

УДК 004.75:004.94

О.А. Дмитрієва, д-р техн. наук, професор  
А.С. Погорєлов, аспірант  
Донецький національний технічний університет, м. Покровськ, Україна  
olga.dmytriyeva@donntu.edu.ua, andrewpogorelov@gmail.com

## Математичне моделювання процесу поширення повідомлень із застосуванням орієнтованих зважених графів у приватних блокчейн-мережах

*Статтю присвячено питанням розробки і обґрунтування математичних моделей процесів поширення повідомлень різного розміру у розподіленій мережі, що дозволяє імітувати функціонування мережі в залежності від розмірів повідомлень та часових характеристик на основі даних про пропускну спроможність каналів передачі між окремими вузлами. Структуру мережі представлено орієнтованим зваженим графом та відповідною матрицею залежностей пропускну спроможностей дуг від розміру повідомлень. Елементи матриці залежності сформовано шляхом виміру пропускну спроможностей каналів з варіюванням розміру повідомлення у певному інтервалі. Для пошуку найкоротшого шляху поширення повідомлення використано алгоритм Дейкстри. Здійснено перевірку адекватності моделі за допомогою визначення експериментальних показників при паралельній передачі повідомлень, проведено порівняльний аналіз отриманих результатів з теоретично розрахованими показниками.*

**Ключові слова:** моделювання, передача повідомлень, орієнтований граф, зважений граф, розподілені мережі, блокчейн.

DOI: 10.31474/1996-1588-2020-2-31-4-13

### Вступ

Розвиток технології блокчейн призвів до значного зростання кількості алгоритмів консенсусу з різними особливостями та функціональними можливостями [1,2]. Існують підстави вважати, що надалі активного розвитку набудуть рішення для функціонування приватних блокчейн-мереж [3]. Для проектування даних рішень може бути корисним порівняння пропускну спроможності мережі при використанні різних алгоритмів консенсусу, кількості вузлів мережі та розмірів повідомлення, яке не потребуватиме розробки складного програмного забезпечення або створення тестових мереж, що дозволить швидше приймати рішення [4] стосовно вибору основних засобів для функціонування мережі.

**Метою роботи** є розробка оптимізаційної математичної моделі процесу поширення повідомлень у розподілених мережах, що функціонують на основі технології блокчейн для змінюваної кількості вузлів.

**Завдання дослідження** полягають у формулюванні теоретичних положень математичної моделі та перевірки її адекватності за допомогою порівняння теоретичних результатів з експериментальними показниками.

### Основні припущення для розробки моделі

Процес передачі інформації в розподілених

мережах, що функціонують за допомогою блокчейн-технології, відбувається за принципом комутації повідомлень [5,6]. При одержанні транзакції або нового блоку від інших вузлів, вузол перевіряє інформацію, зберігає її та анонсує (передає) далі всім іншим відомим йому вузлам мережі, окрім вузла, що надіслав повідомлення. Якщо до вузла надходить дублікат повідомлення, вузол одержувач зберігає лише одну (першу) його копію. Таким чином, для дослідження даного процесу, можна сформулювати відповідну математичну модель, що базується на наступних положеннях [7].

Зважаючи на те, що розподілена мережа використовує механізм комутації повідомлень, її можна представити у вигляді орієнтованого зваженого графу з вершинами – вузлами мережі, та дугами, що являють собою канали передачі. Кожний канал мережі має певну максимальну пропускну спроможність, значення якої – невід’ємне. Відповідно до визначеного рівня пропускну спроможності, час передачі повідомлення встановленого розміру являтиме собою вагу дуги. При цьому повідомлення можна вважати переданим тоді, коли вузол одержав повідомлення і записав його. Таким чином, процес поширення блоку інформації між вузлами мережі є класичним завданням пошуку найкоротшого шляху [7, 8].

Розв’язати таке завдання можна за допомогою великої кількості існуючих алгоритмів [9, 10] (Дейкстри, Беллмана-Форда-Мур,

Флойда-Уоршелла та ін. [7]). Відповідно до [5], для незначної кількості вершин (до 10) найбільш результативним є алгоритм Флойда-Уоршелла, при кількості вершин з 11 до 18 – алгоритм Беллмана-Форда-Мура, а у випадку з більшою кількістю вершин – алгоритм Дейкстри. Оскільки кількість вершин в мережі заздалегідь не регламентується, в роботі за основу прийнято алгоритм Дейкстри, через оптимальний час розрахунку для графів різного розміру.

### Положення моделі

Теоретичний показник пропускної спроможності каналу між вузлами при одночасній паралельній передачі повідомлень визначається та обмежується наступними співвідношеннями, прийнятими в рамках сформованої моделі.

Сукупна теоретична пропускна спроможність каналів (дуг), що виходять з одного вузла, не перевищує встановлену максимальну пропускну спроможність для даного вузла мережі:

$$\sum_{i=0}^n R_i \leq R_{\max}, \quad (1)$$

де  $R_i$  – фактична пропускна спроможність каналу, Мбайт/с;  $R_{\max}$  – максимальна пропускна спроможність вузла мережі, що надсилає повідомлення, Мбайт/с.

У випадку, коли сума пропускних спроможностей каналів при паралельній передачі перевищує максимальну пропускну спроможність вузла мережі, сукупна теоретична пропускна спроможність розподіляється між каналами пропорційно їх середнім значенням при послідовній передачі:

$$R_{i-\text{teor}} = \frac{R_i}{\sum_{i=0}^n R_i} \cdot R_{\max}. \quad (2)$$

Виходячи з вищеприведеного, процес визначення часу поширення повідомлення в розподіленій мережі поділяється на наступні етапи:

- встановлення розміру повідомлення  $b$  (Мбайт);
- розрахунок ваг дуг відповідно до співвідношення:

$$-t = \frac{R}{b}, \quad (3)$$

де  $R$  – пропускна спроможність каналу передачі (дуги) між вузлами, Мбайт/с;

- визначення шляхів поширення повідомлення між вузлами мережі.

