Studia i Materiały Informatyki Stosowanej, Tom 13, Nr 1, 2021
str. 37-41

TECHNOLOGIA BLOCKCHAIN

Maciej Sitko[1], Mieczysław Jagodziński[2]

[1] *Politechnika Śląska, Wydział Automatyki, Elektroniki i Informatyki, 44-101 Gliwice, ul. Akademicka 16*
[2] *Politechnika Śląska, Wydział Automatyki, Elektroniki i Informatyki, 44-101 Gliwice, ul. Akademicka 16*
email: mieczyslaw.jagodzinski@polsl.pl

Streszczenie: *W artykule przedstawiono zasadę działania blockchainu na podstawie Bitcoina oraz smart kontraktów Ethereum. Zostały omówione najistotniejsze zalety technologii blockchain. Zwrócono szczególną uwagę na transparentność, decentralizację oraz bezpieczeństwo proponowanego rozwiązania. Opisano szczegóły funkcjonalne oraz techniczne. Przedstawiono przykładowe zastosowanie blockchainu.*

Słowa kluczowe: *Blockchain, Bitcoin, Ethereum, decentralizacja, inteligentne kontrakty*

Blockchain technology

Abstrac*t: The article presents the principle of blockchain operation based on Bitcoin and Ethereum smart contracts. The most important advantages of blockchain technology were discussed. Particular attention was paid to transparency, decentralization and security of the proposed solution. The functional and technical details are described. An example of the use of blockchain is presented*

Key words: *Blockchain, Bitcoin, Ethereum, decentralization, smart contracts*

1. Wprowadzenie

Technologia blockchain zyskuje w ostatnich latach coraz większą popularność. Początkowo łańcuch bloków znajdował swoje zastosowanie przede wszystkim w branży finansowej w postaci kryptowalut, czyli wirtualnych pieniędzy. Decentralizacja jaką zapewnia blockchain stworzyła alternatywę dla tradycyjnych systemów bankowych i zaproponowała rozwiązanie, które eliminuje potrzebę ingerencji organów trzecich w wymianę środków pomiędzy pojedynczymi podmiotami. Blockchain zapewnia także wysoki poziom bezpieczeństwa przechowywanych danych. Specjalnie zaprojektowana struktura blockchainu nie pozwala na zmianę zapisanych w nim informacji – możliwy jest jedynie ich odczyt. Ponadto wszystkie akcje podejmowane w blockchainie udostępniane są w sieci publicznej. Zapewnia to transparentność wykonywanych transakcji, z zachowaniem anonimowości podmiotów biorących w nich udział. Wraz z rozwojem tej technologii znaleziono także rozwiązania pozafinansowe, do których można zaimplementować architekturę łańcucha bloków. Było to możliwe za sprawą inteligentnych kontraktów (ang. smart contracts).

Blockchain to technologia, która opiera swoje działanie na publicznym, rozproszonym rejestrze danych zachowującym chronologię wykonanych operacji. Rejestr udostępniany jest w sieci o architekturze peer – to – peer. Sam termin „blockchain" oznacza „łańcuch bloków". Bloki to proste struktury danych, które są podstawą działania blockchainu. Przechowuje się w nich transakcje, będące bezpośrednimi dowodami każdej akcji podjętej w sieci. Każdy kolejny stworzony blok posiada referencję do bloku poprzedniego, stąd określenie „łańcuch bloków".

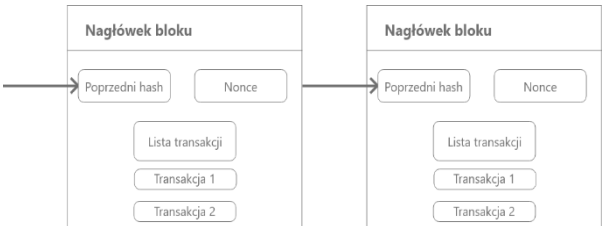
Pierwsze próby stworzenia blockchainu datuje się na końcówkę XX wieku. Mimo to pierwsze w pełni działające rozwiązanie zostało opublikowane w 2008 roku przez Satoshiego Nakamoto – założyciela Bitcoina [1]. Stworzył on kryptowalutę, która opierała swoje działanie na łańcuchu bloków. Kolejny przełom w tej dziedzinie odbył się za sprawą Vitalika Buterina, który w 2013 roku udoskonalił rozwiązanie Nakamoto o smart kontrakty, czyli krótkie programy skryptowe, które znacznie rozszerzają możliwości zarządzania transakcjami w blockchainie. W ten sposób powstało Ethereum, które umożliwiło tworzenie pierwszych zdecentralizowanych aplikacji. W artykule zostanie opisane działanie blockchainu na podstawie Bitcoina oraz krótko scharakteryzowane zostaną smart kontrakty.

