0pt2.5ex plus 1ex minus .2ex1.3ex plus .2ex

POLITECHNIKA WROCŁAWSKA
WYDZIAŁ ELEKTRONIKI

KIERUNEK: Informatyka (INF)
SPECJALNOŚĆ: Systemy Baz Danych (SBD)

PRACA DYPLOMOWA MAGISTERSKA

Analiza łańcucha transakcji w sieci Bitcoin

The analysis of Bitcoin transactions blockchain

AUTOR:
Bartosz Zychal

PROWADZĄCY PRACĘ:
dr inż. Radosław Michaliski

OCENA PRACY:

WROCŁAW 2018

Spis treści

Wprowadzenie

Do napisania na końcu. Ma zawierać informacje o motywacji i celu pracy.

Rozdział 1

Kryptowaluty - wprowadzenie

1.1 Wprowadzenie

Rolą niniejszego rozdziału jest wyjaśnienie istoty oraz sposobu działania kryptowalut. Przedstawiono w nim, czym są kryptowaluty oraz kryptografia, w jaki sposób kryptowaluty korespondują z kryptografią oraz w jaki sposób kryptografia pozwala zapewnić wysokie bezpieczeństwo kryptowaluty. Na przykładzie jednej z najpopularniejszych walut cyfrowych tj. Bitcoina, zaprezentowano zastosowanie kryptografii na potrzeby jej zabezpieczenia.

1.2 Definicja

Krypotowaluta to cyfrowy zasób mogący odpowiadać pewnej wartości środków finansowych. Zasób ten został zaprojektowany w sposób pozwalający określać go jako medium wymiany przy użyciu kryptografii, z którą jest ściśle powiązany. Kryptografia pozwala na zabezpieczenie transakcji, kontrolowanie tworzenia nowych jednostek kryptowaluty oraz weryfikację ilości posiadanych jej jednostek. Aktualnie krypotwaluty klasyfikowane są do trzech grup:

- walut cyfrowych
- walut alternatywnych
- walut wirtualnych

1.3 Bezpieczeństwo w walutach i kryptowalutach

Wszystkie waluty muszą być w jakiś sposób kontrolowane i podlegać różnego rodzaju zabezpieczeniom, tak aby zapobiegać oszustwom. W przypadku walut fiducjarnych, tj. walut nie mających pokrycia w dobrach materialnych, organizacje takie jak banki kontrolują podaż pieniądza oraz oznaczają fizycznie walutę, w celu uniemożliwienia jej podrobienia. Takie zabezpieczenia w pewnym stopniu ograniczają możliwości fałszerstwa, jednakże nie dają stuprocentowej pewności. Kryptowaluty podobnie jak tradycyjne waluty muszą posiadać miary zabezpieczeń w celu uniemożliwienia wpływania na stan systemu i tworzenia niekonsystentnych danych. Dodatkowo muszą one posiadać zabezpieczenia niepozwalające na wielokrotne użycie tych samych środków. W przeciwieństwie do walut fiducjarnych zasady bezpieczeństwa kryptowalut mogą bazować wyłącznie na istniejących

technologiach i nie mogą podlegać kontroli ze strony jakiejkolwiek centralnej instytucji [1].

1.4 Kryptografia

Kryptowaluty bardzo silnie bazują na kryptografii, która oferuje mechanizm bezpiecznego kodowania zasad ich systemu. Kryptografia pozwala nie tylko bronić system przed manipulacjami i matactwami, ale równie dobrze może zostać użyta w celu kodowania zasad tworzenia nowych jednostek kryptowaluty przy pomocy określonego matematycznego protokołu[2].

Kryptografię można sklasyfikować jako dziedzinę wiedzy o zabezpieczeniach przed nieautoryzowanym dostępem do informacji. W dzisiejszych czasach uważa się ją nie tylko za gałąź matematyki, ale i informatyki. Kryptografię można podzielić na:

- symetryczną - polega na możliwości odczytania wiadomości przy pomocy tego samego klucza, którym została podpisana. Znaczącym problemem bezpieczeństwa w tym podejściu jest przekazanie odbiorcy klucza.
- niesymetryczną - polega na istnieniu co najmniej dwóch kluczy:
  - prywatny - nazwa klucza pochodzi od faktu, iż klucz ten nie powinien być nigdy nikomu udostępniony. Przy pomocy klucza prywatnego można odszyfrować wiadomość podpisaną kluczem publicznym. Pozwala również na podpisanie wiadomości, która może być później zweryfikowana za pomocą klucza publicznego.
  - publiczny - nazwa klucza pochodzi od faktu, iż klucz ten może zostać bez żadnych zastrzeżeń upubliczniony. Klucz publiczny tworzy się na podstawie klucza prywatnego, jednakże odtworzenie klucza prywatnego z klucza publicznego jest bardzo trudne. Klucz publiczny używany jest do szyfrowania wiadomości oraz weryfikacji wiadomości podpisanej kluczem prywatnym.

