności, jednak zaletą kartki papieru jest jej duża mobilność i fakt, że zapewnia najwyższy poziom bezpieczeństwa wirtualnego. Wciąż jednak istnieje ryzyko wykradzenia samej kartki – dokładnie tak, jak gotówki z sejfu.

Wybór portfela kryptowalut należy do ciebie. Powinien być dostosowany do twoich potrzeb, częstotliwości korzystania ze zgromadzonych środków oraz – co najważniejsze – musi być spójny z Twoimi przyzwyczajeniami dotyczącymi zachowania ostrożności w sieci. Przy tym wyborze najważniejsze jest bowiem to, jak bardzo cenisz sobie bezpieczeństwo i spokój ducha.

Wybrana bibliografia

- Ammous Saifedean, *The Bitcoin Standard: The Decentralized Alternative to Central Banking*, John Wiley & Sons, 2018,
- Booth Jeff, *The Price of Tomorrow: Why Deflation is the Key to an Abundant Future*, Stanley Press, 2020,
- Pritzker Yan, *Inventing Bitcoin: The Technology Behind The First Truly Scarce and Decentralized Money Explained*, Amazon Digital Services LLC - KDP Print US, 2019,
- Nakamoto Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf
- Chaum David, *Blind signatures for untraceable payments*, Springer Science+Business Media New York, 1983,
- Kabarowski Tomasz, Wójcik Piotr, *Kryptowaluty od zera*, Novae Res, 2020,
- Kopańko Karol, Kozłowski Mateusz, *Bitcoin. Złoto XXI wieku*, Onepress, 2014,
- Szymankiewicz Marcin, Bitcoin. *Wirtualna waluta internetu*, Onepress, 2014,
- Antonopoulos Andreas M., *Bitcoin dla zaawansowanych. Programowanie z użyciem otwartego łańcucha bloków. Wydanie II*, Wydawnictwo Helion, 2018,
- Markowski Krzysztof Rafał, *Kryptowaluty. Powstanie – typologia – charakterystyka*, Civitas et Lex, 2019,
- Van Wirdum Aaron, The Genesis Files: If Bitcoin Had a First Draft, Wei Dai's B-Money Was It, Bitcoin Magazine, 14.06.2018, online

Podczas pisania tej książki autorzy korzystali także z bardzo wielu źródeł internetowych. Aby otrzymać ich pełną listę prosimy o kontakt z wydawnictwem.