2. Blok

Blok to podstawowa struktura danych w blockchainie, któremu technologia ta zawdzięcza

swoją nazwę. Dołączanie kolejnych bloków do łańcucha to podstawowe zadanie, które wykonują użytkownicy w sieci. Uproszczony schemat bloków przedstawiono na rys. 1. W rzeczywistości bloki składają się z kilkunastu pól zawierających informacje niezbędne do funkcjonowania systemu. Najważniejszymi z nich są:

- numer hasz poprzedniego bloku,
- czas utworzenia bloku,
- trudność bloku,
- liczba „nonce”,
- lista transakcji.

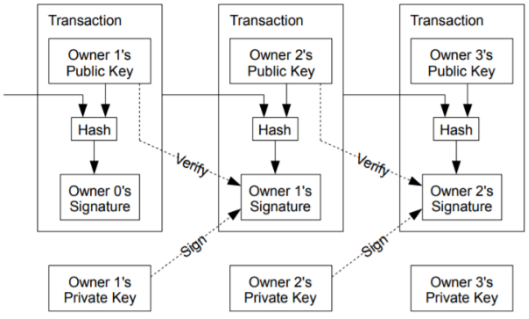


Rysunek 1. Uproszczony schemat bloków w blockchainie. [opracowanie własne]

Każdy blok posiada swój unikalny numer, który powstaje przez zahaszowanie zawartości tego bloku. Funkcja haszująca w Bitcoinie opiera się o szyfrowanie SHA-256, które dowolnie dużej liczbie przyporządkowuje ciąg znaków o stałej długości 256 bitów. Jest to funkcja jednokierunkowa, tzn. prawie niemożliwe jest odkodowanie zaszyfrowanej liczby. Ponadto nawet najmniejsza zmiana w liczbie zaszyfrowanej powoduje całkowitą zmianę wyniku szyfrowania. Obliczenie numeru hasz nazywa się „wykopywaniem bloku” (ang. mining), a osoby podejmujące się tego zadania określa się mianem „górników” (ang. miners). Za wykonanie tego zadania jako pierwszy, górnik otrzymuje nagrodę pieniężna, na którą składają się opłaty z zawartych w bloku transakcji. Wykopanie bloku stanowi dowód pracy (ang. proof-of-work), świadczący o uczciwości użytkownika sieci. Musi on bowiem poświęcić moc obliczeniową swojego urządzenia na wyliczenie numeru hasz, który warunkowany jest przez ustaloną trudność. Trudność bloku to szacunkowa liczba prób obliczenia haszu, jaką musi podjąć użytkownik, aby numer ten spełniał postawione przez blok wymagania. Wymaganiem jest, aby numer hasz był mniejszy niż ustalona liczba, tzw. target. Funkcja haszująca jest na tyle złożona, że niemożliwe jest obliczenie haszu mniejszego niż target innym sposobem niż metodą prób i błędów. Bitcoin zwiększa trudność bloku co 2016 wykopanych bloków, czyli co około 2 tygodnie. Obecnie trudność wynosi 21,448,277,761,059 (stan na 10.03.2021r.). Wykopywanie bloku polega na inkrementacji liczby „nonce”, która jest jednym z wejść funkcji haszującej. Wartości pozostałych wejść są niezmienne, dlatego należy znaleźć taką liczbę „nonce”, która spowoduje, że wyjście funkcji haszującej będzie mniejsze niż określony target. Połączenie kolejnych bloków poprzez referencje do numerów hasz gwarantuje niezmienność danych zapisanych w blockchainie. Zmiana dowolnej wartości zapisanej transakcji powoduje całkowitą zmianę numeru hasz bloku. Oznacza to, że kolejne hasze bloków, które referowały do poprzedniego haszu są błędne i taki atak jest od razu zauważalny przez sieć.

