Program „Od papierowej do cyfrowej Polski”

Strumień „Blockchain i kryptowaluty”

LEKSYKON POJĘĆ NA TEMAT TECHNOLOGII BLOCKCHAIN I KRYPTOWALUT

prof. Krzysztof Piech (red.)

2016-11-08

Dokument nie odzwierciedla poglądów Ministerstwa Cyfryzacji ani rządu Rzeczpospolitej Polskiej.

Spis treści

Architektura sieci

W początkach informatyzacji obliczenia i dane były przechowywane głównie lokalnie, na jednym komputerze. Wraz z rozwojem technologii komunikacyjnych, komputery łączono w sieci.

Podstawowe tewrminy:
- Sieć – zbiór wzajemnie powiązanych węzłów, które wymieniają ze sobą informacje.
- Węzeł (node) – podstawowa część sieci, np. użytkownik (lub komputer).
- Powiązanie – połączenie pomiędzy dwoma węzłami.
- Serwer – węzeł, który ma połączenia do dość dużej liczby innych węzłów.

Są trzy podstawowe typy sieci komputerowych:
- scentralizowana
- zdecentralizowana
- rozproszona

Sieć scentralizowana to taka, w której wszystkie węzły wysyłają swoje dane do centralnego węzła (tj. do serwera), który wysyła dane do odpowiednich węzłów. W przypadku awarii serwera taka sieć nie działa.

Sieć rozproszona nie posiada centralnego serwera, a dane przekazywane są pomiędzy węzłami po możliwie najkrótszych trasach.

Sieć zdecentralizowana jest rodzajem rozproszonej sieci scentralizowanych sieci. Niektóre z węzłów mają charakter super węzłów (*super nodes*), ale nie są centralnymi serwerami.

Różnice pomiędzy sieciami najlepiej zobrazuje słynny rysunek autora tej typologii:

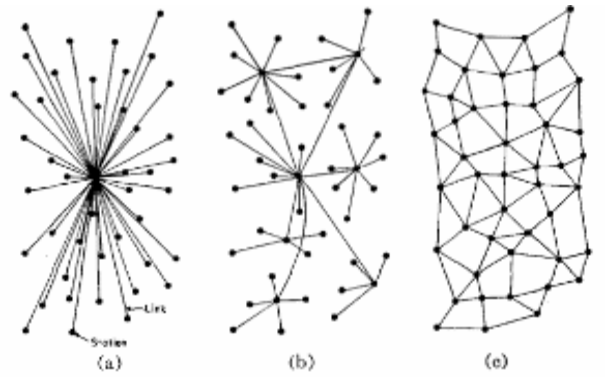


Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.

Źródło: P. Baran, *On Distributed Communication Networks*, Rand Corporation, 1962, s. 4.

Bitcoin

Bitcoin (w znaczeniu waluty – z małej litery) pełni dwie funkcje:
1. dotyczącą całego systemu płatności oraz
2. sposobu jej realizacji za pomocą tokenu cyfrowego.

System bitcoina został zaprojektowany przez Satoshiego Nakamoto[1] w taki sposób, aby możliwe były bezpośrednie transakcje pomiędzy użytkownikami, tj. bez pośrednictwa tzw. trzeciej strony (np. banku). Transakcje weryfikowane są przez węzły sieci (*nodes*) i zapisywane w publicznym, zdecentralizowanym rejestrze zwanym blockchain. Jednostki miary transakcji w systemie Bitcoin nazywane są bitcoinami. Dzielą się one do ośmiu miejsc po przecinku. Najmniejsza jednostka bitcoina (tj. 0,00000001 BTC) nazywa się satoshi.

W systemie Bitcoin nie ma centralnego emitenta bitcoinów, centralnego skarbca, władz czy administratorów. Podaż bitcoinów

1 Nakamoto S., Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, https://bitcoin.org/bitcoin.pdf.

regulowana jest nie przez banki centralne, ale algorytm komputerowy w sieci peer-to-peer. Są one „uwalniane" do sieci (obecnie 12,5 BTC co ok. 10 minut). Bezpieczeństwa systemu strzeże rozproszona sieć wyspecjalizowanych urządzeń (tzw. **koparek**) rozmieszczonych w różnych miejscach na świecie o łącznej mocy obliczeniowej ponad 1000 razy większej niż 500 największych superkomputerów razem wziętych. Dlatego uważa się tę kryptowalutę za jednocześnie najbezpieczniejszą.

Właściciele sprzętu udostępnionego do autoryzowania transakcji mogą uzyskać za to „wynagrodzenie" (w postaci bitcoinów). Jego otrzymanie jednak nie jest pewne (zależy od udziału danego sprzętu w ogólnej mocy obliczeniowej całej sieci). „Górnicy" (*miners*) wynagradzani są również w postaci opłat transakcyjnych (*fee*), które mogą być (opcjonalnie) dodawane do transakcji.

Bitcoiny nie muszą być wyłącznie cyfrowe – mogą być też przechowywane na papierze (*paper wallet*), a także w formie fizycznych żetonów. Wymieniać się nimi można również off-line (bez dostępu do internetu). Istnieje też możliwość przechowywania bitcoinów w pamięci człowieka (*brainwallet*).

Blok

Block jest podstawowym elementem składowym w technologii łańcucha bloków tzw. blockchain.

