03 Podstawy blockchaina

Walcząc z rzeczywistością, nigdy niczego nie zmienisz.
By to uczynić, stwórz nowy model, który sprawi, że obecny stanie się przestarzały.
R. Buckminster Fuller

Blockchain jest zdecentralizowaną strukturą danych obdarzoną wewnętrzną spójnością zapewnianą dzięki konsensusowi użytkowników w kwestii obecnego stanu sieci. To technologia, która rozwiązuje problem bizantyjskich generałów (dotyczący komunikacji między nieufającymi sobie stronami) i otwiera nowe perspektywy dla transakcji niewymagających zaufania oraz wymiany informacji. Jeśli internet zdemokratyzował wymianę informacji w ramach modelu peer-to-peer, blockchain czyni to samo, ale w odniesieniu do wartości. Niniejszy rozdział zaczynamy od przyjrzenia się, jak odbywają się transakcje w sieci Bitcoin. Co za tym idzie, omawiamy strukturę bloku oraz transakcji. Następnie przechodzimy do roli portfeli i adresów użytkownika, by później zająć się metodą Simple Payment Verification (SPV) wdrożoną w sieci Bitcoin. SPV pozwala zrozumieć, skąd bierze się szczególna struktura bloku, a co ważniejsze – jak sieć Bitcoin może zachować wydajność, mimo że rozrasta się w szybkim tempie. Nasze rozważania zamykamy tematem soft i hard forków w blockchainie. Prezentujemy następstwa forków w kontekście kompatybilności w przód i w odniesieniu do handlowców oraz użytkowników zaangażowanych w wykonywanie kodu Bitcoin Core.

Organizacja transakcji

Podstawowym celem protokołu Bitcoin jest umożliwienie użytkownikom sieci dokonywania transakcji w sposób zdecentralizowany. Do tej pory, by nakreślić ogólne tło, omawialiśmy niewielkie części protokołu. Teraz połączymy te koncepcje w jeden

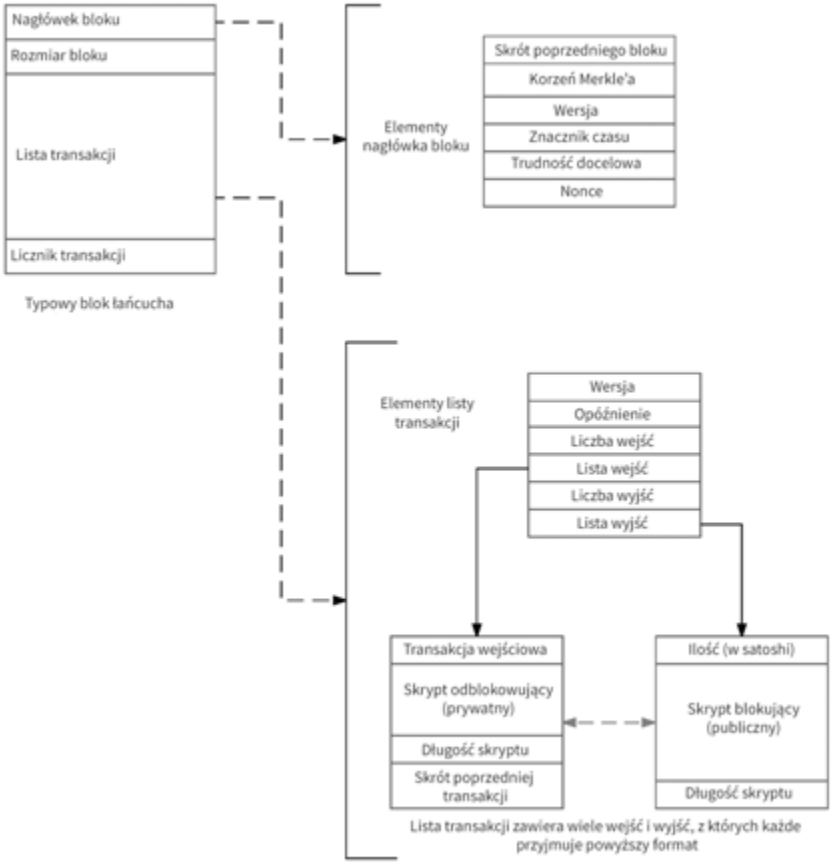
model i zajmiemy się łańcuchem bloków. Ostatecznym rezultatem wydobywania jest zwiększanie liczby bloków wraz z rozwojem sieci w czasie. By pojąć, jak przebiegają transakcje między dwoma użytkownikami (Alice i Bobem), musimy najpierw zrozumieć strukturę bloków, w których są one zapisywane. Mówiąc najprościej, blockchain jest zbiorem bloków połączonych ze sobą zgodnie z dwoma głównymi regułami:

- Wewnętrzna spójność – istnieje kilka zasad determinujących funkcjonowanie bloków, dzięki którym są one wewnętrznie spójne. Przykładowo, każdy blok łańcucha jest połączony z blokiem poprzednim i ma znacznik czasu określający moment jego utworzenia. Te mechanizmy blockchaina sprawiają, że jest on wewnętrznie uporządkowaną strukturą danych przechowującą spójny zapis transakcji.
- Konsensus dotyczący transakcji – wydobywanie opisane w rozdziale 2 jest tylko jednym ze sposobów weryfikacji transakcji; istnieją także inne metody, nieoparte na obliczaniu skrótów w trybie *brute force*. Bądź co bądź każda implementacja zakłada schemat osiągania konsensusu dotyczącego transakcji przeprowadzonych w sieci w określonym przedziale czasu. Proces weryfikacji zawsze zakłada użycie jakiegoś rodzaju dowodu pracy lub innej strategii, dzięki której transakcje są gromadzone w puli, a następnie sprawdzane przez użytkowników sieci.

W podstawowym sensie transakcja to struktura danych, którą zapisuje się w bloku. Jak dokładnie to się odbywa? Żeby prześledzić ten proces, spójrzmy na pełną strukturę bloku przedstawioną na ilustracji 3.1. Każdy z bloków ma przynajmniej dwa unikalne elementy: nagłówek bloku zawierający unikalny skrót (nazywany korzeniem Merkle'a; ang. *Merkle root*), który identyfikuje ten i tylko ten blok, oraz listę transakcji zawierającą nowe transakcje. Zauważmy, że każdy blok zawiera tę samą liczbę transakcji na liście, ale są to transakcje różne. Wynika to stąd, że co dziesięć minut w wyścigu górników wygrywa tylko jeden blok, a pozostałe bloki kandydujące zostają odrzucone, po czym wyścig zaczyna się od początku. W tym uproszczonym modelu istnieją jedynie dwa dodatkowe elementy bloku: rozmiar bloku, który pozostaje stały w obrębie całej sieci, oraz licznik transakcji. My skupiamy się przede wszystkim na nagłówku bloku oraz liście transakcji.

Nagłówek bloku zawiera kilka stałych elementów, takich jak omawiane wcześniej wartość docelowa i nonce. W jego skład wchodzi też numer wersji kodu Bitcoin Core, na której pracował górnik zwycięzca. Unikalną częścią każdego bloku jest także znacznik czasu, który bezbłędnie identyfikuje go w sieci. Nagłówek zawiera również skrót poprzedniego bloku w łańcuchu, a także inny specjalny skrót, który identyfikuje dany blok, zwany korzeniem Merkle'a. Powstawanie korzenia Merkle'a omówimy w dalszej części tego rozdziału.

DOWÓD ŻYCIA. W ostatnim czasie pojawiły się plotki, że Julian Assange, założyciel WikiLeaks, umarł. W odpowiedzi, by udowodnić, że to nieprawda, Assange odbył na Reddicie sesję Ask Me Anything i odczytał skrót ostatniego bloku w blockchainie. Blok został utworzony zaledwie dziesięć minut wcześniej, więc nagranie nie mogło powstać przed tą chwilą, co stało się niezaprzeczalnym dowodem, że Assange żyje. Wówczas po raz pierwszy skrót bloku został wykorzystany w przestrzeni kultury popularnej. Assange określił to dowodem życia.



Ilustracja 3.1. Uproszczona struktura bloku

Nagłówek i lista transakcji to dwa niepowtarzalne elementy każdego bloku. Nagłówek składa się z kilku mniejszych części, z których najbardziej swoistą stanowi korzeń Merkle'a, skrót, który bezbłędnie identyfikuje dany blok. Na nagłówek składa się skrót poprzedniego bloku, nonce użyta do utworzenia obecnego bloku i trudność wydobywania. Są to standardowe elementy związane z wydobywaniem, które omówiliśmy już wcześniej. Każdy blok zawiera także listę transakcji. Oprócz rzeczy-