Kryptografia oparta na kluczu publicznym została opracowana w latach 70. XX wieku i cały czas stanowi solidną podstawę bezpieczeństwa komputerowego i informacyjnego. Od czasu jej powstania odkryto matematyczne funkcje, które są praktycznie nieodwracalne, np. *potęgowanie liczby pierwszej* i *mnożenie krzywych eliptycznych*. Oznacza to, że łatwo obliczyć je w jednym kierunku, jednakże operacja odwrotna jest praktycznie niewykonywalna. Bitcoin korzysta z mnożenia krzywej eliptycznej jako podstawy przy wyliczaniu klucza publicznego. Sposób użycia tej funkcji został przedstawiony w podrozdziale 1.6.

1.5 Zastosowanie kryptografii w sieci Bitcoin

Aktualnie na rynku dostępne jest ponad tysiąc różnych kryptowalut, a wraz z rosnącym zainteresowaniem oraz zaufaniem społecznym ilość walut cyfrowych cały czas rośnie[3]. Niepodważalny jest fakt, że jedną z najbardziej powszechnych i popularnych kryptowalut jest Bitcoin. Bitcoin jest całkowicie zdecentralizowaną, zdigitalizowaną walutą bez globalnego emitenta, który miałby nią zarządzać oraz ją rozpowszechniać. Bazując na specjalistycznym otwartym oprogramowaniu pewna ilość Bitcoinów przekazywana jest użytkownikom w zamian za działania pozwalające na działanie systemu Bitcoin. Użytkownicy Ci zwani są kopaczami lub górnikami, a operacje przez nich wykonywane, w celu

podtrzymania systemu zwane są kopaniem. Kopanie Bitcoinów poza zyskiem ze strony kopaczy, daje olbrzymi zysk dla systemu, pozwalając weryfikować zlecone transakcje.

Właściciele Bitcoinów ustalani są na podstawie kluczy cyfrowych, adresów Bitcoin oraz podpisów cyfrowych. Klucze cyfrowe nie są przechowywane w sieci, jednakże są tworzone przez użytkowników oraz przetrzymywane w ich portfelach w plikach lub bazie danych. Klucz cyfrowy jest całkowicie niezależny od protokołu sieci Bitcoin, dlatego też może być tworzony przez różnie oprogramowania. Oprogramowanie to musi zapewniać użycie bezpiecznego źródła entropii w celu wygenerowania unikalnego klucza[4]. Wygenerowanie istniejącego lub zbyt słabego klucza może spowodować, iż w przyszłości użytkownik utraci zebrane środki. Klucze zapewniają w sieci Bitcoin:

- zdecentralizowane zaufanie
- zaświadczenie o własności
- odporny na kryptografię model bezpieczeństwa

Transakcje w sieci Bitcoin wymagają dodania prawidłowego podpisu do łańcucha bloków, co dokładniej zostało opisane w rozdziale 2. Podpis ten może być wygenerowany przy pomocy ważnych kluczy cyfrowych. Każdy kto posiada kopię tych kluczy może kontrolować środki dostępne na koncie. Protokół sieci Bitcoin korzysta z szyfrowania asymetrycznego, a co za tym idzie w transakcji klucz publiczny odbiorcy jest prezentowy przez jego odcisk palca, zwany adresem Bitcoin. Adresy te są ogólnodostępne i widoczne przez wszystkich[5].

Z klucza publicznego korzysta się w celu odebrania Bitcoinów, natomiast klucz prywatny wymagany jest do wydawania Bitcoinów. Osoba wydająca Bitcoiny musi zaprezentować swój klucz publiczny oraz podpis w transakcji. Podpis za każdym razem jest inny, lecz tworzony z jednego klucza prywatnego, co pozwala na udaną weryfikację przy pomocy dołączonego klucza publicznego. Poprzez załączenie obu tych informacji każdy w sieci może zweryfikować oraz zaakceptować transakcję jako poprawną lub ją odrzucić, w przypadku stwierdzenia, braku środków na adresie nadawcy.

Klucz prywatny w sieci Bitcoin powiązany jest ścisłe z adresem, dlatego też jego utrata powoduje nieodwracalną utratę środków. Pomimo iż środki są cały czas dostępne, nie mogą zostać użyte bez prawidłowego podpisu generowanego z klucza prywatnego.

1.6 Metoda tworzenia kluczy publicznych na przykładzie sieci Bitcoin

Jak już wcześniej wspomniano klucz publiczny obliczany jest z klucza prywatnego przy pomocy *mnożenia krzywej eliptycznej*. Metoda ta została szczegółowo opisana przez *Andreas M. Antonopoulos*[4], jednakże w celu przedstawienia siły zabezpieczenia, jakie daje szyfrowanie asymteryczne, przedstawiono ją poniżej w skróconej formie.

Klucz publiczny jest praktycznie nieodwracalny i sposób jego wyliczania można zapisać jako:

$$K = k * G, \tag{1.1}$$

gdzie:

k jest wartością klucza prywatnego,

G jest stałym punktem zwanym punktem generującym,

K jest wynikowym kluczem publicznym.