Składa się on z nagłówka i danych (transakcje). W nagłówku mamy m.in. zapisane odniesienie do poprzedniego bloku w łańcuchu (jego skrót, ang. hash), znacznik czasowy utworzenia bloku oraz korzeń drzewa haszy (*merkle tree root*) transakcji zawartych w bloku. W bloku danych mamy drzewo haszy transakcji zawartych w bloku, a następnie same transakcje.

Taki sposób zapisu pozwana na wyszukiwanie transakcji po jej haszu, bez konieczności odczytu wszystkich danych (odczytujemy tylko nagłówki i drzewa haszy).

Blockchain

(polski odpowiednik: „łańcuch bloków" rzadko używany, wcześniejsza pisownia też „block chain")

Blockchain to rozproszona baza danych, która zawiera stale rosnącą ilość informacji (rekordów) pogrupowanych w bloki i powiązanych ze sobą w taki sposób, że każdy następny blok zawiera oznaczenie czasu (*timestamp*), kiedy został stworzony oraz link do poprzedniego bloku, będący zaszyfrowanym „streszczeniem" (*hash*) jego zawartości.

Ponieważ każdy blok transakcji zawiera odwołanie do bloku poprzedniego, nie ma możliwości zmiany transakcji zawartej wcześniej w jakimś bloku bez modyfikacji wszystkich następujących po nim bloków. W ten sposób tworzony jest nierozerwalny łańcuch bloków danych (czyli blockchain). Dzięki niemu dokonanie jakiejkolwiek zmiany w zapisach historycznych (bez zmiany całej historii transakcji) jest niemożliwe.

Aby uniemożliwić takie „cofnięcie" czy zmianę w systemie bitcoin zastosowano rozwiązanie oparte na „dowodzie pracy" (proof-of-work, PoW), który jest wymagany do zatwierdzenia bloku transakcji.

Technologia blockchain została po raz pierwszy użyta w 2009 r. w kryptowalucie bitcoin, jako

sposób księgowania wszystkich transakcji nią dokonywanych bez możliwości podwójnego wydania (*double spend*) tych samych środków. Blockchain bitcoinowy ma charakter publiczny (każdy może mieć do niego dostęp, wziąć udział w tworzeniu nowych bloków).

Istnieją trzy podstawowe rodzaje blockchainów:

1. **Publiczny**, którego najbardziej znanym przykładem jest blockchain bitoina. Główna jego funkcjonalność: każdy może pobrać dowolny fragment lub całość bazy danych oraz zazwyczaj ma prawo udostępniać swoją kopię innym węzłom (NOD'om).
2. **Prywatny**. Jego główna funkcja związana jest z tym, że blockchain ten może pobierać / udostępniać jedynie wybrana grupa podmiotów. Prywatny blockchain wykorzystywany jest, gdy sieć biznesowa zawiera poufne dane lub gdy regulacje prawne nie pozwalają poszczególnym członkom na korzystanie z Blockchaina publicznego. Przykładem blockchaina prywatnego jest R3 Corda lub Hyperledger.
3. **Hybrydowy**. Teoretyczny przykład blockchaina hybrydowego, to sieć prywatna z własnym protokołem konsensusu i mechanizmami kontroli dostępu do rejestru, ale korzystająca z blockchaina publicznego w celach rozliczeniowych, w celu potwierdzenia istnienia danego stanu w danym czasie (*proof of existence*) lub do wykorzystania kryptowaluty.

Zgodnie z innym podziałem blockchain może być:

- Udostępniany uczestnikom tej sieci za uprzednią zgodą (***permissioned***). Jest to rodzaj blockchaina przewidziany raczej do zastosowań korporacyjnych, gdzie liczba członków sieci (np. banków wraz z regulatorami i innymi podmiotami, do których ma się zaufanie) może być ograniczona.
- Udostępniany każdemu (permissionless). Taki charakter ma przykładowo blockchain bitcoinowy. Jest to rozwiązanie oparte na demokratycznym konsensusie – 51% członków sieci (węzłów) ma rację, a głos każdego z nich jest równy[2] co do udziału w mocy obliczeniowej sieci.

Oryginalny blockchain bitcoinowy ma charakter niezaprzeczalny (***immutable***). Oznacza to, że można było do niego jedynie dodawać informacje, a nie korygować istniejące[3]. Pojawiła się też koncepcja korygowalnych (*correctable*, ***editable***) blockchainów, umożliwiających ingerencję w dane historyczne. Takim przykładem jest blockchain firmy Accenture, przygotowany z myślą o zastosowaniach w firmach.

Rozwiązanie takie nie zostało przyjęte z entuzjazmem środowiska kryptowalutowego argumentującego, że niezaprzeczalność transakcji nie jest wadą blockchaina, a jego ważną cechą[4] oraz że rozwiązanie to wymaga zaufanej trzeciej strony, której potrzebę istnienia oryginalny blockchain wyeliminował.

DAO

Zob. Zdecentralizowana Autonomiczna Organizacja. Najbardziej znanym przykładem jest The DAO.

2 W blockchainie bitcoinowym „dzieci w Kenii mają ten sam poziom dostępu, co szef FEDu". P. Włodarek, *Enterprise blockchains are a HUGE overpromise*, 2 listopada 2016 r., https://medium.com/@qertoip/enterprise-blockchains-are-a-huge-overpromise-7ca2d19324b3#.fxpf7ykz1.

