УДК 004.056 **DOI:10.30837/rt.2022.2.209.13**

В.І. ЮХИМЕНКО, О.І. ФЕДЮШИН, канд. техн. наук

АНАЛІЗ МАСШТАБУВАННЯ БЛОКЧЕЙН ПРОЄКТУ TELEGRAM OPEN NETWORK

Актуальність теми та постановка завдання

Блокчейн, також відомий як технологія розподіленої книги (DLT), було визнано проривною технологією в різних галузях, не тільки в криптовалютах, а ще і в фінансах, Internet of Things, охороні здоров'я, енергетиці та логістиці. У порівнянні з традиційними централізованими рішеннями блокчейн має ряд значних переваг, таких як незмінність, підвищена безпека, відмовостійкість та прозорість.

Однак децентралізована природа блокчейну різко обмежує його продуктивність (наприклад, пропускну здатність і затримку). Так, Bitcoin [1] може досягти лише низької пропускної здатності сім транзакцій в секунду (TPS), а для створення нового блоку з транзакціями потрібно близько 10 хвилин. На відміну від нього, поточні централізовані платіжні системи, такі як VisaNet і MasterCard, можуть охоплювати тисячі TPS і здійснювати платежі майже в реальному часі.

Використовуючи подібний алгоритм консенсусу, Proof-of-Work (PoW), інші блокчейн платформи, такі як Ethereum [2] і Litecoin, також успадковують недоліки продуктивності Bitcoin.

Без сумніву, проблема продуктивності стала основною перешкодою для застосування рішень на базі блокчейну у системах з великою кількістю активних користувачів. Це особливо актуально для систем, які потребують високої продуктивності, таких як онлайн-обробка транзакцій і платіжні системи в режимі реального часу.

Щоб подолати цю проблему, розробники блокчейн систем докладають зусиль, щоб покращити свою продуктивність, наприклад, змінюючи структуру системи та розробляючи нові алгоритми консенсусу. Для вирішення цієї проблеми запропоновано багато методів, таких як використання side-chain, off-chain та орієнтованих ациклічних графів [3 – 6]. Однак вони мають притаманні накладні витрати, такі як, наприклад, утворення "паразитних" ланцюжків. Шардинг став хорошим кандидатом на рішення, оскільки є стандартним рішенням для горизонтального масштабування у традиційних базах даних, то ж може бути застосованим для розподілення консенсусного навантаження та транзакцій для прискорення часу обробки транзакції та створення нового блоку[7 – 12].

Цікавим та інноваційним блокчейн проєктом є Telegram Open Network (TON) [13]. Розпочавши розробку системи у 2017 р., команда Павла Дурова та його брата, швидко привернула увагу інвесторів та криптоспільноти, заявивши, що їхня система вирішує проблеми масштабування блокчейну за допомогою шардингу, і при цьому система масштабується динамічно залежно від поточного навантаження на систему.

Мета роботи – зробити огляд блокчейн проєкту Telegram Open Network, а саме TON Blockchain, та проаналізувати безпеку, надійність та масштабування цієї системи.

TON Blockchain

У цій частині наведено опис основного компоненту екосистеми Telegram Open Network – TON Blockchain, а також стислий опис механізму динамічного шардування та консенсусної мережі.

Telegram Open Network (скор. TON) – базована на блокчейні децентралізована комп'ютерна мережа, а також проєкт захищеної вбудованим проксі та анонімайзером даркнет-платформи, побудованої на принципі оверлейної P2P-мережі, що має послуги обміну повідомленнями, платіжних операцій у криптовалюті Gram, зберігання даних, а також операційна система для розподілених програм.

Концепція TON розроблена братами Дуровими [1], які залучили під цей проєкт інвестиції у кілька мільярдів доларів та запланували переведення на TON свого популярного месенджера Telegram.