Kryptografia krzywej eliptycznej jest rodzajem kryptografi asymetrycznej bazującej na problemie logarytmu dyskretnego wyrażona jako sumy i iloczyny punktów na tej krzywej eliptycznej. Dlatego też, operacją odwrotną do mnożenia krzywej eliptycznej jest *odnalezienie logarytmu dyskretnego* i wymaga zastosowania wyszukiwania przy pomocy algorytmu typu *brute-force*, czyli przeglądu zupełnego.

W przypadku Bitcoina parametry krzywej eliptycznej są ściśle określone i zdefiniowane przy pomocy standardu zwanego *secp256k1*. Standard ten został ustalony przez amerykańską Narodową Instytucję Standaryzacji i Technologii. Zastosowana w tej kryptowalucie krzywa eliptyczna tworzona jest na podstawie określonego zbioru stałych matematycznych i jest wyrażana przy pomocy funkcji:

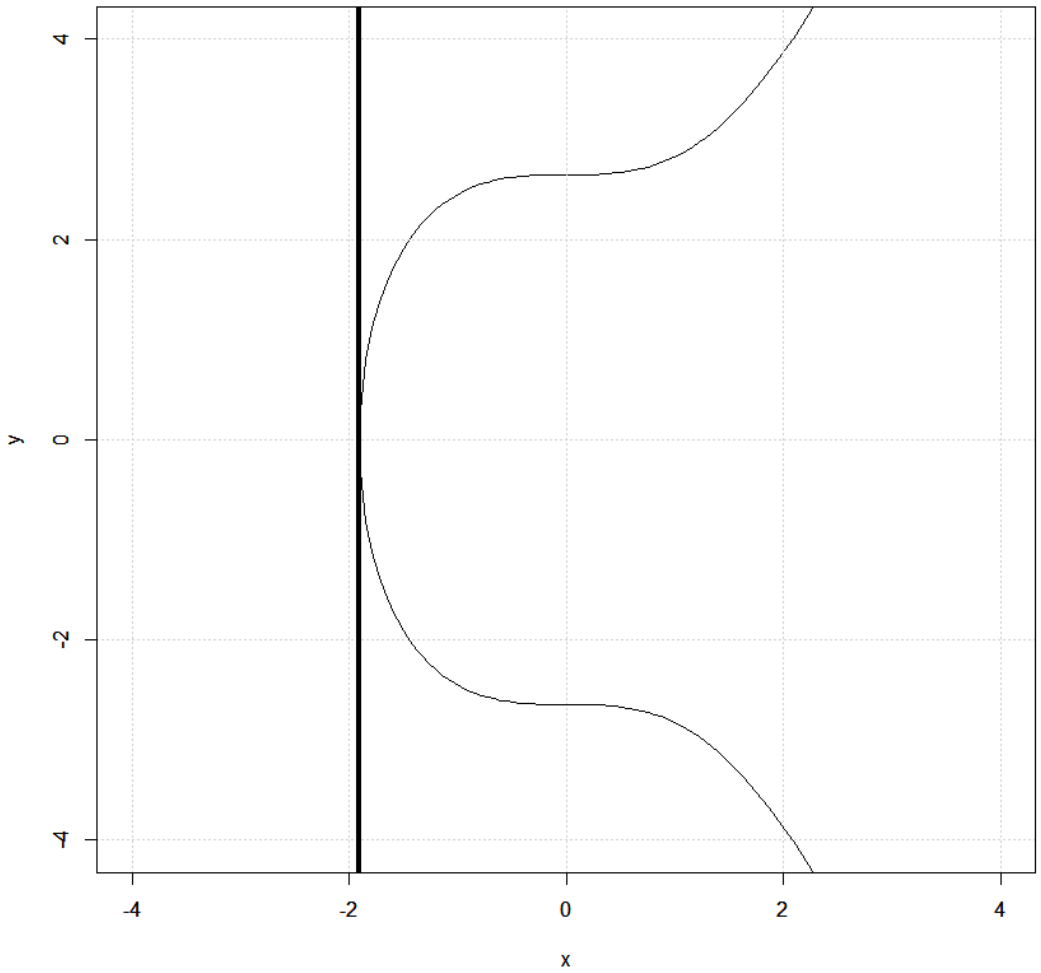
$$y^2 = x^3 + 7 \tag{1.2}$$

lub:

$$y2 \mod p = (x^3 + 7) \mod p \tag{1.3}$$

Moduł liczby pierwszej *mod p* implikuje właściwość krzywej jako znajdującej się nad skończonym polem pierwszego rzędu p. Można ją również zapisać jako funkcję F_p, gdzie $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$ jest olbrzymią liczbą pierwszą. Oznacza to, że od pewnego momentu krzywa zdefiniowana jest przy pomocy liczb zespolonych, a nie rzeczywistych. Utrudnia to jej wizualizację, gdyż wykres takiej funkcji musiałby zostać przedstawiony w dwóch wymiarach i składał by się z wielu pojedynczych punktów w przestrzeni. Na potrzeby graficznego przedstawienia uproszczono wykres 1.1 funkcji 1.6 przedstawiając go tylko w świecie liczb rzeczywistych. Wykres ten został podzielony na dwa obszary przy pomocy pionowej kreski, która nie jest częścią wykresu funkcji. Lewy obszar obejmuje wartości funkcji w świecie liczb zespolonych, który pominięto, natomiast prawa strona wykresu przedstawia funkcję 1.6, w świecie liczb rzeczywistych.