Процес поширення повідомлення в розподіленій мережі можна надати в наступному

вигляді. Нехай мережа  $G(V, U)$  з множиною вершин  $V = \{1, 2, \dots, n\}$  і множиною дуг  $U = \{(i, j)\}$  задана матрицею залежностей пропускних спроможностей дуг  $R$  (Мбайт/с) від індексу розміру повідомлення (4), що являють собою поліноми другого ступеня з найбільшою величиною достовірності апроксимації для набору точок:

$$R = \begin{bmatrix} 0 & R_{12}(i) & 0 & R_{14}(i) \\ R_{21}(i) & 0 & R_{23}(i) & 0 \\ R_{31}(i) & 0 & 0 & 0 \\ R_{41}(i) & 0 & 0 & 0 \\ 0 & R_{52}(i) & 0 & 0 & \dots \\ 0 & R_{62}(i) & R_{63}(i) & R_{64}(i) \\ 0 & 0 & 0 & R_{74}(i) \\ 0 & 0 & R_{83}(i) & 0 \\ 0 & R_{16}(i) & 0 & 0 \\ R_{25}(i) & 0 & 0 & 0 \\ 0 & R_{36}(i) & 0 & R_{38}(i) \\ R_{45}(i) & R_{46}(i) & 0 & 0 \\ \dots & 0 & 0 & R_{57}(i) & R_{58}(i) \\ 0 & 0 & 0 & 0 \\ R_{75}(i) & 0 & 0 & R_{78}(i) \\ R_{85}(i) & 0 & R_{87}(i) & 0 \end{bmatrix}, \quad (4)$$

де  $i$  – індекс розміру повідомлення у векторі розмірів повідомлення  $B$ .

Залежності даної матриці формуються шляхом виміру пропускних спроможностей каналів з варіюванням розміру повідомлення у певному інтервалі. Наприклад, для залежностей даної матриці використаний вектор розмірів  $B = \{1, 5, 10, 20, 50, 100\}$  (Мбайт):

$$\begin{aligned} R_{12}(i) &= -3,9423 \cdot x^2 + 30,799 \cdot x - 7,7366, \\ R_{14}(i) &= -0,2373 \cdot x^2 + 2,7843 \cdot x - 0,1413, \\ R_{16}(i) &= -0,3436 \cdot x^2 + 3,1584 \cdot x - 0,7461, \\ R_{21}(i) &= -1,3001 \cdot x^2 + 13,184 \cdot x + 7,7786, \\ R_{23}(i) &= -0,3701 \cdot x^2 + 2,9606 \cdot x + 1,2384, \\ R_{25}(i) &= -0,3414 \cdot x^2 + 3,4854 \cdot x - 0,7437, \\ R_{31}(i) &= -0,5209 \cdot x^2 + 5,0796 \cdot x - 2,0562, \\ R_{36}(i) &= -0,1967 \cdot x^2 + 2,2193 \cdot x - 0,7878, \\ R_{38}(i) &= -0,166 \cdot x^2 + 2,2465 \cdot x - 0,5901, \end{aligned}$$

$$\begin{aligned}
R_{41}(i) &= -0,3186 \cdot x^2 + 3,2732 \cdot x - 0,7487, \\
R_{45}(i) &= -1,2993 \cdot x^2 + 11,076 \cdot x + 5,5878, \\
R_{46}(i) &= -0,918 \cdot x^2 + 7,2659 \cdot x + 5,198, \\
R_{52}(i) &= -0,389 \cdot x^2 + 4,202 \cdot x - 1,6355, \\
R_{57}(i) &= -0,2066 \cdot x^2 + 2,4006 \cdot x - 1,0063, \\
R_{58}(i) &= -0,0908 \cdot x^2 + 1,465 \cdot x - 0,6907, \\
R_{62}(i) &= -0,2396 \cdot x^2 + 2,78 \cdot x - 1,2256, \\
R_{63}(i) &= 0,0998 \cdot x^2 + 0,1824 \cdot x + 0,6468, \\
R_{64}(i) &= -0,1656 \cdot x^2 + 3,1768 \cdot x - 1,4634, \\
R_{74}(i) &= -0,1115 \cdot x^2 + 1,9398 \cdot x - 0,6787, \\
R_{75}(i) &= -0,1945 \cdot x^2 + 2,3808 \cdot x - 1,1231, \\
R_{78}(i) &= -0,3949 \cdot x^2 + 4,0641 \cdot x - 1,5748, \\
R_{83}(i) &= -0,5516 \cdot x^2 + 4,6761 \cdot x - 3,0359, \\
R_{85}(i) &= -0,055 \cdot x^2 + 1,1904 \cdot x - 0,4022, \\
R_{87}(i) &= -0,4737 \cdot x^2 + 4,3691 \cdot x - 1,9147.
\end{aligned}$$

За умови, що розмір повідомлення становить  $b = 1$  Мб ( $i = 1$ ) і максимальна пропускна спроможність кожного вузла мережі – 1 Гбіт/с (125 Мбайт/с), сукупність пропускної спроможності каналів від будь-якого одного вузла мережі не перевищуватиме даного значення:

$$\begin{aligned}
R_{s1}(i) &= R_{12}(1) + R_{14}(1) + R_{16}(1) = \\
&= 19,1201 + 2,4057 + 2,0687 = 23,5945 < 125, \\
R_{s2}(i) &= R_{21}(1) + R_{23}(1) + R_{26}(1) = \\
&= 19,6625 + 3,8289 + 2,4003 = 25,8917 < 125, \\
R_{s3}(i) &= R_{31}(1) + R_{36}(1) + R_{38}(1) = \\
&= 2,5025 + 1,2348 + 1,4904 = 5,2277 < 125, \\
R_{s4}(i) &= R_{41}(1) + R_{45}(1) + R_{46}(1) = \\
&= 2,2059 + 15,3645 + 11,5459 = 29,1163 < 125, \\
R_{s5}(i) &= R_{52}(1) + R_{57}(1) + R_{58}(1) = \\
&= 2,1775 + 1,1877 + 0,6835 = 4,0487 < 125, \\
R_{s6}(i) &= R_{62}(1) + R_{63}(1) + R_{64}(1) = \\
&= 1,3148 + 0,929 + 1,5478 = 3,7916 < 125, \\
R_{s7}(i) &= R_{74}(1) + R_{75}(1) + R_{78}(1) = \\
&= 1,1497 + 1,0632 + 2,0944 = 4,3073 < 125, \\
R_{s8}(i) &= R_{83}(1) + R_{85}(1) + R_{87}(1) = \\
&= 1,0886 + 0,7332 + 1,9807 = 3,8025 < 125.
\end{aligned}$$

Таким чином, значення пропускних спроможностей каналів, що наведені у (4) також будуть адекватно відображати пропуску спроможність при паралельній передачі даних всім пов'язаним вузлам.