3. Transakcje

Bitcoin został stworzony jako elektroniczna waluta. Podstawową operacją w tym blockchainie jest transfer pieniędzy, który realizowany jest poprzez transakcje. Aby transakcja mogła dojść do skutku, adresat oraz nadawca transakcji muszą należeć do sieci blockchain, tzn. muszą posiadać swój klucz publiczny i prywatny. Klucz publiczny służy do identyfikacji użytkownika i jest niejako adresem, który używany jest do korespondowania w sieci. Klucz prywatny stosuje się do podpisywania transakcji. Na jego podstawie oblicza się podpis cyfrowy, który służy do weryfikacji adresata. Podobnie jak blok, każda transakcja posiada swój numer hasz. Jest on obliczany na podstawie numeru hasz poprzedniej transakcji, danych obecnej transakcji oraz klucza publicznego odbiorcy. Można więc stwierdzić, że kolejne transakcje, podobnie jak bloki, również są połączone w łańcuch. Schemat takiego połączenia przedstawiono na rys. 2.



Rysunek 2. Schemat połączenia kolejnych transakcji [opracowanie własne na podstawie [1]]

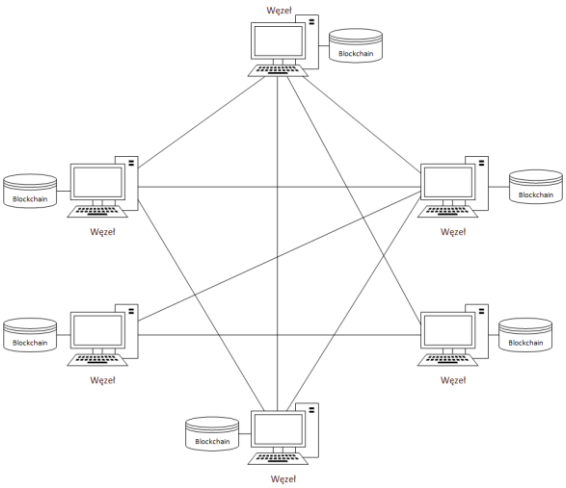
Początkowo transakcje można wyobrazić sobie jako transfer pewnej kwoty x od użytkownika A do użytkownika B. Wydaje się więc, że po udanej transakcji, kwota x zostaje odjęta od stanu konta użytkownika A, a następnie dodana do stanu konta użytkownika B. Jednak w Bitcoinie mechanizm ten funkcjonuje zupełnie inaczej. Transakcje polegają

na przesyłaniu środków jako monet (ang. coin), które tworzone są na podstawie poprzednich transakcji. Nowa transakcja na wejściu otrzymuje referencje do poprzednich transakcji i na ich podstawie tworzy wyjście. Transakcje, podobnie jak rzeczywiste monety, są niepodzielne. W przypadku, gdy łączna wartość użytych monet jest większa niż wartość wysyłana, nadawcy zwracana jest reszta. Można więc powiedzieć, że portfel Bitcoin to nie pojedyncza liczba stanowiąca saldo konto, a łańcuch wszystkich przeprowadzonych transakcji.

Po wysłaniu przez użytkownika operacji, transakcja trafia do puli. Za weryfikację poprawności transakcji odpowiedzialne są węzły sieci. Czas oczekiwania na zatwierdzenie transakcji w Bitcoinie to około 10 minut. Czas ten może być krótszy, jeśli nadawca dołączy do transakcji dodatkową opłatę transakcyjną. Taka operacja jest znacznie bardziej atrakcyjna dla górników, którzy otrzymają za nią większą nagrodę.

4. Sieć

Blockchain to publiczny rejestr, który dostępny jest dla każdego użytkownika. Umożliwia to sieć o architekturze peer – to – peer, przedstawiona na rys. 3.



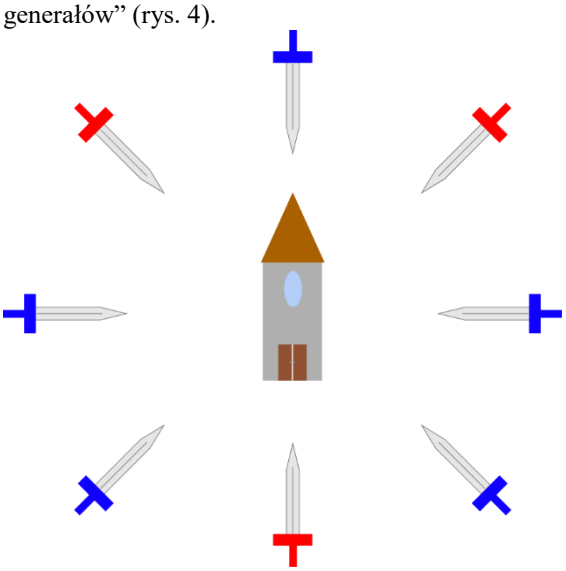
Rysunek 3. Schemat sieci peer – to – peer podłączonej do blockchainu. [opracowanie własne na podstawie [1]]