Parametr G został wybrany na podstawie powyższej krzywej eliptycznej przez protokół Bitcoina przy użyciu standardu *secp256k1*. Parametr ten jest przypisywany do wszystkich użytkowników sieci. Implikuje to wygenerowanie za każdym razem takiego samego klucza publicznego na podstawie tego samego klucza prywatnego. Klucz prywatny może mieć wartość od 1 do prawie 2^{256}, a zależność pomiędzy jego wartością k i wartością klucza publicznego K jest stała. Oznacza to, że aby przy znajomości stałej wartości G odtworzyć wartość klucza publicznego K wymagany jest przegląd wszystkich możliwych wartości klucza prywatnego k.



Rysunek 1.1 Krzywa eliptyczna zastosowana do wyznaczenia wartości G w protokole Bitcoin

1.7 Podsumowanie

Reasumując za każdą walutą musi stać określony system zabezpieczeń. W przypadku tradycyjnych walut są to centralne instytucje nadzorujące obrót i podaż określonego pieniądza. W przypadku kryptowalut bezpieczeństwo zapewnione jest poprzez zastosowanie prostej w użyciu, aczkolwiek skomplikowanej w budowie kryptografii. Zapewnia to możliwości bardzo szybkiej weryfikacji posiadanych środków, przy bardzo niskim nakładzie pracy. Dodatkowo kryptografia w porównaniu do tradycyjnych metod zabezpieczania pieniądza, nie pozwala na kontrolowanie przez jedną osobę, organizację czy instytucję poprawności danych. To zadanie wykonywane jest przez wszystkich kopaczy w sieci Bitcoin.

Rozdział 2

Blockchain - rejest transakcji

2.1 Wprowadzenie

W tym rozdziale przedstawiono oraz wyjaśniono ideę rejestru transakcji, tzw. blockchaina. Opisano strukturę bloku, transakcji oraz wejść i wyjść w transakcji. Rozdział ten opisuje również w jaki sposób tworzone są transakcje, jak są weryfikowane i jakie koszty ponosi się za przekazanie Bitcoinów innemu uczestnikowi sieci. Dodatkowo przedstawiono proces tworzenia oraz dodawania nowego bloku do blockchaina.

2.2 Definicja Blockchain'a. Czym jest łańcuch bloków?

Łancuch bloków (ang. Blockchain) jest uporządkowaną strukturą zwaną jednokierunkową listą składającą się z bloków transakcji. Listę tę charakteryzuje połączenie wsteczne co oznacza, że blok następny wskazuje na blok poprzedni. Każdy kolejny blok ma przypisaną swoją wysokość w łańcuchu bloków. Wysokość ta ustalana jest na podstawie odległości bloku od pierwszego bloku w łańcuchu. Blok ten, zwany blokiem genezy, stanowi pierwszego *rodzica* oraz wspólnego przodka dla wszystkich bloków w całym łańcuchu[6]. Idea łańcucha bloków przedstawiona jest na ilustracji 2.

Pierwszy blok łańcucha bloków w sieci Bitcoin został wygenerowany w 2009 roku i jako jedyny z bloków zapisany jest w kodzie źródłowym oprogramowania - zapewnienia to zaufanego wspólnego przodka dla wszystkich bloków łańcucha.

Bloki rozpoznaje się na podstawie unikalnego hash'a, który generowany jest przy użyciu algorytmu kryptograficznego SHA256. Wynikowy hash ma 256 bitów i w celu ułatwienia jego odczytu prezentowany jest zazwyczaj w systemie heksadecymalnym. Blok nie zawierają swojego hasha w nagłówku, co komplikuje szybkie odnajdowanie bloku. Tak by być szybko i łatwo identyfikowalnym, dane o bloku muszą być przetrzymywane w bazie danych zawierającej dodatkowe informacje o łańcuchu bloków. Każdy z węzłów sieci oblicza hash bloku w trakcie jego odbierania. W nagłówku blok zawiera informację tylko o rodzicu, tzn. przechowuje hash rodzica. Poruszając się wstecz przy pomocy tych hash'y powróci się do pierwszego bloku - bloku genezy.

Hash bloku powstaje na podstawie jego zawartości włączając w to nagłówek bloku, w którym znajduje się wspomniany hash poprzednika. Powoduje to, iż ingerencja w dane znajdujące się w blokach staje się niemożliwa ze względu na ilość obliczeń jakie należałoby wykonać, aby je zmienić. Jakakolwiek zmiana w bloku rodzica wymusza zmianę w bloku

dziecka, dlatego im blok jest starszy tym jest bezpieczniejszy. Taka struktura stanowi podstawę bezpieczeństwa w sieci Bitcoin.