Відповідно, за формулою (3) визначимо матрицю часу передачі повідомлення необхідного розміру (1 Мбайт) між вузлами (5) і побудуємо схему графу мережі (с) (рис. 1):

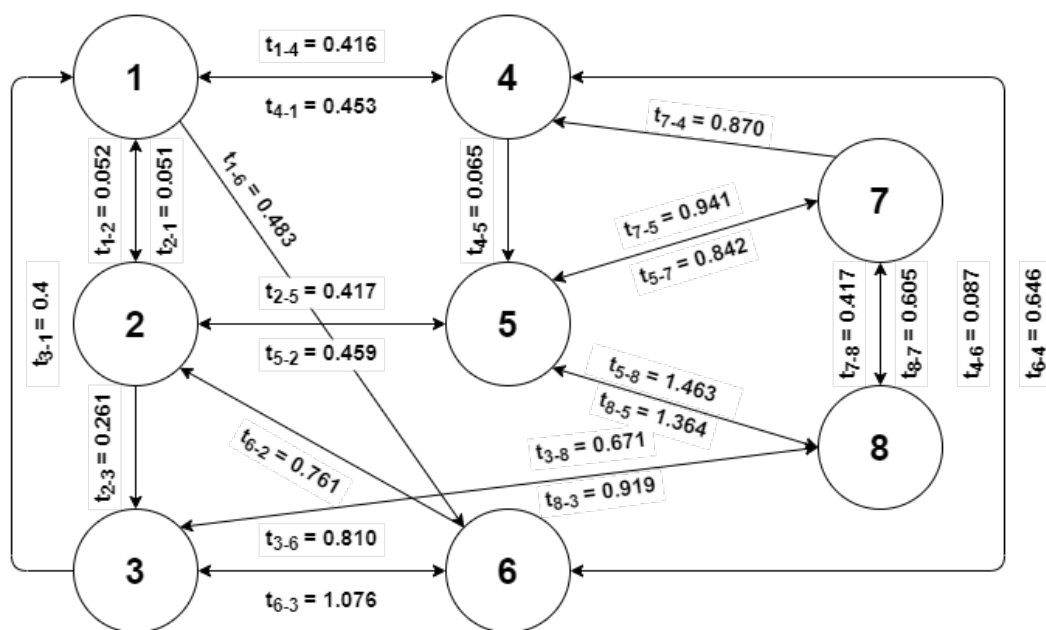


Рисунок 1 – Граф розподіленої мережі G

$$T(1) = \begin{bmatrix} - & 0,052 & - & 0,416 \\ 0,051 & - & 0,261 & - \\ 0,4 & - & - & - \\ 0,453 & - & - & - \\ - & 0,459 & - & - & \dots \\ - & 0,761 & 1,076 & 0,646 \\ - & - & - & 0,870 \\ - & - & 0,919 & - \\ - & 0,483 & - & - \\ 0,417 & - & - & - \\ - & 0,810 & - & 0,671 \\ 0,065 & 0,087 & - & - \\ \dots & - & - & 0,842 & 1,463 \\ - & - & - & - \\ 0,941 & - & - & 0,477 \\ 1,364 & - & 0,505 & - \end{bmatrix} \quad (5)$$

Визначимо час поширення повідомлення мережею. Користуючись алгоритмом Дейкстри можна розрахувати найкоротший шлях до кожного вузла мережі з вузла 1 (витоку), який першим одержав повідомлення:

$$t_{1-2} = 0,052 \text{ c}, \quad t_{1-5} = 0,469 \text{ c}, \\ t_{1-3} = 0,313 \text{ c}, \quad t_{1-6} = 0,483 \text{ c},$$

$$t_{1-4} = 0,416 \text{ c}, \quad t_{1-7} = 1,311 \text{ c}, \\ t_{1-8} = 0,984 \text{ c}.$$

Таким чином, час поширення повідомлення розміром 1 Мбайт мережею з вузла 1 дорівнюватиме найдовшому шляху і складе 1,311с.

### Перевірка адекватності моделі

Для перевірки адекватності положень моделі було проведено ряд експериментів із застосуванням хмарних серверів (Amazon EC2 t2.micro, 1 CPU, 1Gb RAM), розташованих в різних зонах, та пакету iperf3 для вимірювання параметрів каналів мережі. На основі отриманих результатів побудовано відповідні графіки (рис. 2-3).

На рис. 2-3 можна побачити, що сукупна пропускна спроможність каналів при паралельній передачі більша за пропуску спроможність вузла. Така ситуація може бути пояснена тим фактом, що через малий розмір повідомлення і велику пропуску спроможність окремого каналу, час передачі повідомлення цим каналом значно менший, порівняно з іншими каналами.