3 Choć należy tu wspomnieć o tzw. hard-forkach. Najbardziej chyba znany wystąpił w sieci Ethereum w lipcu 2016 r. i był odpowiedzią na problemy związane z wyprowadzeniem części środków z The DAO.

4 B. Kelly, *The Case Against Editable Blockchains*, CoinDesk, 30 września 2016 r., http://www.coindesk.com/sorry-accenture-bitcoins-un-editable-blockchain-feature-not-flaw/.

Distributed Ledger Technology (DLT)

Zob. Technologia rozproszonego rejestru.

Dowód wykonania pracy

Ang. Proof of Work (PoW). Mechanizm, dzięki któremu sieć Bitcoin rozwiązuje „problem bizantyjskich generałów”. Jest to protokół osiągania konsensusu w większości kryptowalut.

PoW wymaga od węzła zatwierdzającego blok transakcji znalezienie rozwiązania równania, którego wynik musi mieć wartość niższą niż aktualna wartość trudności. Ponieważ rozwiązanie jest wartością losową, węzeł musi go szukać metodą prób i błędów.

Im większa jest moc obliczeniowa węzłów zatwierdzających, tym wyższa jest trudność równania. Algorytm reguluje trudność tak, aby średnia częstotliwość zatwierdzania bloków transakcji była stała.

Zwiększanie mocy obliczeniowej przeznaczanej na PoW powoduje zwiększanie bezpieczeństwa zatwierdzonych transakcji, bo do zmiany zatwierdzonej w bloku transakcji wymagane jest wykonanie wszystkich obliczeń potrzebnych do zatwierdzenia zawierającego ją bloku i wszystkich kolejnych bloków.

Na pewnym poziomie trudności, z ekonomicznego punktu widzenia, dzięki nagrodzie za zatwierdzenie bloku węzłowi zatwierdzającemu transakcje bardziej opłaca się poprawnie zatwierdzać kolejne bloki, niż modyfikować wcześniej zatwierdzone transakcje.

Ethereum

To publiczna, zdecentralizowana i dystrybucyjna platforma obliczeniowa, oparta na technologii blockchain i używająca smart kontraktów. Maszyny wirtualne uruchomione w sieci P2P tworzą węzły. Maszyna Wirtualna Ethereum (EVM) pozwala na uruchamianie smart kontraktów. Żeby je uruchomić potrzebny jest tzw. gas. Ten pochodzi z konwersji kryptowaluty ether. Ją zaś można np. nabyć na popularnych giełdach kryptowalutowych.

Hasz

Ang. hash, zob. skrót.

Hyperledger

Projekt *open source* zarządzany przez Linux Foundation i funkcjonujący na zasadzie federacji współpracujących ze sobą stron. Jest podstawowym kodem używanym w produktach, usługach i rozwiązaniach blockchainowych firmy IBM.

Jego pierwotnym zastosowaniem ma być tworzenie prywatnych sieci biznesowych (prywatnych blockchainów) dla np. uczestników rynku finansowego.

Klucz publiczny, klucz prywatny

Por. też „szyfrowanie”.

W kryptografii asymetrycznej stosowanej w blockchainie polityka otwartego oraz prywatnego klucza (*public-private key*) polega w skrócie na tym, że dane zaszyfrowane za pomocą klucza A można odszyfrować tylko i wyłącznie za pomocą klucza B. Klucze A i B wiąże pewna zależność matematyczna, której nie da się odgadnąć, znając tylko klucz A lub tylko klucz B[5].

Jaki ma to wymiar praktyczny?

„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. (…)

Ten algorytm i jego pochodne mają olbrzymie znaczenie dla internetu, handlu elektronicznego oraz świata finansów. Dzięki niemu, dzięki gwarancji bezpieczeństwa przekazywanych informacji, internet staje się bezpiecznym miejscem. Za pomocą tej technologii można bardzo tanim kosztem rozwiązać problem bezpieczeństwa transmisji oraz weryfikacji prawidłowości danych. Możemy przesyłać najbardziej poufne dane nie obawiając się, że ktoś niepożądany je przeczyta lub postara się je zmienić."[6]

Konsensus

Proces, w ramach którego strony biorące udział w sieci opartej na technologii blockchain zgadzają się na przeprowadzenie transakcji zatwierdzanej przez wszystkich uczestników tej sieci. Konsensus gwarantuje integralność danych każdej kopii rejestru i zmniejsza ryzyko przeprowadzenia nieautoryzowanej transakcji

5 J. Dąbkowski, M. Olszański, *Modele i kwestie finansowe e-biznesu* [w:] K. Piech, M. Olszański (red.), *E-biznes – innowacje w usługach. Teoria, praktyka, przykłady*, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2012, s. 96.

6 Ibidem, s. 97.

poprzez zastosowanie technik kryptograficznych zawartych w protokołach konsensusu.

Nad osiągnięciem konsensusu czuwa protokół będący zbiorem technik kryptograficznych oraz logicznych. W blockchainie bitcoinowym (oraz w wielu innych) tym protokołem jest proof-of-work (PoW). Jedną z alternatyw, nad którą trwają prace, jest proof-of-stake (PoS). Zgodnie z nim dowodzi się własności danej ilości kryptowaluty i nie ma konieczności używania dużej ilości energii elektrycznej, jak to jest w PoW.

