Blockchain

Podstawy technologii łańcucha bloków w 25 krokach

—

Daniel Drescher

Helion

Tytuł oryginału: Blockchain Basics: A Non-Technical Introduction in 25 Steps

Tłumaczenie: Leszek Sielicki

ISBN: 978-83-283-8486-6

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/blockv
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

ETAP

8

Planowanie łańcucha bloków

Podstawowe koncepcje zarządzania własnością za pomocą łańcucha bloków

Na wcześniejszych etapach ustaliliśmy istnienie związku pomiędzy zaufaniem, integralnością, całkowicie rozproszonymi systemami *peer-to-peer* i łańcuchem bloków. W efekcie tych ustaleń dobrze rozumiesz, czym jest łańcuch bloków, dlaczego jest potrzebny i jaki problem rozwiązuje. Nadal nie znasz jednak wewnętrznego sposobu funkcjonowania łańcucha bloków. Na tym etapie dowiesz się w zarysie, jak działa łańcuch bloków, zapoznając się z ogólnym scenariuszem jego stosowania, który poprowadzi Cię przez kolejne etapy. Omówimy także główne zadania związane z projektowaniem łańcucha bloków do celów zarządzania własnością oraz przyjrzymy się podstawowym koncepcjom z nim związanym. Ten etap jest punktem wyjścia do kolejnych, w których szczegółowo omówimy koncepcje i technologie składające się na łańcuch bloków.

Cel

Celem naszych aktualnych rozważań będzie zrozumienie koncepcji składających się na pojęcie łańcucha bloków. Ze względów dydaktycznych zajmiemy się działaniami związanymi z tworzeniem własnego systemu zarządzania własnością. Staniesz więc przed takimi samymi problemami, z jakimi musiał się kiedyś zmierzyć i jakie z powodzeniem rozwiązał wynalazca łańcucha bloków. Chodzi o opracowanie programu zarządzającego własnością w całkowicie rozproszonym systemie peer-to-peer, który będzie działał w bezwzględnie otwartym i niezaufanym środowisku.

Punkt początkowy

Oto punkt wyjścia — podstawowe fakty dotyczące rozważanego systemu możemy zestawić w następujący sposób:

- System będzie całkowicie rozproszonym systemem *peer-to-peer*, składającym się z zasobów obliczeniowych udostępnianych przez jego użytkowników.
- System *peer-to-peer* wykorzystuje Internet jako sieć łączącą poszczególne węzły.
- Ani liczba węzłów, ani ich wiarygodność i poziom zaufania nie są znane.
- Celem systemu *peer-to-peer* jest zarządzanie własnością dobra cyfrowego (np. punktów premiowych lub cyfrowej waluty).

Ścieżka postępowania

Istnieje siedem głównych zadań, którymi należy się zająć podczas opracowywania i tworzenia oprogramowania zarządzającego własnością z wykorzystaniem całkowicie rozproszonego systemu *peer-to-peer* w otwartym i niezaufanym otoczeniu. Oto one:

- opis własności,
- ochrona własności,
- przechowywanie danych transakcji,
- przygotowywanie rejestrów do rozproszenia w niezaufanym środowisku,
- rozpraszanie rejestrów,
- dodawanie nowych transakcji do rejestrów,
- określanie, które rejestry odpowiadają prawdzie.

Zadanie 1. Opis własności

Zanim zaczniemy tworzyć łańcuch bloków, musimy zadać sobie pytanie, co zamierzamy z nim zrobić. Ponieważ będziemy chcieli zaprojektować system oprogramowania, który zarządza własnością, musimy najpierw zadecydować, jak tę własność opisać. Okazuje się, że dobrym sposobem opisu wszelkiego rodzaju przeniesień własności są transakcje, a pełna historia transakcji jest kluczem do identyfikacji aktualnych właścicieli. Na etapie 9 zajmiemy się więc transakcjami, ustalając, czym są, jak można je opisywać i wykorzystywać do ustalania własności.