Даний процес передачі повідомлення може бути описаний наступним чином. Встановлюються пропускні спроможності каналів при послідовній передачі повідомлення розміром 10 Мбайт ( $i=3$ ) за допомогою відповідних залежностей:

$$R_{12(\text{посл})}(i) = -0,0904 \cdot x^2 + 1,5748 \cdot x - 0,5945,$$

$$R_{13(\text{посл})}(i) = -0,4696 \cdot x^2 + 4,8759 \cdot x - 1,9527,$$

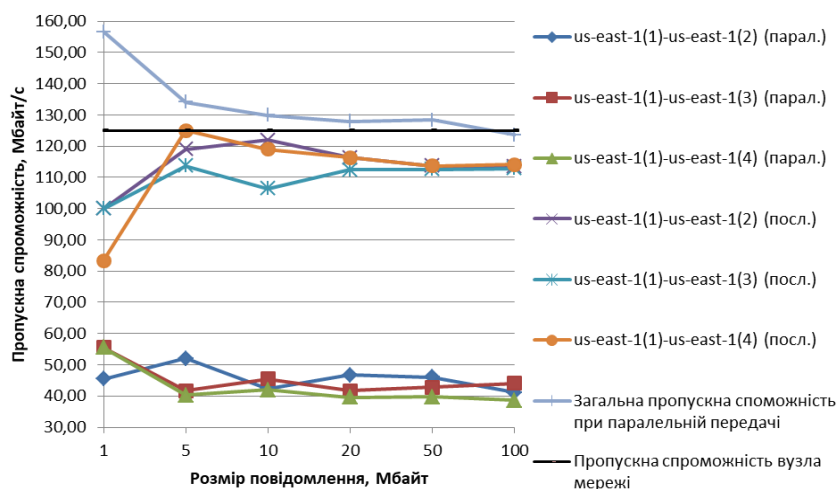


Рисунок 2 – Графіки пропускних спроможностей одержаних при послідовній та паралельній передачі повідомлень для вектору розмірів повідомлень  $B$  між одним вузлом-відправником та трьома вузлами одержувачами, що розташовані в одному регіоні

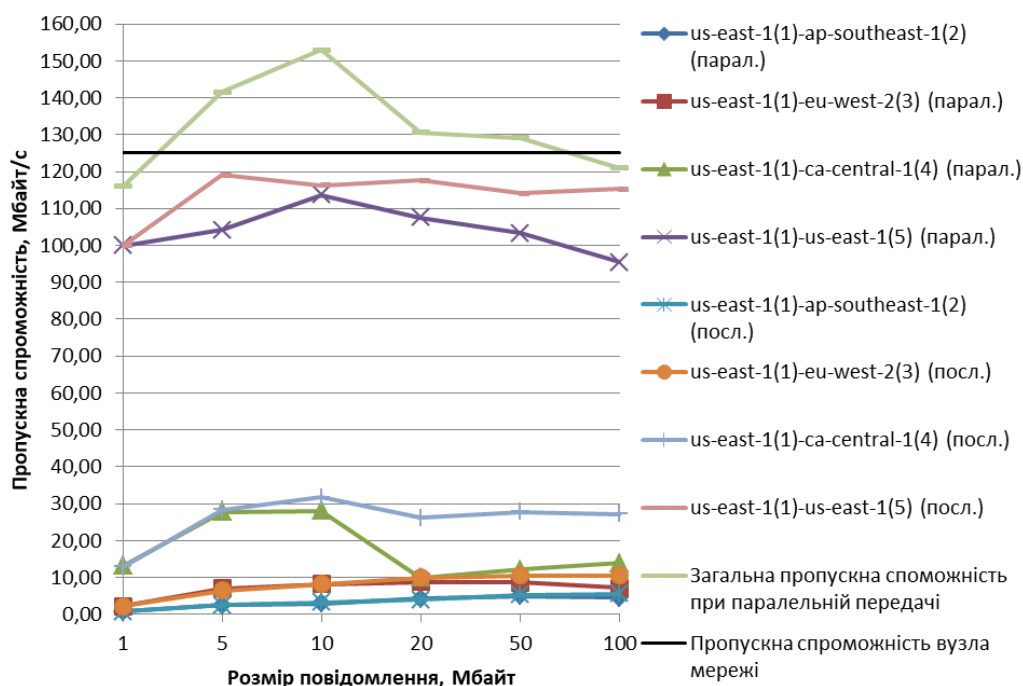


Рисунок 3 – Графіки пропускних спроможностей одержаних при послідовній та паралельній передачі повідомлень для вектору розмірів повідомлень В між одним вузлом-відправником та вузлами одержувачами, що розташовані в різних регіонах

$$R_{14(носл)}(i) = -1,5525 \cdot x^2 + 12,714 \cdot x + 4,7127,$$

$$R_{15(носл)}(i) = -1,6584 \cdot x^2 + 13,401 \cdot x + 91,972,$$

$$R_{12(носл)}(3) = -0,0904 \cdot 3^2 + 1,5748 \cdot 3 - 0,5945 = 3,32 \text{ Мбайт/с},$$

$$R_{13(носл)}(3) = -0,4696 \cdot 3^2 + 4,8759 \cdot 3 - 1,9527 = 8,45 \text{ Мбайт/с},$$

$$R_{14(носл)}(3) = -1,5525 \cdot 3^2 + 12,714 \cdot 3 + 4,7127 = 28,88 \text{ Мбайт/с},$$

$$R_{15(носл)}(3) = -1,6584 \cdot 3^2 + 13,401 \cdot 3 + 91,972 = 117,25 \text{ Мбайт/с}.$$

Оскільки  $R_{15(носл)}(3) > R_{14(носл)}(3) > R_{13(носл)}(3) > R_{12(носл)}(3)$  час передачі повідомлення однакового розміру між вузлами буде підпорядковуватися наступному співвідношенню:  $t_{15} < t_{14} < t_{13} < t_{12}$ . Пропускна спроможність вузла-відправника становить  $R_g = 125$  Мбайт/с.