Kryptowaluta

Ang. *cryptocurrency* – rodzaj tokena cyfrowego opierającego się na kryptografii użytej do cyfrowego podpisywania transakcji oraz do kontroli wzrostu podaży tokenów. Kryptowaluty oparte są na zdecentralizowanej sieci ***peer-to-peer*** (P2P).

Kryptowaluty są to nośniki wartości. Niektóre z nich spełniają wszystkie lub niektóre funkcje pieniądza takie jak podzielność, zachowanie wartości (z pewnym zastrzeżeniem dotyczącym amplitudy wahań cen kryptowalut), wymienialność. Nie zostały jak dotąd powszechnie uznane za w pełni legalny pieniądz lub waluta.

Pierwszą, najbardziej znaną kryptowalutą, jest bitcoin. Pozostałe określa się mianem „**altcoin**y” (**a**lternatywne **coin**y).

Legalność technologii blockchain w Polsce

W prawie polskim nie obowiązuje zakaz korzystania z technologii blockchain, a zatem jest ona dozwolona i legalna. W praktyce mogą zaistnieć ograniczenia dopuszczalności jej zastosowania w tych sytuacjach, w których prawo przewiduje szczególne formy na dokonanie danej czynności (np. forma aktu notarialnego) lub wyklucza możliwość wykorzystania szeroko pojętych środków „elektronicznych”. Takie sytuacje należą jednak do wyjątków i nie wpływają na legalność technologii blockchain.

Dane zgromadzone w blockchainie, rozumianym jako rozproszona baza danych, mogą być nośnikiem oświadczeń woli. W świetle przepisu art. 60 kodeksu cywilnego (z zastrzeżeniem wyjątków) wola osoby dokonującej czynności prawnej może być wyrażona przez **każde zachowanie się tej osoby**, które ujawnia jej wolę w sposób dostateczny, w tym również przez ujawnienie tej woli **w postaci elektronicznej**.

Wykorzystanie technologii blockchain do składania oraz odbierania oświadczeń woli pociąga za sobą praktyczną możliwość zaskarżania wywołanych w taki sposób skutków prawnych – w szczególności dochodzenia roszczeń wynikających z zawartych umów. Dane zgromadzone w blockchainie mogą zostać wykorzystane **jako dowód** na okoliczność dokonania danej czynności (np. zawarcia danej umowy).

Legalność walut cyfrowych w Polsce

W prawie polskim nie obowiązuje zakaz korzystania z walut cyfrowych i zakaz tworzenia nowych walut cyfrowych. Oznacza to, że waluty cyfrowe są w pełni legalne. Problematyczne jest jednak określenie jaki status maja waluty cyfrowe, w tym w szczególności, czy należy nadać im status zrównany z tradycyjną walutą.

W Polsce brak jest aktu prawnego, który jednoznacznie definiowałby czym są wirtualne

waluty. Kwestia zdefiniowania walut cyfrowych może być uważana za sporną, ponieważ waluty cyfrowe – z uwagi na ich funkcje – mogą być uważane za pieniądz, instrument płatniczy, czy też instrument finansowy. Wynika to stąd, że walutom cyfrowym służy atrybut w postaci wartości oraz że mogą być przenoszone w drodze czynności prawnej (umowy) ze zbywcy na nabywcę.

Na gruncie prawa cywilnego, obie wskazane powyżej cechy walut cyfrowych są przewidziane w przepisach obowiązującego prawa jako elementy tworzące „inny niż pieniądz miernik wartości". W świetle przepisu art. 358^1 § 2 kodeksu cywilnego strony mogą zastrzec w umowie, że wysokość świadczenia pieniężnego zostanie ustalona według innego niż pieniądz miernika wartości. **Waluty cyfrowe** są więc jednym z przykładów innych niż pieniądz mierników wartości (jak np. metale szlachetne). **Można się więc nimi legalnie posługiwać.** Dlatego waluty cyfrowe mogą – podobnie jak pieniądze – służyć do umarzania zobowiązań, jako środki płatnicze w szerokim rozumieniu. Umowa przewidująca świadczenie przynajmniej jednej ze stron w postaci waluty cyfrowej rodzi zaskarżalne roszczenia i może być przedmiotem rozpoznania przez sąd.

Także brak jest przepisów karnych penalizujących samo użycie walut cyfrowych, czy też ich wytworzenie (wydobycie). Dyskusja na temat legalności walut cyfrowych w ujęciu prawa karnego koncentruje się na ich funkcji, nie zaś istocie prawnej. Zdarzają się przypadki wykorzystania walut cyfrowych do popełnienia przestępstwa. Nie oznacza to jednak, że samo ich używanie może być uznane za nielegalne. Korzystanie z walut cyfrowych w praktyce wymaga od organów ścigania większej wiedzy, możliwości analitycznych czy technicznych służących do identyfikacji sprawcy i jego zamiarów.

Podobnie dyskusja na temat legalności walut cyfrowych w ujęciu prawa publicznego koncentruje się na ich funkcji, nie zaś istocie prawnej. W praktyce, najwięcej kontrowersji budzą kwestie podatkowe dotyczące obrotu kryptowalutami. Zasady opodatkowania nie wpływają na status walut cyfrowych. Jednak sam fakt opodatkowania dochodów uzyskiwanych z tytułu obrotu nimi potwierdza – w sposób pośredni – legalność takich walut. Na gruncie ustaw o podatkach dochodowych, opodatkowaniu nie podlegają przychody z działalności, która nie może być przedmiotem prawnie skutecznej umowy (a więc z działalności nielegalnej). Skoro dochody uzyskane z walut cyfrowych podlegają opodatkowaniu, to są one w pełni legalne.