Im blok znajduje się dalej w łańcuchu tym jest stabilniejszy i pewniejszy, natomiast ostatnie bloki, tzn. najświeższe, mogą ulegać zmianom w wyścigu prowadzonym przez kopaczy. W tym samym momencie na ostatni blok może wskazywać wiele nowych bloków wyprodukowanych w trakcie kopania. Taka sytuacja prowadzi do rozgałęzienia się łańcucha bloków. Jest to nieakceptowalne w opisywanej strukturze, dlatego ostatecznie do łańcucha bloków dołączany zostaje jeden z wygenerowanych bloków, a reszta bloków zostaje odrzucona. Bardziej szczegółowo problem ten został opisany w podrozdziale 2.5.

2.3 Struktura i zawartość bloku

Każdy blok ma ściśle określoną strukturę, która zawsze jest taka sama i składa się z:

- rozmiaru bloku
- nagłówka bloku
- licznika transakcji
- transakcji

Pierwsze trzy elementy maja stały lub ograniczony rozmiar. Rozmiar potrzebny na zapis transakcji w bloku zależy od ich ilości i jest zmienny. Poniżej przedstawiono bardziej szczegółowo każdy z elementów bloku.

Rozmiar bloku zapisany jest jako podstawowa informacja na samym początku bloku. Pozwala to na odczytanie odpowiedniej ilości danych.

Nagłówek bloku ma zawsze rozmiar 80 bajtów i zawiera informacje dotyczące:

- wersji protokołu sieci użytej do wygenerowania bloku - 4 bajty
- bloku poprzedniego, tzn. jego hash - 32 bajty
- podsumowania transakcji reprezentowanej przy pomocy drzewa Merkle - 32 bajty
- szacowany czas wykopania bloku - 4 bajty
- trudność wykopania bloku przy pomocy określonego algorytmu proof-of-work - 4 bajty
- licznik potrzebny dla algorytmu proof-of-work kopania bloku - 4 bajty

Licznik transakcji wskazuje na ilość transakcji zapisanych w rejestrze bloku i zajmuje od 1 do 9 bajtów.

Ostatnią, ale najważniejszą częścią bloku są transakcje. Zawartość transakcji zostały opisane w osobnym podrozdziale 2.4.

Ilustracja 2.2 przedstawia rzeczywiste dane jednego z bloków. Dane te zaczerpnięto ze strony blockchain.info pozwalającej na eksplorowanie Bitcoinowego Blockchaina[5].

Hash bloku	00000000000000000a7b47a1e58e456 fd54ae5a30cb92a35ca3e5acee065287
Wysokość bloku	496201
Rozmiar:	1071.607 kB
Liczba transakcji:	2032
Nagłówek bloku	
Wersja:	0x20000000
Hash poprzedniego bloku:	00000000000000000c6dd215947b569 fa06de2cb856dec643daf5a7e8efc72e
Markle root:	b96da6d09865e36e4862b5a612fb1893 275d889989feb5a7a217503fd84019e3
Czas wykopania:	2017-11-26 13:51:02
Trudność:	1,347,001,430,558.57
Transakcje	

⇓

Hash bloku	00000000000000000c6dd215947b569 fa06de2cb856dec643daf5a7e8efc72e
Wysokość bloku	496200
Rozmiar:	1062.264 kB
Liczba transakcji:	1036
Nagłówek bloku	
Wersja:	0x20000000
Hash poprzedniego bloku:	00000000000000000c645c295fbd91d f2f53e0346a4ecf8821abc8cc18fa4b1
Markle root:	c6be2f384d7fa195dfac1ce367ee3a9f 9ccfaf9cd337b261be1a0ff0e5d73bc4
Czas wykopania:	2017-11-26 13:43:52
Trudność:	1,347,001,430,558.57
Transakcje	

⇓

Hash bloku	00000000000000000c645c295fbd91d f2f53e0346a4ecf8821abc8cc18fa4b1
Wysokość bloku	496199
Rozmiar:	1059.467 kB
Liczba transakcji:	1758
Nagłówek bloku	
Wersja:	0x20000000
Hash poprzedniego bloku:	00000000000000000004f4c7ee2fad2a6 51b5bc1e7ce4254fe48490f7a1640dde
Markle root:	20e56ffedbf72d4d729d668037ac1a18 70ef937e4ae9491eb7ac7c69f7792447
Czas wykopania:	2017-11-26 13:43:59
Trudność:	1,347,001,430,558.57
Transakcje	

Rysunek 2.1 Przykładowy łańcuch 3 bloków sieci Bitcoin.

Hash bloku	00000000000000000a7b47a1e58e456 fd54ae5a30cb92a35ca3e5acee065287
Wysokość bloku	496201
Rozmiar:	1071.607 kB
Liczba transakcji:	2032
Nagłówek bloku	
Wersja:	0x20000000
Hash poprzedniego bloku:	00000000000000000c6dd215947b569 fa06de2cb856dec643daf5a7e8efc72e
Markle root:	b96da6d09865e36e4862b5a612fb1893 275d889989feb5a7a217503fd84019e3
Czas wykopania:	2017-11-26 13:51:02
Trudność:	1,347,001,430,558.57
Transakcje	

Rysunek 2.2 Przykładowa rzeczywista zawartość bloku sieci Bitcoin.