Для інтервалу від 0 до  $t_{15}$  (с), за допомогою (2) розраховуються пропускні спроможності:

$$R_{заг} = R_{12(носл)} + R_{13(носл)} + R_{14(носл)} + R_{15(носл)} = 3,32 + 8,45 + 28,88 + 117,25 = 157,9 \text{ Мбайт/с},$$

$$R_{12(1)} = \frac{R_{12(носл)} \cdot R_g}{R_{заг}} =$$

$$= \frac{3,32 \cdot 125}{157,9} = 2,63 \text{ Мбайт/с},$$

$$R_{13(1)} = \frac{R_{13(носл)} \cdot R_g}{R_{заг}} =$$

$$= \frac{8,45 \cdot 125}{157,9} = 6,69 \text{ Мбайт/с},$$

$$R_{14(1)} = \frac{R_{14(носл)} \cdot R_g}{R_{заг}} =$$

$$= \frac{28,88 \cdot 125}{157,9} = 22,86 \text{ Мбайт/с},$$

$$R_{15(1)} = \frac{R_{15(носл)} \cdot R_g}{R_{заг}} =$$

$$= \frac{117,25 \cdot 125}{157,9} = 92,82 \text{ Мбайт/с},$$

$$R_{12(1)} \leq R_{12(носл)} \Rightarrow R_{12(1)} = 2,63 \text{ Мбайт/с},$$

$$R_{13(1)} \leq R_{13(\text{носл})} \Rightarrow R_{13(1)} = 6,69 \text{ Мбайт} / \text{с},$$

$$R_{14(1)} \leq R_{14(\text{носл})} \Rightarrow R_{14(1)} = 22,86 \text{ Мбайт} / \text{с},$$

$$R_{15(1)} \leq R_{15(\text{носл})} \Rightarrow R_{15(1)} = 92,82 \text{ Мбайт} / \text{с}.$$

Розмір частин повідомлення, що були передані за даний період можна розрахувати наступним чином:

$$t_{15} = \frac{b_{15(1)}}{R_{15(1)}} = \frac{b}{R_{15(1)}} = \frac{10}{92,82} = 0,108 \text{ с},$$

$$b_{12(1)} = R_{12(1)} \cdot t_{15} =$$

$$= 2,63 \cdot 0,108 = 0,284 \text{ Мбайт},$$

$$b_{13(1)} = R_{13(1)} \cdot t_{15} =$$

$$= 6,69 \cdot 0,108 = 0,722 \text{ Мбайт},$$

$$b_{14(1)} = R_{14(1)} \cdot t_{15} =$$

$$= 22,86 \cdot 0,108 = 2,469 \text{ Мбайт}.$$

Для інтервалу від  $t_{15}$  до  $t_{14}$  (с), за допомогою (2) розраховуються пропускні спроможності:

$$R_{\text{заг}} = R_{12(\text{носл})} + R_{13(\text{носл})} + R_{14(\text{носл})} =$$

$$= 3,32 + 8,45 + 28,88 = 40,65 \text{ Мбайт} / \text{с},$$

$$R_{12(1)} = \frac{R_{12(\text{носл})} \cdot R_{\text{г}}}{R_{\text{заг}}} =$$

$$= \frac{3,32 \cdot 125}{40,65} = 10,21 \text{ Мбайт} / \text{с},$$

$$R_{13(1)} = \frac{R_{13(\text{носл})} \cdot R_{\text{г}}}{R_{\text{заг}}} =$$

$$= \frac{8,45 \cdot 125}{40,65} = 25,98 \text{ Мбайт} / \text{с},$$

$$R_{14(1)} = \frac{R_{14(\text{носл})} \cdot R_{\text{г}}}{R_{\text{заг}}} =$$

$$= \frac{28,88 \cdot 125}{40,65} = 88,81 \text{ Мбайт} / \text{с},$$

$$R_{12(2)} \geq R_{12(\text{носл})} \Rightarrow R_{12(2)} = 3,32 \text{ Мбайт} / \text{с},$$

$$R_{13(2)} \geq R_{13(\text{носл})} \Rightarrow R_{13(2)} = 8,45 \text{ Мбайт} / \text{с},$$

$$R_{14(2)} \geq R_{14(\text{носл})} \Rightarrow R_{14(2)} = 28,88 \text{ Мбайт} / \text{с}.$$

Розмір частин повідомлення, що були передані за даний період, розраховується наступним чином:

$$t_{14} = \frac{b_{14(2)}}{R_{14(2)}} = \frac{b - b_{14(1)}}{R_{14(2)}} = \frac{10 - 2,469}{28,88} = 0,261 \text{ с},$$

$$b_{12(2)} = R_{12(2)} \cdot t_{14} =$$

$$= 3,32 \cdot 0,261 = 0,866 \text{ Мбайт},$$

$$b_{13(2)} = R_{13(2)} \cdot t_{14} =$$

$$= 8,45 \cdot 0,261 = 2,205 \text{ Мбайт}.$$

Для інтервалу від  $t_{14}$  до  $t_{13}$  (с), за допомогою (2) розраховуються пропускні спроможності:

$$R_{\text{заг}} = R_{12(\text{носл})} + R_{13(\text{носл})} =$$

$$= 3,32 + 8,45 = 11,77 \text{ Мбайт} / \text{с},$$

$$R_{12(3)} = \frac{R_{12(\text{носл})} \cdot R_{\text{г}}}{R_{\text{заг}}} =$$

$$= \frac{3,32 \cdot 125}{11,77} = 35,24 \text{ Мбайт} / \text{с},$$

$$R_{13(3)} = \frac{R_{13(\text{носл})} \cdot R_{\text{г}}}{R_{\text{заг}}} =$$

$$= \frac{8,45 \cdot 125}{11,77} = 89,76 \text{ Мбайт} / \text{с},$$

$$R_{12(3)} \geq R_{12(\text{носл})} \Rightarrow R_{12(3)} = 3,32 \text{ Мбайт} / \text{с},$$

$$R_{13(3)} \geq R_{13(\text{носл})} \Rightarrow R_{13(3)} = 8,45 \text{ Мбайт} / \text{с}.$$

Розмір частин повідомлення, що були передані за даний період, розраховується наступним чином:

$$t_{13} = \frac{b_{13(3)}}{R_{13(3)}} = \frac{b - b_{13(1)} - b_{13(2)}}{R_{13(3)}} =$$

$$= \frac{10 - 0,722 - 2,205}{8,45} = 0,837 \text{ с},$$

$$b_{12(3)} = R_{12(3)} \cdot t_{13} =$$

$$= 3,32 \cdot 0,837 = 2,78 \text{ Мбайт},$$

$$b_{13(3)} = R_{13(3)} \cdot t_{13} =$$

$$= 8,45 \cdot 0,837 = 7,07 \text{ Мбайт}.$$

Для інтервалу від  $t_{13}$  до  $t_{12}$  (с), за допомогою (2) розраховується пропускна спроможність:

$$R_{12(4)} = R_{\text{г}} = 125 \text{ Мбайт} / \text{с},$$

$$R_{12(4)} \geq R_{12(\text{носл})} \Rightarrow R_{12(4)} = 3,32 \text{ Мбайт} / \text{с}.$$