Każdy użytkownik może pobrać kopię rejestru na swoje urządzenie. Zapewnia to transparentność dokonywanych transakcji. Użytkowników sieci blockchain można podzielić na kilka typów:

- pełny węzeł,
- lekki węzeł,
- górnik.

Najważniejsze dla sprawnego funkcjonowania sieci są pełne węzły (ang. full nodes). Przechowują one pełną kopię blockchainu. Odpowiadają także za weryfikację wszystkich transakcji i bloków oraz dystrybucję tych informacji w całej sieci. Z uwagi na duży rozmiar pełnej kopii łańcucha (obecnie jest to około 140 GB danych), coraz popularniejsze są lekkie węzły (ang. light nodes). Nie przechowują one pełnej kopii łańcucha, ale same nagłówki bloków o maksymalnej wielkości 80 bajtów, co znacznie redukuje eksploatację sprzętu. Ostatnim typem użytkowników są górnicy, którzy pobierają tylko dane ostatnie bloku, żeby wyliczyć nowy hasz.

Jednak w rozwiązaniu opierającym się na topologii sieci peer – to - peer pojawia się problem ze zgodnością przechowywanych wersji. W jaki sposób dojść do porozumienia w sprawie kolejności transakcji oraz ich poprawności. Sytuacja ta określana jest jako „problem bizantyjskich generałów" (rys. 4).



Rysunek 4. Wizualizacja „problemu bizantyjskich generałów".[opracowanie własne na podstawie [3]]

Problem został sformułowany następująco przez Marshalla Pease'a, Leslie Lamporta i Roberta Shostaka:

„Grupa armii bizantyjskich otacza miasto nieprzyjaciela. Rozkład sił jest taki, że jeśli wszystkie armie zaatakują razem, to będą w stanie zdobyć miasto. Innym sposobem uniknięcia porażki jest odwrót wszystkich armii. Generałowie poszczególnych armii mają zaufanych posłańców, którzy z powodzeniem dostarczą każdy komunikat od jednego generała do innego. Jednak niektórzy generałowie mogą być zdrajcami usiłującymi doprowadzić do porażki armii bizantyjskich. Należy opracować algorytm, który umożliwi wszystkim wiernym generałom uzgodnienie pewnego planu działania. Ostateczna decyzja powinna być z grubsza taka, jaka zostałaby podjęta w drodze głosowania większościowego nad decyzjami poszczególnych generałów. W przypadku

nierozstrzygnięcia głosowania końcową decyzją ma być odwrót". [3]

Jako pierwszy, zadanie to rozwiązał Satoshi Nakamoto – twórca Bitcoina. Dowodem uczciwości uczestników sieci jest dowód pracy (proof – of – work) wykonanej przy obliczaniu numeru hasz. Ponadto transakcja zostaje dodana do bloku dopiero wtedy, gdy ponad połowa uczestników sieci ją zaakceptuje, a także zakłada się, że co najmniej połowa użytkowników sieci jest uczciwa. W takiej sytuacji nieopłacalne staje się bycie nieuczciwym, ponieważ szansa na oszustwo jest bardzo niska a każda taka próba obarczona kosztem eksploatacji sprzętu oraz Internetu. Przypadek gdy ponad połowa użytkowników sieci jest nieuczciwa określa się jako „atak 51%".