P2P

Peer-to-peer (osoba do osoby) – model komunikacji w sieci komputerowej, w której zadania rozdzielone są pomiędzy równe sobie pod względem uprawnień osoby (węzły). Członkowie sieci P2P współdziałają bezpośrednio miedzy sobą bez pośrednictwa centralnego serwera. Inaczej niż w architekturze klient-serwer, im więcej jest uczestników sieci P2P, tym jest ona bardziej wydajna. Przykładem może być sieć torrent.

Pieniądz cyfrowy / waluta cyfrowa

Ang. *digital money / digital currency* – środek wymiany w postaci innej niż fizyczna (w postaci banknotów i monet). Może mieć charakter nieograniczony (kryptowaluty) lub przeznaczony do specyficznych zastosowań (np. w grach czy sieciach społecznościowych – waluty wirtualne). Z reguły nie jest to „legalny środek płatniczy" (*legal tender*) konkretnego kraju, nie jest emitowany przez bank centralny ani inną władzę publiczną.

Portfel

Zbiór prywatnych kluczy lub oprogramowanie do zarządzania nimi oraz do przeprowadzania transakcji w sieci Bitcoin. Może być to aplikacja mobilna, urządzenie, serwis internetowy czy nawet kartka papieru (*paper wallet*) zawierająca daną wartość kryptowaluty.

Problem bizantyjskich generałów

Zagadnienie dotyczące uzgadniania rozważane w teorii gier, kryptografii oraz teorii systemów rozproszonych (w tym systemów wieloagentowych).

Więcej informacji: https://pl.wikipedia.org/wiki/Problem_bizantyjskich_genera%C5%82%C3%B3w

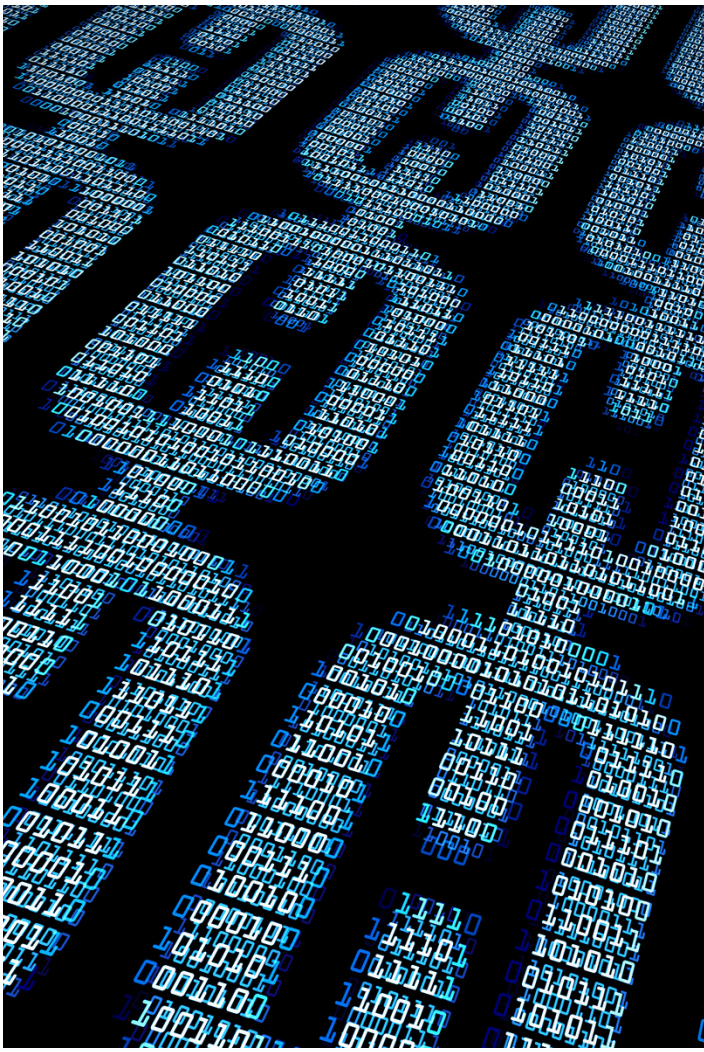
Proof of Work (PoW)

Zob. dowód wykonania pracy.

Sieć Bitcoin

Jest to jedna z dwóch funkcji bitcoina (obok funkcji pieniądza). Jest to rozproszona sieć rejestrów oparta na komunikacji przeprowadzanej za pośrednictwem sieci internet.

Węzły sieci Bitcoin opierają się na technologii blockchaina bitcoinowego. Część z nich jest zainstalowana na potrzeby tzw. kopania (tworzenia nowych bloków) i podłączona do specjalistycznego sprzętu (zwanego popularnie koparkami).



Sieć rozproszona

Jest to rodzaj sieci komputerowej, w której wykorzystywane dane są rozproszone pomiędzy węzłami. Funkcjonowanie tej sieci jest utrudnione ze względu na twierdzenie CAP, zgodnie z którym nie jest możliwe w systemie rozproszonym jednoczesne zapewnienie:

- spójności (*consistency*),
- dostępności (*availability*) i
- tolerancji podzielności (*partition tolerance*).