Розраховується значення  $t_{12}$ :

$$t_{12} = \frac{b_{12(4)}}{R_{12(4)}} = \frac{b - b_{12(1)} - b_{12(2)} - b_{12(3)}}{R_{12(4)}} =$$

$$= \frac{10 - 0,284 - 0,866 - 2,78}{3,32} = 1,83 \text{ с}.$$

Теоретичні пропускні спроможності при паралельній передачі повідомлення між вузлами можна розрахувати наступним чином:

$$\begin{aligned}
 R_{12(\text{парал})} &= \frac{b}{t_{12} + t_{13} + t_{14} + t_{15}} = \\
 &= \frac{10}{1,83 + 0,837 + 0,261 + 0,108} = \\
 &= \frac{10}{3,036} = 3,29 \text{ Мбайт / с}, \\
 R_{13(\text{парал})} &= \frac{b}{t_{13} + t_{14} + t_{15}} = \\
 &= \frac{10}{0,837 + 0,261 + 0,108} = 8,29 \text{ Мбайт / с}, \\
 R_{14(\text{парал})} &= \frac{b}{t_{14} + t_{15}} = \\
 &= \frac{10}{0,261 + 0,108} = 27,1 \text{ Мбайт / с}, \\
 R_{15(\text{парал})} &= \frac{b}{t_{15}} = \frac{10}{0,108} = 92,59 \text{ Мбайт / с}.
 \end{aligned}$$

Таким чином, сукупна пропускна спроможність становитиме:

$$\begin{aligned}
 R_{(\text{парал})} &= R_{12(\text{парал})} + R_{13(\text{парал})} + \\
 &+ R_{14(\text{парал})} + R_{15(\text{парал})} = 3,29 + 8,29 + \\
 &+ 27,1 + 92,59 = 131,27 \text{ Мбайт / с}.
 \end{aligned}$$

Отже, сукупна теоретична пропускна спроможність каналів (дуг), які виходять з одного вузла, не перевищує встановлену максимальну пропускну спроможність для даного вузла мережі в кожний окремий період часу.

Вищенаведений розрахунок дозволяє також стверджувати, що у випадку, коли сума пропускних спроможностей каналів при паралельній передачі перевищує максимальну пропускну спроможність вузла мережі, сукупна теоретична пропускна спроможність розподіляється між каналами пропорційно їх середнім значенням при послідовній передачі.

Одержані експериментальні дані дозволяють припустити, що наведене твердження вірне, оскільки максимальне відхилення теоретично розрахованих часток сукупної пропускної спроможності не перевищує 14,22% порівняно з експериментально визначеними. При цьому, середній рівень відхилення становить 4,26% і 3,62% для двох різних типів експериментів.

Залежності апроксимації в матриці

пропускних спроможностей  $R$  є реальними залежностями пропускних спроможностей каналів. Для фактичної перевірки працеспроможності моделі була сформована матриця часу паралельної передачі повідомлення між вузлами (Мбайт/с) (6):

$$T^*(1) = \begin{bmatrix} - & 0,06 & - & 0,52 \\ 0,06 & - & 0,324 & - \\ 0,454 & - & - & - \\ 0,52 & - & - & - \\ - & 0,52 & - & - & \dots \\ - & 0,696 & 0,992 & 0,11 \\ - & - & - & 1,074 \\ - & - & 0,834 & - \\ - & 0,628 & - & - \\ 0,516 & - & - & - \\ - & 0,982 & - & 0,834 \\ 0,264 & 0,108 & - & - \\ \dots & - & - & 1,022 & 1,634 \\ - & - & - & - \\ 1,038 & - & - & 0,546 \\ 1,634 & - & 0,55 & - \end{bmatrix} \quad (6)$$

Схему графу мережі (рис. 4) було побудовано на основі фактичних даних.

Використовуючи алгоритм Дейкстри та дані (5) і (6), розраховувався час поширення повідомлення мережею з кожного вузла із застосуванням залежності апроксимації пропускної спроможності та фактичних показників (с):

$$T_{\text{теор}} = \begin{bmatrix} - & 0,052 & 0,313 & 0,416 \\ 0,051 & - & 0,261 & 0,467 \\ 0,400 & 0,452 & - & 0,816 \\ 0,453 & 0,505 & 0,766 & - \\ 0,510 & 0,459 & 0,720 & 0,926 & \dots \\ 0,812 & 0,761 & 1,022 & 0,646 \\ 1,323 & 1,375 & 1,396 & 0,870 \\ 1,319 & 1,371 & 0,919 & 1,375 \\ 0,469 & 0,483 & 1,311 & 0,984 \\ 0,417 & 0,534 & 1,259 & 0,932 \\ 0,869 & 0,810 & 1,176 & 0,671 \\ 0,065 & 0,087 & 0,907 & 1,384 \\ \dots & - & 0,993 & 0,842 & 1,319 \\ 0,711 & - & 1,553 & 1,693 \\ 0,935 & 0,957 & - & 0,477 \\ 1,364 & 1,462 & 0,505 & - \end{bmatrix} \quad (8)$$