Zadanie 2. Ochrona własności

Opis własności za pomocą transakcji to tylko punkt wyjścia. Niezbędny jest także sposób, aby uniemożliwić niepowołanym osobom uzyskiwanie dostępu do własności innych. W codziennym życiu łatwo jest uniemożliwić obcym skorzystanie z naszego samochodu czy wejście do naszego domu za sprawą drzwi zaopatrzonych w zamki. Okazuje się, że sposób ochrony transakcji na poziomie indywidualnym, przypominający drzwi z zamkami, które chronią samochód lub dom, zapewnia kryptografia.

Ochrona własności składa się z trzech podstawowych elementów, którymi są: identyfikacja i uwierzytelnianie właścicieli oraz umożliwianie dostępu do przedmiotu własności wyłącznie jego właścicielom. W ramach etapów 12 i 13 wyjaśnimy te pojęcia bardziej szczegółowo, posługując się koncepcją wartości skrótu. Jeżeli nigdy wcześniej nie słyszałeś o wartościach skrótu, nie ma powodów do obaw. Ich szczegółowe wyjaśnienie zawiera treść etapów 10 i 11. Interesujące informacje znajdą w nich jednak także czytelnicy dysponujący wykształceniem technicznym lub wiedzą o wartościach skrótu.

Zadanie 3. Przechowywanie danych transakcyjnych

Opisywanie własności za pomocą transakcji i posiadanie środków bezpieczeństwa, które chronią własność na poziomie poszczególnych transakcji, to istotne etapy na drodze do zaprojektowania systemu oprogramowania, który będzie zarządzał własnością. Niezbędny jest jednak także sposób przechowywania całej historii transakcji, bo historia ta służy do ustalania własności. Historia transakcji jest fundamentalnym składnikiem procesu ustalania własności, więc musi być przechowywana w bezpieczny sposób. Okazuje się, że struktura danych łańcucha bloków jest cyfrowym odpowiednikiem rejestru. W ramach etapów 14 i 15 zapoznamy się z wymaganiami, jakie musi spełniać struktura danych łańcucha bloków, aby służyć jako cyfrowy rejestr, i dowiemy się, jaki jest sposób jej implementacji.

Zadanie 4. Przygotowywanie rejestrów do rozproszenia w niezaufanym środowisku

Dobrze jest posiadać jeden wyizolowany rejestr czy też strukturę danych łańcucha bloków, która zawiera dane transakcyjne, ale naszym celem jest zaprojektowanie rozproszonego systemu *peer-to-peer*, który będzie działał w niezaufanym środowisku. Kopie rejestru będą więc funkcjonować w niezaufanych węzłach i w niezaufanej sieci. Co więcej, kontrolę nad rejestrami przekażemy całej sieci, bez centralnego punktu kontrolnego lub koordynacyjnego. Jak w takiej sytuacji zapobiec fałszowaniu rejestrów lub manipulowaniu nimi (np. poprzez usuwanie transakcji z historii lub dodawanie do niej transakcji nielegalnych)? Okazuje się, że najlepszym sposobem zapobiegania wprowadzaniu zmian w historii transakcji jest sprawienie, aby była ona niemożliwa do zmiany. Oznacza to, że rejestrów — i tym samym historii transakcji — nie można zmieniać po ich zapisaniu. W efekcie nie będziemy musieli się obawiać, że rejestry zostaną zmanipulowane lub sfałszowane, bo po prostu nie da się ich zmienić. Jednakże posiadanie rozproszonego systemu *peer-to-peer*, do którego niemożliwe jest wprowadzanie zmian, wydaje się być czymś wyjątkowo bezpiecznym, ale za to okazuje się zupełnie bezużyteczne, bo nie da się dodawać do niego nowych transakcji. Dlatego też wyzwanie dla struktury danych łańcucha bloków polega na tym, aby była ona z jednej strony niezmienna, a z drugiej przyjmowała nowe transakcje. Samo w sobie brzmi to jak sprzeczność, ale okazuje się, że jest możliwe dzięki sztuczce technicznej, którą wyjaśnimy na etapie 16. W efekcie jej zastosowania powstaje struktura danych łańcucha bloków z atrybutem „tylko-do-dopisywania": możliwe jest dodawanie nowych transakcji, ale praktycznie nie da się wprowadzać zmian w danych, które zostały dodane w przeszłości.