2.4 Transakcje i opłaty

Jednym z najważniejszych elementów w sieci Bitcoin są transakcje, które pozwalają na przekazywanie środków pomiędzy klientami sieci. Jak wspomniano w rozdziale 2.3 transakcje są zapisywane w blokach, w łańcuchu bloków. Łańcuch ten jest publicznie dostępny, co implikuje właściwość transakcji jako publicznych.

Każda nowo powstała transakcja rozgłaszana jest w sieci, gdzie jest weryfikowana przez węzły, a w konsekwencji dodana do nowo tworzonego bloku, który zostaje dołączony do blockchaina. Proces ten jest bardzo pracochłonny i wymaga rozesłania informacji o nowej transakcji w całej sieci. Sieć Bitcoin oparta jest na modelu komunikacji typu P2P (peer-to-peer). Oznacza to, że każdy z węzłów połączony jest z paroma innymi uczestnikami sieci, a z kolei Ci uczestnicy połączeni są z paroma kolejnymi uczestnikami. Powoduje to rozprzestrzenianie się informacji w sieci wykładniczo. Każdy z węzłów sieci po otrzymaniu transakcji weryfikuje ją pod kątem poprawności. W przypadku wykrycia niepoprawnej transakcji jest ona natychmiastowo odrzucana i przestaje być dalej rozpowszechniana. Komunikacja w sieci Bitcoin jest synchroniczna. Oznacza to, że węzeł, który rozgłosił transakcję dostaje informację zwrotną od węzłów z nim połączonymi o poprawności stworzonej transakcji. Kryptografia asymetryczna pozwala na anonimizację węzłów w sieci. Nie muszą się one znać, ani sobie ufać. Wystarczy, że transakcja jest prawidłowo podpisana, a będzie przekazana dalej. Struktura transakcji oraz proces przekazywania Bitcoinów przy pomocy transakcji są skonstruowane w sposób w pełni zabezpieczający środki. Przekaz nie potrzebuje żadnych dodatkowych zabezpieczeń takich jak, np. szyfrowanie łącza. Może być rozpowszechniany bez jakiegokolwiek szyfrowania, co w porównaniu z walutami fiducjarnymi jest ogromnym zyskiem[4].

Struktura transakcji składa się elementów zaprezentowanych w tabeli 2.1, jednakże najważniejsze z nich to:

- adresy kluczy publicznych (wejścia do transakcji), reprezentujące źródło środków potrzebnych na pokrycie deklarowanej sumy przekazu,
- adresy kluczy publicznych (wyjścia z transakcji), reprezentujące cel przekazu.

Element	Rozmiar (bajty)	Opis
wersja protokołu	4	określa użytą wersję prokołu użytą do stworzenia transakcji
ilość adresów wejściowych	1-9	ilość adresów reprezentujących źródło przekazywanych środków
adresy wejściowe	zmienna	adresy reprezentujące źródło przekazywanych środków
ilość adresów wyjściowych	1-9	ilość adresów reprezentujących cel przekazywanych środków
adresy wyjściowe	zmienna	adresy reprezentujące cel przekazywanych środków
czas blokady	4	określa czas, kiedy transakcja może zostać wykonana, zazwyczaj ustawiana na 0 w celu jak najszybszego podpisania

Tabela. 2.1 Struktura transakcji.

Przekazywane Bitcoiny nie są fizycznie dostępne na adresach wejściowych, a jedynie są zablokowane kluczem znanym tylko właścicielom tych adresów. Po podpisaniu transakcji środki z adresów wejściowych zostaną zablokowane na rzecz adresów wyjściowych i tylko właściciele tych adresów będą mogli uwierzytelniać kolejne przekazy, używając ich jako adresów wejściowych.

W celu określenia aktualnie dostępnych środków na adresie wejściowym zliczane są *niewydatkowane bloki wynikowe transakcji* lub *niewydane wyjścia transakcyjne* zwane UTXO (ang. Unspend Transaction Output). UTXO są to niepodzielne oraz jeszcze nie wydane kawałki bitcoinów. Bitcoiny dzielą się na mniejsze kawałki zwane tzw. Satoshi i UTXO mogą składać się z ich wielokrotności.

W momencie potwierdzania transakcji weryfikowane są wszystkie UTXO przypisane do adresów wejściowych, a następnie po wpisaniu jej do łańcucha bloków rejestrowany jest nowy zablokowany UTXO przypisany do adresu wyjściowego. Jak pisano wcześniej UTXO może zostać odblokowany jedynie przez jego właściciela. W sieci Bitcoin nie istnieje jeden główny bilans wszystkich adresów. Podczas realizacji każdej z transakcji sprawdzany jest cały łańcuch bloków i sumowane są wszystkie UTXO należące do określonego klucza publicznego. Właściciel UTXO podczas jego użycia musi wydać całą zablokowaną sumę Satoshi, dlatego też chęć przelania tylko części środków na UTXO powoduje stworzenie wielu nowych UTXO. Część z nich wskazywać będzie na adresy wyjściowe, a część jako reszta z UTXO będzie wskazywać na adres nadawcy transakcji. Bardzo często zdarza się sytuacja, w której to właściciel wielu UTXO chce przelać środki na jeden adres. W takim przypadku dozwolone jest połączenie tych jednostek w celu osiągnięcia oczekiwanej sumy bitcoinów i przekazania jej na adres odbiorcy.