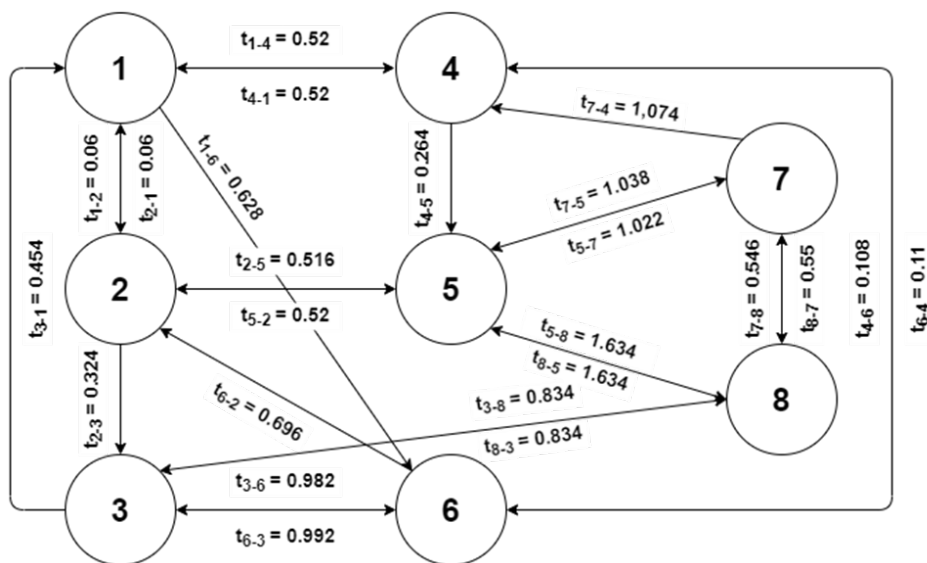


Рисунок 4 – Граф розподіленої мережі  $G$  з вагами дуг одержаними на основі фактичних показників при паралельній передачі повідомлення розміром 1 Мбайт

$$T_{\text{факт}} = \begin{bmatrix} - & 0,060 & 0,384 & 0,520 \\ 0,060 & - & 0,324 & 0,580 \\ 0,454 & 0,514 & - & 0,974 \\ 0,520 & 0,580 & 0,904 & - \\ 0,580 & 0,520 & 0,844 & 1,100 & \dots \\ 0,630 & 0,690 & 0,992 & 0,110 \\ 1,594 & 1,558 & 1,380 & 1,074 \\ 1,288 & 1,348 & 0,834 & 1,624 \end{bmatrix} \quad (9)$$

$$\begin{bmatrix} 0,576 & 0,628 & 1,598 & 1,218 \\ 0,516 & 0,688 & 1,538 & 1,158 \\ 1,030 & 0,982 & 1,384 & 0,834 \\ 0,264 & 0,108 & 1,286 & 1,738 \\ \dots & - & 1,208 & 1,022 & 1,568 \\ 0,374 & - & 1,396 & 1,826 \\ 1,038 & 1,182 & - & 0,546 \\ 1,588 & 1,732 & 0,550 & - \end{bmatrix}$$

$$\Delta = \begin{bmatrix} - & 13,333 & 18,490 & 20,000 \\ 15,000 & - & 19,444 & 19,483 \\ 11,894 & 12,062 & - & 16,222 \\ 12,885 & 12,931 & 15,265 & - \\ 12,069 & 11,731 & 14,692 & 15,818 & \dots \\ 28,889 & 10,290 & 3,024 & 487,273 \\ 17,001 & 11,746 & 1,159 & 18,994 \\ 2,407 & 1,706 & 10,192 & 15,333 \\ 18,756 & 23,089 & 17,960 & 19,212 \\ 19,186 & 22,384 & 18,140 & 19,516 \\ 15,631 & 17,515 & 15,029 & 19,544 \\ 75,379 & 19,444 & 29,471 & 20,368 \\ \dots & - & 17,798 & 17,613 & 15,880 \\ 90,107 & - & 11,246 & 7,284 \\ 9,923 & 19,036 & - & 12,637 \\ 14,106 & 15,589 & 8,182 & - \end{bmatrix} \quad (10)$$

### Висновки

Таким чином, середнє відхилення показників, прийнятих в рамках моделі, від фактичних показників, що були одержані паралельним поширенням повідомлення, складає 26,26% для повідомлення розміром 1 Мбайт. Матриця відносних відхилень від фактичних показників має наступний вигляд (%). Визначення середнього відхилення для всіх точок інтервалу розмірів  $B$  потребує значної кількості експериментів. Тому доцільно припустити рівень загального середнього відхилення на основі результатів даного розрахунку.

В рамках дослідження сформульовано математичну модель процесу поширення повідомлень в розподілених мережах на основі технології блокчейн, здійснено перевірку адекватності моделі, підтверджені її основні положення. На основі результатів, що були отримані експериментально, та виходячи з теоретичних розрахунків, які було проведено на основі розробленої математичної моделі, встановлено, що максимальне відхилення теоретично розрахованих пропорцій сукупної пропускної спроможності при паралельній передачі не перевищує 14,22% порівняно з експериментально визначеними. При цьому,



середній рівень відхилення становить 4,26% і 3,62% для двох різних типів експериментів.

За допомогою наведеної моделі також був розрахований час поширення повідомлення розподіленою мережею для однієї точки вектору розмірів повідомлення  $B$ . Середнє відхилення показників часу передачі повідомлення між вузлами, отриманих за допомогою розробленої моделі для повідомлення розміром 1 Мбайт, складає 26,26% по відношенню до фактичних показників, які були одержані паралельним поширенням повідомлення. Що дозволяє припустити рівень загального середнього відхилення на основі результатів даного розрахунку. Проведені експерименти з моделлю дозволили оцінювати пропускні спроможності мережі для змінюваної кількості вузлів – отримувачів при послідовній та паралельній

передачі повідомлень. При цьому вузли-одержувачі розміщувалися як в одному, так і в різних регіонах.

**Наукова новизна** полягає у формулюванні положень математичної моделі поширення повідомлень в розподілених мережах, що функціонують на основі технології блокчейн, із застосуванням орієнтованих зважених графів, та в обґрунтуванні адекватності даної моделі.

**Практична значимість** полягає у можливості моделювання процесу поширення повідомлень різного розміру в розподілених мережах зі змінюваною кількістю вузлів. Модель може бути застосована для пошуку найбільш близького до оптимального алгоритму консенсусу для конкретної мережі, для проектування та оптимізації вже існуючих мереж.