Zadanie 5. Rozpraszanie rejestrów

Gdy rejestr ma atrybut „tylko-do-dopisywania", można stworzyć rozproszony system rejestrów *peer-to-peer*, udostępniając jego kopie każdemu, kto o to wystąpi. Samo udostępnianie kopii rejestrów tylko do dopisywania nie spełni jednak zakładanych celów. Rozproszony system zarządzający własnością oznacza interakcje między uczestnikami czy też węzłami. Dlatego na etapie 17 wyjaśnimy, w jaki sposób węzły systemu współdziałają ze sobą i jakimi informacjami się wymieniają.

Zadanie 6. Dodawanie nowych transakcji do rejestrów

Rozproszony system *peer-to-peer* składa się z uczestników, których komputery przechowują poszczególne kopie struktury danych łańcucha bloków z atrybutem „tylko-do-dopisywania". Ponieważ struktura danych pozwala na dodawanie nowych danych transakcyjnych, należy sprawić, aby dodawane były wyłącznie prawidłowe i autoryzowane transakcje. Okazuje się, że jest to możliwe dzięki zezwoleniu wszystkim uczestnikom systemu *peer-to-peer* na dodawanie nowych danych i dodatkowo przekształceniu wszystkich uczestników systemu *peer-to-peer* w nadzorców innych uczestników. W efekcie wszyscy uczestnicy systemu będą się wzajemnie nadzorować i wskazywać błędy popełniane przez „ich" uczestników. Na etapie 18 wyjaśnimy tę kwestię bardziej szczegółowo, a także zajmiemy się zagadnieniem zapewniania motywacji uczestników systemu, tak aby wypełniali te funkcje.

Zadanie 7. Określanie, które rejestry odpowiadają prawdzie

Gdy można już dodawać nowe transakcje do poszczególnych rejestrów w systemie *peer-to-peer*, pojawia się problem typowy dla każdego rozproszonego systemu *peer-to-peer*: do różnych użytkowników mogą docierać różne transakcje, co powoduje, że historie przechowywanych przez nich transakcji będą się różnić. W związku z tym w systemie *peer-to-peer* mogą funkcjonować różne wersje historii transakcji. Ponieważ historia transakcji jest podstawą identyfikacji uprawnionych właścicieli, dysponowanie różnymi sprzecznymi historiami transakcji stanowi poważne zagrożenie dla integralności systemu. Dlatego istotne jest, aby znaleźć sposób umożliwiający albo zapobieganie pojawianiu się różnych historii transakcji, albo decydowanie, która historia transakcji odpowiada prawdzie. Ze względu na charakter całkowicie rozproszonego systemu *peer-to-peer* zastosowanie pierwszej z metod nie jest możliwe. W efekcie musimy określić, na podstawie jakiego kryterium będziemy ustalać i wybierać jedną historię transakcji, którą uznamy za prawdziwą. I jest jeszcze jeden problem: w całkowicie rozproszonym systemie *peer-to-peer* nie ma organu centralnego, który mógłby określić, którą historię transakcji należałoby wybrać. Okazuje się, że problem ten można rozwiązać, umożliwiając każdemu z węzłów systemu *peer-to-peer* samodzielne decydowanie, która historia transakcji odpowiada prawdzie, w taki sposób, aby większość uczestników systemu niezależnie zgodziła się z tą decyzją. Okazuje się także, że rozwiązanie tego problemu zawiera sam sposób, w jaki łańcuch bloków umożliwia dodawanie nowych transakcji do struktury danych łańcucha bloków z atrybutem „tylko-do-dopisywania". Kryteria te i sposób ich stosowania wyjaśnimy szczegółowo na etapie 19.