5. Bezpieczeństwo

Innym problemem sieci rozproszonej jest „problem podwójnego wydatkowania" (ang. double spending problem). Powstaje on w systemach, gdzie nie ma jednostki centralnej, która określa kolejność wykonanych transakcji. W celu rozwiązania tego problemu Satoshi Nakamoto wprowadził znaczniki czasowe (ang. timestamps), które jednoznacznie definiują chronologię wykonanych transakcji. W przypadku gdy kilka bloków zostanie stworzonych w tym samym momencie, część użytkowników może wybrać inny blok jako ten stworzony według nich najszybciej z uwagi na różny czas propagacji informacji w sieci. Przy tworzeniu kolejnego bloku szansa na wystąpienie takiej sytuacji jest jeszcze mniejsza, więc zachowany zostanie ten blok, który wraz z kolejnymi blokami będzie tworzył najdłuższy łańcuch, tzw. reguła najdłuższego łańcucha. Polega ona na cyklicznym sprawdzaniu, który łańcuch w blockchainie jest najdłuższy, a dokładniej, który łańcuch ma największą sumaryczną trudność. Połączenie rejestru znaczników czasu transakcji i rejestru dopasowującego klucze publiczne do prywatnych było kluczowym czynnikiem działania systemu stworzonego przez Satoshiego.

Należy rozpatrzeć także sytuację, gdy nieuczciwy użytkownik sieci dokona próby dołączenia własnej kopii łańcucha. Zgodnie z regułą najdłuższego łańcucha, musi stworzyć łańcuch o co najmniej jeden blok dłuższy niż aktualny blockchain. Problem, z którym musi się zmierzyć to tzw. problem ruiny gracza (ang. Gambler's ruin). Nieuczciwy użytkownik zawsze zaczyna wyścig o obliczanie nowego bloku z pewnym deficytem. Musi on bowiem obliczyć hasze wszystkich poprzednich bloków, a także hasz nowego bloku wcześniej niż wszyscy użytkownicy sieci obliczą i zatwierdza nowy blok. W dokumencie technicznym Satoshi Nakamoto obliczył, że dla łańcucha składającego się z 1 bloku, prawdopodobieństwo takiego zdarzenia wynosi 20%, przy 5 blokach wynosi już 0,09%. Przy obecnej liczbie bloków Bitcoina sytuacja ta staje się praktycznie niemożliwa, jednak wciąż stanowi niebezpieczeństwo dla mniejszych blockchainów.

6. Smart kontrakty

Smart kontakty to krótkie programy skryptowe, które stanowią podstawę działania blockchainu Ethereum. Są także głównym czynnikiem wyróżniającym Ethereum na tle Bitcoina. Smart kontrakty umożliwiają zarządzanie funkcjonalnościami blockchainu za pośrednictwem dodania warunków logicznych do transakcji oraz interakcji pomiędzy kontraktami. Ich działanie opiera się o EVM (Ethereum Virtual Machine), czyli wirtualną maszynę autorstwa Ethereum, która odpowiada za wykonywanie instrukcji zapisanych w kontraktach.

Swoją popularność Ethereum zawdzięcza także tzw. tokenom. Za pośrednictwem smart kontraktów możliwe jest stworzenie wirtualnych żetonów, którym przypisuje się funkcje określone przez dane standardy. Obecnie najpopularniejszym z nich jest ERC-20. Używanie standardów pozwala na jednorodną implementację funkcjonalności, która jest niezbędna przy tak łatwym dostępie do stworzenia własnego tokenu. Token może pełnić rolę pieniądza, akcji bądź usługi

7. Podsumowanie

Decentralizacja działań w sieci jest tematem coraz częściej poruszanym w dzisiejszych czasach, a wizję Internetu pozbawionego kontroli jednostek centralnych określa się mianem Web 3.0. Rynek aplikacji opartych o blockchain rozwija się dynamicznie, a zastosowanie tego rozwiązania można zauważyć w wielu branżach pozafinansowych. Przykładem jest branża spożywcza, która umożliwia przechowywanie danych o dystrybuowanych produktach za pomocą blockchainu oraz monitorowanie daty przydatności do spożycia za pośrednictwem smart kontraktów. Innym przykładem jest branża nieruchomości. Za pomocą tokenów możliwe jest sprzedaż tylko części budynku czy ziemi, której wartość poddaje się tokenizacji, czyli przypisaniu tokenowi określonej części wartości danego dobra.

Literatura

1. Nakamoto S. Bitcoin: *A Peer-to-Peer Electronic Cash System* https://bitcoin.org/bitcoin.pdf [data dostępu: 2021-03-10]

2. Sitko Maciej, Praca inżynierska *„Smart contracts z wykorzytaniem technologii blockchain”*
3. Wikipedia, wolna encyklopedia. *Problem generałów bizantyjskich.* https://pl.wikipedia.org/wiki/Problem_bizantyjskich_genera%C5%82%C3%B3w [data dostępu: 2021-03-10]