Każdy z bloków zawiera jedną transakcję stworzoną przez jednego uczestnika sieci - zwycięskiego kopacza, który otrzymuje profity z tytułu podpisania bloku. Jest to zawsze pierwsza transakcja tzw. *coinbase*. Proces ten został krótko opisany w podrozdziale 2.5.

Wszystkie adresy wejściowe można traktować jako punktory do transakcji wyjściowych, zrealizowanych oraz niezrealizowanych (z nich powstają UTXO). Zrealizowane transakcje zawierają również odblokowane skrypty, co pozwala na przekazanie ich dalej. Należy podkreślić, że adresy wejściowe nie niosą informacji o ilości posiadanych środków, a jedynie

informację o miejscu, w którym można się o tym dowiedzieć. Poniżej, w tabeli 2.2, przedstawiono strukturę wyjścia transakcji.

Element	Rozmiar (bajty)	Opis
kwota	8	ilość Bitcoinów przedstawionych w Satoshi
rozmiar skryptu blokującego	1-9	długość skryptu blokującego przedstawiona w bajtach
skrypt blokujący	zmienna	skrypt określający warunki do spełnienia w celu odblokowania wyjścia

Tabela. 2.2 Struktura wyjścia transakcji.

Transakcje zazwyczaj tworzone za pomocą klienta Bitcoin, co jest wygodnym i bezpiecznym sposobem przekazywania środków. Podczas tworzenia transakcji aplikacja ta dba, aby w transakcji znalazły się wszystkie wymagane informacje. W tabeli 2.3 przedstawiono strukturę tworzenia transakcji. Pozwala ona spełnić wszystkie warunki określone w tabeli 2.2 przez wyjście transakcji.

Element	Rozmiar (bajty)	Opis
hash transakcji	32	punktor do transakcji zawierającej UTXO do wydania
indeks wyjścia	4	numer indeksu UTXO do wydania
rozmiar skryptu odblokowującego	1-9	długość skryptu odblokowującego wyrażona w bajtach
skrypt odblokowujący	zmienna	skrypt spełniający wszystkie wymagane warunki skryptu blokującego UTXO
numer sekwencji	4	aktualnie nieużywana funkcjonalność wymiany Tx

Tabela. 2.3 Struktura wyjścia transakcji.

Za każdą przeprowadzaną transakcję trzeba ponieść koszty operacyjne. W przypadku Bitcoina jest to opłata dla górników mająca zachęcać do kopania. Wielkość opłaty nie zależy od ilość przekazywanych Bitcoinów, a od wielkości stworzonej transakcji. Oznacza to, że osoba, która posiada wiele UTXO i chce je skonsumować w jednej transakcji musi zapłacić wyższą opłatę. Wynika to z faktu, że górnik w celu weryfikacji posiadanych UTXO musi wykonać dużo więcej pracy, niż gdyby transfer odbywał się z jednego UTXO. Górnicy bardzo często ustalają kryteria i tworzą priorytety transakcji, które chcą przetwarzać. W niektórych przypadkach może się okazać, że przez zbyt niską opłatę żaden z górników nie będzie podejmował się wyzwania sprawdzenia i podpisania konkretnej transakcji. Jeżeli transakcja nie zostanie podpisana przez górnika nie znajdzie się w wytwarzanym bloku. Transakcja ta *wisieć* będzie w sieci do czasu przetworzenia przez któregoś z kopaczy.

2.5 Proces tworzenia kolejnego bloku z transakcjami i dołączania go do łańcucha bloków

Wszystkie transakcje rozsyłane po sieci trafiają do górników, którzy gromadzą je w celu zbudowania nowego bloku. Transakcje te są jedynie kandydatami do znalezienia się w bloku, a które z nich znajdą się w zbudowanym bloku zależy od priorytetów górnika.

Przypuszczając sytuację, w której górnik otrzymuje wiadomość o powstaniu nowego bloku X, nad który też pracował, akceptuje otrzymane rozwiązanie i podejmuje się wyzwania skonstruowania bloku $X + 1$. Porównuje transakcje z bloku X z otrzymanymi transakcjami. Redukuje ich ilość, tak by nie próbować umieszczać tych samych transakcji w kolejnym bloku i próbuje wytworzyć kolejny blok. Sprawdza wszystkie transakcje przeznaczone do umieszczenia w bloku pod względem poprawności, a następnie generuje transakcję zwaną *coinbase*.

Transakcja *coinbase* zawiera w wejściu do transakcji nowe bitcoiny, które są nagrodą za wygenerowany blok oraz opłaty wniesione przez zleceniodawców transakcji. Ilość nowych bitcoinów zależy ilości istniejących bloków w sieci. Nagroda ta zmniejsza się wraz z ich ilością. Na początku istnienia sieci wynosiła ona 50 BTC i zmniejsza się o połowę co 210 tys. bloków. Aktualnie wynosi 12.5 BTC. Każdy górnik po otrzymaniu bloku sprawdza, czy górnik, który wytworzył blok nie oszukał generując transkację *coinbase*. W przypadku oszustwa taki blok zostaje odrzucony, a praca i koszty poniesione przez górnika zostają niepokryte. W przeciwnej sytuacji, kiedy to górnik poprawnie wykonał swoją pracę, bitcoiny zwarte w tej transakcji trafiają na adres w niej określony. Zazwyczaj tym adresem jest adres górnika.