W takim systemie mogą być spełnione najwyżej dwie spośród ww. funkcji.

Zob. też architektura sieci.

Skrót

Inaczej hasz (ang. *hash*), czyli krótki ciąg znaków przyporządkowany do dowolnie dużego zbioru danych za pomocą funkcji mieszającej (haszującej). Z punktu widzenia założeń kryptograficznych przewidzianych w technologii blockchain najważniejsze właściwości to:

a) odporność na kolizje, czyli brak możliwości wygenerowania dwóch takich samych skrótów do różnych zbiorów danych,
b) jednokierunkowość, czyli brak możliwości poznania danych na postawie samej wartości skrótu.

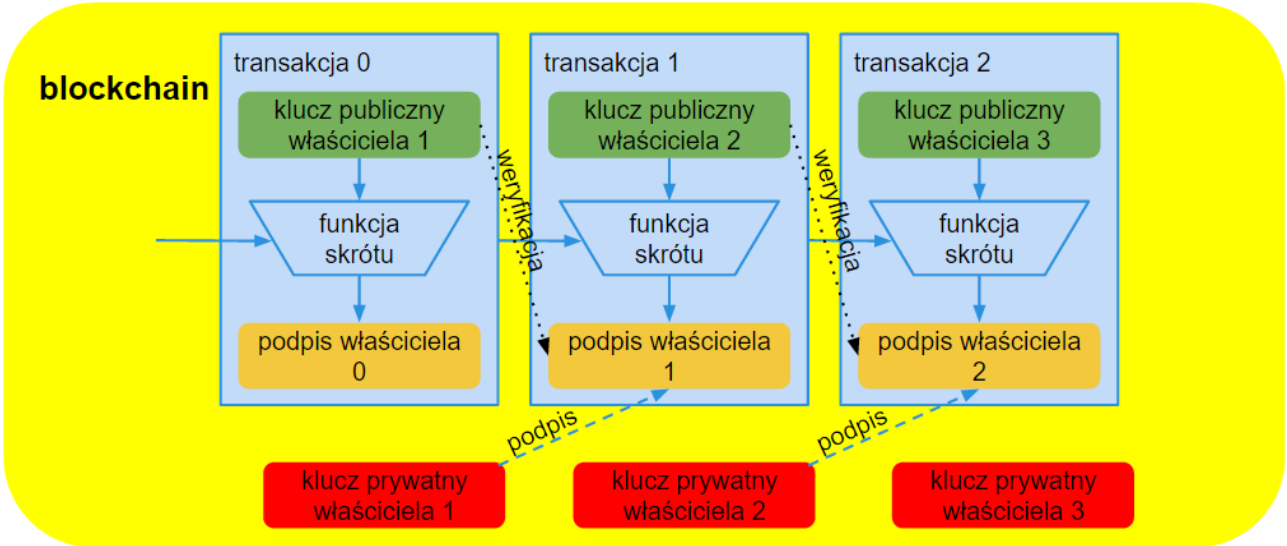
Skróty są wygodne, bo zamiast dużych ilości danych, można użyć stosunkowo krótkiego ciągu znaków np. 267bfa2dde48a4f751aa59580ba-206e07e90e43a3842dec80c1f1e3b2d4b4e3e, a później sprawdzić w blockchainie, jaka transakcja[7] przyporządkowana była do tego skrótu.

Przykładowo dodanie nawet jednej spacji do jakiegokolwiek pliku zmieni średnio aż połowę zawartości hasza takiego pliku. Przy takim rozwiązaniu nie ma potrzeby porównywania zawartości całych dokumentów, ale tylko ich skrótów cyfrowych, by szybko i niezaprzeczalnie wykryć każdą modyfikację dokumentu (np. oddanie słów „i czasopisma").

W blockchainie można przechowywać hasze dokumentów i dzięki czemu uzyskuje się niezaprzeczalny dowód na istnienie dokładnie tych dokumentów (zob. np. serwis https://proofofexistence.com/). Na podstawie takiego mechanizmu opartego na blockchainie działa np. estońska e-administracja.

Funkcje haszujące mają wiele zastosowań. Używa się ich m.in. w zakresie podpisu elektronicznego, weryfikacji integralności danych, potwierdzania wiedzy, weryfikacji hasła, stempli czasowych oraz usług kryptograficznych takich

Schemat transakcji w blockchainie



Źródło: K. Szydłowski, *Pieniądz i bitcoin. Przeszłość i przyszłość*, slajd 13 pt. „Łańcuch transakcji", https://docs.google.com/presentation/d/1iWQoN4mkM1lv2o4CyUcOIgn9KooC4asQYGvrmXYuPrgk/edit?usp=sharing, dostęp: 5.11.2016

7 Przy czym transakcją w bazach danych nazywamy każdą zmianę rejestru – również wpisanie treści. W serwisie blockchain.info można sprawdzić ww. skrót oraz jego „skrypt wyjściowy" – niespodzianka (dla zaawansowanych).

jak: poufność, integralność, uwierzytelnianie, kontrola dostępu, niezaprzeczalność.

Smart kontrakt

Ang. smart contract, inaczej: inteligentny kontrakt, inteligentna umowa.

