

## Laboratorium nr 9

# Badanie mechanizmów blockchain

Czas wykonania: lab 9

Liczba punktów: 5 + 2

PRK: T-L-6

## 1. Opis laboratorium

Celem laboratorium jest przebadanie koncepcji mechanizmu dowodu wykonania pracy (PoW, Proof-of-Work) będącego głównym elementem, który umożliwił powstanie pierwszej kryptowaluty, tj. Bitcoina. Mechanizm PoW umożliwia zbudowania protokołu konsensusu, w którym wiele stron jest w stanie uzgodnić stan rejestru. W przypadku kryptowalut rejestrem jest zbiór transakcji, których wynik pokazuje stanu środków na kontach. System działa, dopóki węzły posiadające ponad 50% mocy obliczeniowej są uczciwe.

### Materiały pomocnicze:

1. Wykład dotyczący Blockchain
2. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System,  
<https://bitcoin.org/bitcoin.pdf>

## 2. Zadania do wykonania

Zaimplementuj aplikację demonstrującą działanie mechanizmu Proof-of-Work (PoW) wykorzystywanego w kryptowalucie Bitcoin.

- 1) **Zadanie 11.1** (4) – Utwórz komponent implementujący tzw. kopanie nowych bloków:
  - a) komponent przyjmuje na wejściu serie skrótów z transakcji (czyli tablice stringów lub bajtów) oraz skrót z poprzedniego bloku;
  - b) komponent na wyjściu zwraca blok zawierający:
    - i) skrót z wszystkich transakcji obliczony z wykorzystaniem drzewa Merkla;
    - ii) skrót z poprzedniego bloku;
    - iii) aktualny czas oraz numer bloku;
    - iv) liczbę losową;
    - v) skrót z punktów i-iv posiadający  $j$  pierwszych bitów ustawionych na 0;
  - c) Obliczanie skrótu z punktu b)v) jest problemem obliczeniowym wymagającym włożenia konkretnej mocy obliczeniowej. Aby uzyskać ten skrót wybieramy kolejne liczby losowe, dopóki uzyskamy wymaganą liczbę zerowych **bitów** na początku (*częstym błędem jest szukanie zerowych wartości w zapisie hex lub bajtów*). Liczbą  $j$  steruje się trudnością problemu, np.  $j=30$ , czyli 30 zerowych bitów na początku to  $2^{30} = 1073741824$  liczb losowych do sprawdzenia.
  - d) Jako funkcje skrótu należy wykorzystać SHA256.
  - e) Przetestuj, czy komponent działa z użyciem aplikacji konsolowej.
- 2) **Zadanie 11.2** – (1 pkt) - Jaką  $j$  musi mieć wartość, aby na twoim komputerze blok był wykopywany co 1 s, co 1 min oraz co 10 min? Wykonaj testy używając programu z zadania 1.
- 3) **Zadanie 11.3** (opcjonalne, 5 pkt) – Zasymuluj działanie mechanizmu PoW dla 4 węzłów (z wykorzystaniem komponentu opracowanego w zadaniu 1. W tym celu:

- a) Każdy z węzłów kopiących to osobny proces (lub kopia programu uruchomiona na innym porcie) posiadający uruchomiony komponent z pkt 1.
  - i) Tworzymy też węzeł pośrednika symulujący sieć. Generuje on co 1s nowy skrót z transakcji. Następnie wysyła go do węzłów 1-4.
  - ii) Węzeł kopiący po wykopaniu bloku wysyła go do węzła pośrednika, a węzeł pośrednik do pozostałych węzłów kopiących.
  - iii) Węzeł pośrednik wyświetla informacje o każdym wykopanym bloku na konsoli.
  - iv) Węzeł kopiący po otrzymaniu informacji od pośrednika o nowo wykopanym bloku zaprzestaje wydobywania aktualnego bloku i stara się wydobyć kolejny blok biorąc otrzymany od pośrednika jako wejściowy.
  - v) Należy uwzględnić możliwość desynchronizacji. Węzeł pośrednika odrzuca blok z numerem  $x$ , jeżeli blok  $x$  z został już wykopany.
  - vi) Uwaga: w zadaniu w celu jego ułatwienia pomijamy kwestie sprawdzania transakcji, przechowywania blockchain oraz zakładamy, że wszystkie węzły zawsze otrzymają wykopany blok na czas i blockchain się nie rozgałęzi.
- b) Dobierz eksperymentalnie tak wartość  $j$  aby blok w twojej zasymulowanej sieci z pkt. 3 wydobywał się co 10 sekund. Jak to wartość?