Po dodaniu transakcji *coinbase* tworzony jest nagłówek bloku, który zawiera wszystkie dane informacje opisane w rozdziale 2.3. W nagłówku dostępny jest hash bloku poprzedniego oraz hash drzewa Merkle, który pozwala na szybką weryfikację *zaksięgowania* transakcji w bloku. Algorytm tworzenia drzewa Merkle wymaga istnienia parzystej liczby transakcji w bloku. W przypadku zawarcia nieparzystej ilości transakcji w bloku, ostatnia z nich jest duplikowana na potrzeby stworzenia drzewa.

Kolejnym krokiem tworzenia bloku jest podpisanie go poprzez znalezienie rozwiązania określonego algorytmu *proof-of-work*. Algorytm ten polega na wielokrotnym mieszaniu nagłówków bloków oraz jednej zmiennej do momentu uzyskania hash'a o określonych właściwościach. Hash'e generowane są przy pomocy algorytmu kryptograficznego wspomnianego w rozdziale 2.2 zwanego funkcją skrótu SHA256. Warunki do spełnienia mogą się zmieniać wraz ze zmianami w sieci. Przykładową własnością docelową poszukiwanego hasha może być, aby hash ten był mniejszy niż ustalony próg celu, tzn. musi być mniejszy niż określony hash.

Po odnalezieniu hash'a bloku $X+1$, zostaje on rozsyłany po sieci w celu ogłoszenia jego wygenerowania. Klienci sieci otrzymują tę informację i weryfikują poprawność nowego bloku. Oznacza to, że każdy węzeł sieci musi przeprowadzić wiele testów weryfikacyjnych zanim wyśle blok do połączonych węzłów. Po zaakceptowaniu bloku przez węzeł, zostaje on dodany do lokalnego łańcucha i wysłany dalej. W przypadku kiedy węzeł otrzyma blok Y od innego węzła wskazujący na ten sam poprzedni blok(X), co blok $X + 1$, blok Y zostaje odrzucony.

W tak skonstruowanym systemie może się wydarzyć sytuacja, w której dwóch górników jednocześnie zacznie rozsyłać poprawny blok po sieci. Oznaczać to będzie, że węzły zatwierdzą blok *górnika 1* oraz blok *górnika 2* i powstanie rozwidlenie sieci. W takich

sytuacjach sieć oczekuje na wyprodukowanie kolejnego bloku, który użyje jednego z bloków wyprodukowanych przez *górnika 1* lub *górnika 2* w celu odnalezienia globalnego consensus. Zachowanie sieci w tym przypadku zależy od wskazania w tym generowanym bloku hasha bloku poprzedniego. Dłuższy łańcuch bloków jest przez sieć traktowany jako ważniejszy i nieużyty blok w tym łańcuchu zostaje przegłosowany, a konsekwencji staje się blokiem sierocym. Łańcuchy bloków stworzone przez węzły na podstawie przegłosowanego bloku zostają skorygowane i zastosowany zostaje dłuższy łańcuch bloków.

2.6 Podsumowanie

Konkludując Blockchain jest strukturą zbudowaną z bloków wstecznie połączonych. Każdy blok z łańcucha zawiera informacje o zrealizowanych transakcjach oraz o hashu bloku poprzedniego. Transakcje składają się z wejść do transakcji oraz wyjść z transakcji. Wejścia są punktorami do niewydanych wyjść transakcji z poprzednich bloków, a wyjścia transakcji wskazują na adresy uczestników sieci, do których mają trafić bitcoiny. Bloki generowane są z transakcji przez górników, którzy walczą w wyścigu o nagrodę w postaci nowych bitcoinów oraz opłat transakcyjnych. Nowo wygenerowane bloki dołączane są do łańcucha bloków w procesie znajdowania globalnego consensusu w sieci.

Rozdział 3

Przegląd metod analiz sieci złożonych (też temporalnych) oraz analiz blockchaina

Rozdział 4

Część eksperymentalna

4.1 Plan badań

4.2 Analiza blockchaina Bitcoin

4.3 Wnioski

Podsumowanie

Bibliografia

[1] Sebastian Bala Witold Srokosz. *Kryptowaluty jako elektroniczne instrumenty platnicze bez emitenta*. Wydawnictwo Uniwersytetu Wroclawskiego, 2016.

[2] Michael J. Casey Paul Vigna. *Cryptocurrency*. Random House UK Ltd, 2016.

[3] un. coinmarketcap.com. https://coinmarketcap.com/, November 2017.

[4] Andreas M. Antonopoulos. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, 2014.

[5] un. blockchain.info. https://blockchain.info/, 2017.

[6] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies*. Princeton Univers. Press, 2016.

Spis rysunków

Spis tabel.