Streszczenie

Na tym etapie określiliśmy siedem zadań, tworzących etapy pełnej wyzwań intelektualnej podróży w świat koncepcji opisujących łańcuch bloków. Po wykonaniu tych zadań zdobędziemy szczyt: zrozumiemy łańcuch bloków. Na etapie 21 połączymy wszystkie te koncepcje i będziemy mogli cieszyć się efektami nabytej wiedzy. Etap 21 to rozdział podsumowujący, jak ten, ale wymagający wiedzy technicznej, którą zdobędziesz podczas dalszej lektury.

Podsumowanie

- Aby zaprojektować całkowicie rozproszony system rejestrów *peer-to-peer* w celu zarządzania własnością, należy odnieść się do następujących zadań, którymi są:
  - opis własności,
  - ochrona własności,
  - przechowywanie danych transakcji,
  - przygotowywanie rejestrów do rozproszenia w niezaufanym środowisku,
  - rozpraszanie rejestrów,
  - dodawanie nowych transakcji do rejestrów,
  - określanie, które rejestry odpowiadają prawdzie.
- Zadania opisane powyżej zostaną omówione na kolejnych 12 etapach.

Skorowidz

E

F

H

I

K

L

Ł

M

N

O

P

R

S

Ś

T

U

W

Z

Ź

Łańcuch bloków. Czym jest? Do czego się przyda? W jaki sposób działa?

W pewnym uproszczeniu łańcuch bloków (blockchain) jest rozproszoną bazą danych, która utrzymuje stale rosnącą liczbę rekordów danych zabezpieczonych kryptograficznie przed manipulacją i próbą naruszenia integralności. Może posłużyć jako rozproszona księga rachunkowa. Technologia ta cieszy się dużym zainteresowaniem, a niektórzy entuzjaści nazywają ją nawet przełomową. Aby zrozumieć, do czego łańcuch bloków może się przydać, poprawnie ocenić uzasadnienie biznesowe startupów wykorzystujących łańcuch bloków czy też móc śledzić dyskusję na temat jego oczekiwanych efektów ekonomicznych, konieczne jest zrozumienie podstawowych pojęć związanych z technologią blockchain i uświadomienie sobie jej potencjalnych zastosowań.

Ta publikacja stanowi przystępne wprowadzenie do założeń technologii łańcucha bloków. Poszczególne pojęcia przedstawiono bez nadmiernej liczby szczegółów technicznych. Dzięki książce można przyswoić takie koncepcje związane z łańcuchem bloków jak transakcje, wartości haszujące, kryptografia, struktury danych, systemy peer-to-peer, systemy rozproszone, integralność systemu i konsensus w systemach rozproszonych. Książka została napisana w stylu konwersacyjnym, w sposób umożliwiający etapowe, stopniowe poznawanie problematyki. Matematyczne podstawy kryptografii i algorytmów zostały celowo pominięte, a zamiast tego zastosowano metafory i analogie. Dzięki temu zawarte tu treści będą zrozumiałe nawet dla czytelników bez przygotowania technicznego.

W książce między innymi:

- główne koncepcje inżynierii programowania i potrzebna terminologia
- zastosowanie łańcucha bloków i zalety tej technologii
- wewnętrzne zasady działania łańcucha bloków
- ograniczenia łańcucha bloków i sposoby ich przezwyciężania
- omówienie kierunków prac rozwojowych nad technologią
- wykorzystywanie łańcucha bloków w warunkach rzeczywistych

Dr Daniel Drescher zawodowo zajmuje się bankowością. Od wielu lat pracuje w różnych bankach. Specjalizuje się w elektronicznym obrocie papierami wartościowymi. Jest ekspertem w dziedzinie automatyzacji, uczenia maszynowego i zagadnień big data w kontekście obrotu papierami wartościowymi.

ISBN 978-83-283-8486-6