### Список літератури

1. Bach L. M., Mihaljevic B., Zagar M. Comparative analysis of blockchain consensus algorithms. 41<sup>st</sup> International Convention on Information and Communication Technology, Electronics and Microelectronic (MIPRO), May 21-25. 2018. Opatija: MIPRO. 2018. P. 1545-1550.
2. Alsunaidi S., Alhaidari F. A Survey of Consensus Algorithms for Blockchain Technology. 2019 International Conference on Computer and Information Sciences. 2019. P. 1-6.
3. Pawczuk L., Holdowsky J., Massey R., Hansen B. Deloitte's 2020 Global Blockchain Survey. Deloitte University Press, 2020. 44 p.
4. Stockemer D. Quantitive Methods for the Social Sciences. Springer International Publishing, 2019. 185p.
5. Amelchenko M., Dolev S. Blockchain abbreviation: Implemented by message passing and shared memory (Extended Abstract). 2017 IEEE 16<sup>th</sup> International Symposium on Network Computing and Applications (NCA), Cambridge: IEEE. 2017. P. 1-7.
6. Sadawarte Y., Gaikwad M., Patrikar R. Comparative Study of Switching Techniques for Network-on-Chip Architecture. Proceedings of the 2011 International Conference on Communication, Computing & Security (ICCCS), February 12-14. 2011. New York: Association for Computing Machinery. P. 243-246.
7. Bang-Jensen J., Gutin G. Digraphs: theory, algorithms and applications. London: Springer-Verlag, 2017. 754 p.
8. Черников А. С., Паус А. С. Многопоточная маршрутизация в программно-конфигурируемых сетях. Радиооптика. Москва: МГТУ им. Н. Э. Баумана, 2016. №6. С. 35-46.
9. Glabowski M., Musznicki B., Nowak P., Zwierzykowski P. Review and Performance Analysis of Shortest Path Problem Solving Algorithms. International Journal on Advances in Software. IARIA, 2014. Vol. 7, No. 12. P. 20-30.
10. Lewis R. Algorithms for Finding Shortest Paths in Networks with Vertex Transfer Penalties. Algorithms. Basel: MDPI, 2020. Vol. 13, No. 11. 269 p.

### References

1. Bach, L. M., Mihaljevic, B., Zagar, M. (2018), "Comparative analysis of blockchain consensus algorithms", 41<sup>st</sup> International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija, MIPRO, pp. 1545-1550.
2. Alsunaidi, S., Alhaidari, F. (2019), "A Survey of Consensus Algorithms for Blockchain Technology", International Conference on Computer and Information Sciences (ICCIS), pp. 1-6.
3. Pawczuk, L., Holdowsky, J., Massey, R., Hansen, B. (2020), Deloitte's 2020 Global Blockchain Survey, Deloitte University Press, 44 p.
4. Stockemer, D. (2019), Quantitive Methods for the Social Sciences, Springer International Publishing, 185p.
5. Amelchenko, M., Dolev, S. (2017), "Blockchain abbreviation: Implemented by message passing and shared memory" (Extended Abstract). 2017 IEEE 16<sup>th</sup> International Symposium on Network Computing and Applications (NCA), pp. 1-7.
6. Sadawarte, Y., Gaikwad, M., Patrikar, R. (2011), "Comparative Study of Switching Techniques for

Network-on-Chip Architecture", *Proceedings of the 2011 International Conference on Communication, Computing & Security*, pp. 243-246.

7. Bang-Jensen, J., Gutin, G. (2017), *Digraphs: theory, algorithms and applications*, London: Springer-Verlag, 754 p.

8. Chernikov, A. S., Paus, A. S. (2016), "Multithreaded routing in software-configurable networks" ["Mnogopotchnaya marshrutizatsiya v programmno-konfiguriruemyykh setyakh"], *Radiooptika*, No. 6, pp. 35-46.

9. Glabowski, M., Musznicki, B., Nowak, P., Zwierzykowski, P. (2014), "Review and Performance Analysis of Shortest Path Problem Solving Algorithms", *International Journal on Advances in Software*, Vol. 7, No. 12, pp. 20-30.

10. Lewis, R. (2020), *Algorithms for Finding Shortest Paths in Networks with Vertex Transfer Penalties*. Algorithms, Basel: MDPI, Vol. 13, No. 11, 269 p.

Надійшла до редакції 03.09.2020

#### **O. DMITRIEVA, A. POHORIELOV**

Donetsk National Technical University, Pokrovsk, Ukraine  
olga.dmytriyeva@donntu.edu.ua, andrewpogorelov@gmail.com

#### **MATHEMATICAL MODELING OF THE MESSAGE PROPAGATION PROCESS USING ORIENTED WEIGHTED GRAPHS IN PRIVATE BLOCKCHAIN NETWORKS**

Development of blockchain technology has led to a significant increase in the number of consensus algorithms with different features and functionality. There is reason to believe that further active development will be solutions for the operation of private blockchain networks. To design these solutions can be useful to compare network bandwidth using different consensus algorithms, number of network nodes and message size, which will not require the development of complex software or test networks, which will allow faster decision on the choice of fixed assets for network operation. The article is devoted to the development and substantiation of different sizes message propagation process mathematical models in a distributed network, which allows to simulate the network operation depending on message sizes and time characteristics based on data about bandwidth between transmission nodes. Network structure is represented by an oriented weighted graph and the corresponding matrix of bandwidth arc dependences on the size of messages. Dijkstra's algorithm was used to find the shortest way to spread the message. Model adequacy was checked by determining the experimental indicators for parallel transmission of messages, a comparative analysis of the obtained results with the theoretically calculated indicators. Scientific novelty lies in the formulation of the provisions of the mathematical model of message propagation in distributed networks operating on the basis of blockchain technology, using oriented weighted graphs, and is substantiating the adequacy of this model. The practical significance lies in the possibility of different sizes messages modeling propagation process in distributed networks with different variable number of nodes. Model can be used to find the closest to optimal consensus algorithm for a particular network, to design and optimize existing blockchain based distributed networks.

**Key words:** modeling, message passing, oriented graph, weighted graph, distributed networks, blockchain.