Skompilowany kod programistyczny, którego kopia wpisana jest w rejestr blockchain (np. sieci Ethereum) i reprezentujący zasady dokonania transakcji pomiędzy stronami. Raz rozpropagowany w ramach sieci, smart kontrakt jest uruchomiony na wszystkich węzłach jako program wykonywalny i uruchamia konkretną funkcję przewidzianą przez autora.

Smart kontrakt jest cyfrową reprezentacją zasad lub procesów funkcjonujących w danej organizacji biznesowej, które regulują sposób dokonywania i przebieg transakcji. Smart kontrakty pełnią również rolę kontrolującą aktywa lub mogą wywoływać zdarzenia, ustalone za pomocą technik programistycznych (funkcje if… then… else…). Rozbudowany system smart kontraktów mający na celu autonomicznie zarządzać aktywami nazywany jest Zdecentralizowaną Autonomiczną Organizacją.

Szyfrowanie

Dla zapewnienia bezpieczeństwa technologii blockchain niezbędne jest zastosowanie zaawansowanych technologii kryptograficznych, a zatem uwzględniających szyfrowanie danych.

„Metody szyfrowania w swej istocie były takie same na przestrzeni dziejów. Polegały na stosowaniu wspólnego klucza. Nieco upraszczając, dwie osoby najpierw spotykały się osobiście, uzgadniały algorytm szyfrowania i/lub hasło, a po poufnej ich wymianie mogły bez obaw wymieniać się informacjami. Ten prosty system nie mógł jednak funkcjonować online. Sprzedawca i kupujący z reguły nie spotykają się fizycznie, nie mogą się wymienić kluczem. Do rozwoju eCommerce przyczynił się rewelacyjny wynalazek z lat 70. XX w., który doprowadził do rewolucji w metodach szyfrowania. Zaproponowano rozwiązanie, które pozwalało na bezpieczną wymianę szyfrowanych danych nawet bez wcześniejszej wymiany klucza. Nazwano to wymianą klucza Diffiego-Hellmana od nazwisk jego odkrywców, kryptografą klucza asymetrycznego, czy też – i jest to bardziej znana nazwa – **algorytmami publicznego** (otwartego) oraz **prywatnego klucza** (zwykle zwanym algorytmem RSA)."[8]

Technologia rozproszonego rejestru

Ang. *distributed ledger technology* (DLT) – technologia rozproszonej bazy danych, której rejestry są replikowane, współdzielone i zsynchronizowane w ramach konsensusu różnych osób, firm czy instytucji, także rozproszonych geograficznie (w różnych krajach).

Termin został spopularyzowany stosunkowo niedawno (styczeń 2016 r.) w raporcie Głównego Doradcy Naukowego rządu Wielkiej Brytanii[9]. Bardziej popularnym, choć o nieco węższym znaczeniu, jest pojęcie „blockchain".

8 J. Dąbkowski, M. Olszański, op. cit., s. 96.

9 *Distributed Ledger Technology: beyond block chain, A report by the UK Government Chief Scientifc Adviser*, Government Office for Science, London 2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/ file/492972/gs-16-1-distributed-ledger-technology.pdf.

Inaczej jednak niż w technologii blockchain, dane utrzymywane są raczej w formie ciągłej bez podziału na bloki. By dodać nowy zapis potrzebny jest konsensus, ale możliwy jest on do osiągnięcia między ograniczoną liczbą uczestników – walidatorów (w systemie Ripple jest ich do 200), do których trzeba mieć większe zaufanie, niż np. w blockchainie bitcoinowym[10].

Innym znanym systemem DLT (nie będącym blockchainem) jest R3 Corda™. Platforma ta korzysta z kilku cech technologii blockchain, ale została zaprojektowana – na potrzeby instytucji finansowych – zupełnie od nowa. Nie ma ona natywnej kryptowaluty, korzysta z cech blockchaina takich jak autentyfikacja, niezmienność, czy unikalność usług, ale inaczej rozwiązuje kwestie konsensusu (nie pomiędzy wszystkimi uczestnikami, a tylko pomiędzy stronami) oraz walidacji (dokonywanej przez interesariuszy, a nie wszystkich lub wybranych uczestników).

10 *Tamże*, s. 17-18.

Timestamp

Stempel czasu. Zob. znacznik czasu.

Token cyfrowy

Ang. *digital token* – przez analogię do fizycznego **żetonu**: cyfrowa reprezentacja żetonu. W zależności od jego wydawcy (wystawcy), można wyróżnić tokeny:

1. wbudowane w blockchain (tzw. natywne) oraz
2. wyemitowane przez daną stronę (z wykorzystaniem technologii blockchain lub nie) w celu późniejszego ich odkupienia (*I Owe You – IOU*).

Pierwsze z nich stanowią wartość samą w sobie. Wartość drugich zabezpieczana jest aktywami (i zaufaniem) do wystawcy. Zabezpieczeniem roszczenia mogą być np. akcje, złoto, diamenty,

ale także wyłącznie sama reputacja firmy (obietnica spłaty). Niektóre z tych aktywów można całkowicie zdematerializować (np. akcje) i zapewnić możliwość dokonywania nimi transakcji w niezaprzeczalny sposób (przez blockchain). W przypadku innych – przykładowo – za pomocą publicznie otwartych baz danych można śledzić roszczenia do nich.

Drugie z tych tokenów bywają wykorzystywane w ICO (Initial Coin Offering), czyli – wzorowanej nieco na IPO – kampanii crowdfundingowej na sfinansowanie nowego projektu kryptowalutowego polegającej na rozdysponowaniu w pierwszej partii podaży tokenów. Przykłady takich udanych akcji to np. Ethereum, Bitshares, NXT, Mastercoin, Factom.

Transakcja

Jest to rodzaj zapisu w księgach (rejestrach) określający przepływ tokenów cyfrowych lub zapis informacji.

Węzeł

Ang. node – zob. Architektura sieci.

Zaufana trzecia strona

Ang. Trusted Third Party.

Jest to osoba lub instytucja, której powierzono funkcję pełnioną zwykle przez notariusza:

- odpowiada za weryfikację tożsamości stron transakcji oraz
- potwierdza zawarcie transakcji.

Pojęcie to nabrało znaczenia zwłaszcza w przypadku dokonywania transakcji na odległość, gdy obie jej strony nie widzą się, czy nawet nie znają.

Rolę zaufanej trzeciej strony pełnią władze certyfikujące. Potwierdzają one, że dany klucz należy do danej osoby, co umożliwia używanie podpisu kwalifikowanego, tj. takiego, który jest równoważny podpisowi odręcznemu. Ponieważ zarządzają one zaufaniem, są często regulowane[11].

Uważa się, że technologia blockchain wyeliminowała konieczność istnienia zaufanej trzeciej strony do potwierdzania transakcji (choć nie do weryfikowania tożsamości stron). Blockchain nie zastępuje też czynności dokonywanych przez notariuszy.

Zdecentralizowana Autonomiczna Organizacja

Rozbudowany kod programistyczny posiadający cechy smart kontraktu, rozszerzający go o duży zakres samodzielności. Najczęściej DAO jest wdrażany jako szereg smart kontraktów powiązanych ze sobą wspólną domeną działań i dzielącymi się swoim interfejsem API. W odróżnieniu od smart kontraktów, które są odzwierciedleniem transakcyjnej relacji między stronami umowy, rolą DAO może być autonomiczne zarządzanie aktywami, podejmowanie decyzji i aktywna interakcja z otoczeniem (stronami umów, siecią, światem zewnętrznym etc.) jako strona/osoba.

11 W Polsce Narodowe Centrum Certyfikacji prowadzi „Rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne związane z podpisem elektronicznym".

Znacznik czasu

(też: stempel czasu) jest to dowód, że dany dokument / plik / przedmiot istniał w określonym momencie czasu.

FAQ: technologia blockchain a kryptowaluty

- **Czy rozproszone rejestry i blockchain to to samo?**
  - Nie. System (technologia) rozproszonych rejestrów jest szerszym pojęciem, blockchain jest jednym z rodzajów rozproszonej bazy danych.

- **Czy kryptowaluta może istnieć bez blockchaina?**
  - Nie. To właśnie w blockchain zapisywane są wszystkie informacje o transakcjach dokonywanych kryptowalutami.

- Czy pieniądz cyfrowy może istnieć bez blockchaina?
  - Tak. Pieniądz cyfrowy może istnieć poza technologią blockchain, może być stworzony dla potrzeb konkretnego środowiska - np. dla graczy komputerowych.

- **Czy blockchain może istnieć bez tokena cyfrowego?**
  - Tak, są już takie rozwiązania.

Bibliografia

- Baran P., *On Distributed Communication Networks*, Rand Corporation, 1962
- Dąbkowski J., M. Olszański, *Modele i kwestie finansowe e-biznesu* [w:] K. Piech, M. Olszański (red.), *E-biznes – innowacje w usługach. Teoria, praktyka, przykłady*, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2012, s. 96.
- *Distributed Ledger Technology: beyond block chain, A report by the UK Government Chief Scientifc Adviser*, Government Office for Science, London 2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf
- Kelly B., *The Case Against Editable Blockchains*, CoinDesk, 30 września 2016 r., http://www.coindesk.com/sorry-accenture-bitcoins-un-editable-blockchain-feature-not-flaw/
- Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, https://bitcoin.org/bitcoin.pdf
- Szydłowski K., Pieniądz i bitcoin. Przeszłość i przyszłość, slajd 13 pt. „Łańcuch transakcji", https://docs.google.com/presentation/d/1iWQoN4mkM1lv2o4CyUcOIgn9KooC4asQYGrmXYuPrgk/edit?usp=sharing, dostęp: 5.11.2016.
- Włodarek P., *Enterprise blockchains are a HUGE overpromise*, 2 listopada 2016 r., https://medium.com/@qertoip/enterprise-blockchains-are-a-huge-overpromise-7ca2d19324b3#.fxpf7ykz1
- Zacharzewski K., *Bitcoin jako przedmiot stosunków prawa prywatnego*, „Monitor Prawniczy" 2014, nr 21.
- Zacharzewski K., *Praktyczne znaczenie bitcoina na wybranych obszarach prawa prywatnego*, „Monitor Prawniczy" 2015, nr 4.

Autorzy

- Marcin Jagodziński
- Maciej Jędrzejczyk
- Rafał Kiełbus
- Prof. nadzw. dr hab. Krzysztof Piech (Uczelnia Łazarskiego)
- Marcelina Szwed (DLA Piper Wiater sp. k.)
- Stanisław Wołoch (Quark)
- dr hab. Konrad Zacharzewski (UMK w Toruniu)