На думку рецензентів, TON, з одного боку, приваблює інвесторів ідеєю популярної криптовалюти, а з іншого – дозволяє користувачам у країнах із сильною Інтернет-цензурою вільно використовувати інформаційні ресурси, оминаючи державні системи блокування та відстеження.

30 травня 2019 р. Telegram представив спрощену версію платформи.

7 травня 2020 р., у зв'язку з відмовою команди TON від запуску проєкту після тривалих судових розглядів з комісією з цінних паперів та бірж США, на базі протоколу TON був запущений блокчейн-проєкт Everscale [14] (також відомий як Free TON).

12 травня 2020 р. Павло Дуров у своєму Telegram-каналі оголосив, що закрив блокчейн-проєкт TON.

29 червня 2021 р. Павло Дуров передав домен ton.org та GitHub-репозиторій незалежному співтовариству розробників The Open Network (TON).

TON Blockchain – це умовна назва децентралізованої мережі (сукупності ланцюжків блоків) або 2D-блокчейн, що складається з трьох основних типів блокчейнів:

- Master blockchain або Masterchain – єдиний у своєму роді ланцюжок блоків, що містить загальну інформацію про протокол і поточні значення його параметрів, набір валідаторів та їх часток, набір активних на даний момент workchains та їх «шардів» – shardchains, а також набір хешів останніх блоків workchains та shardchains .
- Working blockchains або Workchains – безліч (до 2^{32}) блокчейнів, які є «робочими волами», що містять транзакції з інформацією про переміщення активів та смарт-контракти. При цьому окремі workchains можуть мати власні «правила», формати адрес акаунтів, формати транзакцій, різні віртуальні машини для смарт контрактів, різні базові токени або криптовалюти і т.д. Але всі вони повинні відповідати деяким основним критеріям функціональної сумісності для забезпечення простої взаємодії між собою. Таким чином, TON Blockchain по суті є гетерогенним, також як блокчейни EOS та Polkadot.
- Shard blockchains або Shardchains – підмножина блокчейнів (до 2^{60}) всередині безлічі workchains, що забезпечує роботу системи шардингу і має ті самі правила та формат блоків, що й у workchains. Shardchains містять лише підмножину облікових записів, в залежності від декількох перших (найбільш значущих) бітів адреси кожного конкретного облікового запису. Оскільки всі shardchains мають загальний формат і правила побудови блоків, TON Blockchain у цьому відношенні є гомогенним і відповідає вимогам, описаним в одній з пропозицій з масштабування блокчейн системи Ethereum.

Кожен блок shardchain (так само як і masterchain) насправді не просто блок, а невеликий блокчейн. Як правило, цей «вертикальний блокчейн» складається рівно з одного блоку; таким чином, його можна вважати просто блоком відповідного йому «традиційного» блокчейна (або «горизонтального блокчейна»). Однак, якщо виникає необхідність у виправленні некоректних блоків, то в «вертикальний блокчейн» додається новий блок, який містить або заміну діючого «горизонтального» блоку, або «різницю блоків», що містить тільки опис тих частин попередньої версії блоку, які потребують заміни. Цей специфічний для TON механізм заміни виявлених некоректних блоків без необхідності hardfork отримав назву 2D-блокчейн, або просто 2-блокчейн (рис. 1). Ідея шардингу полягає в тому, щоб розділити базу даних (або розподілену базу даних, тобто блокчейн) на кілька незалежних дійсних частин – шарди (англ. “shards” – сегмент). Таким чином, база даних в першу чергу розбивається на рядки, а не на стовпці.

У результаті кожен шард складається з усіх необхідних даних. Шардинг може здійснюватися відповідно до попередньо визначеної структури або динамічно, коли транзакції можуть ініціювати роздвоєння або злиття шардів. Розробники TON пропонують динамічний шардинг на основі Infinite Sharding Paradigm (парадигма нескінченного шардингу).

Згідно з цією парадигмою кожен workchain складається з множини (розміром $2^{(0..M)}$, де M=60) shardchains, і підтримує динамічне шардування.

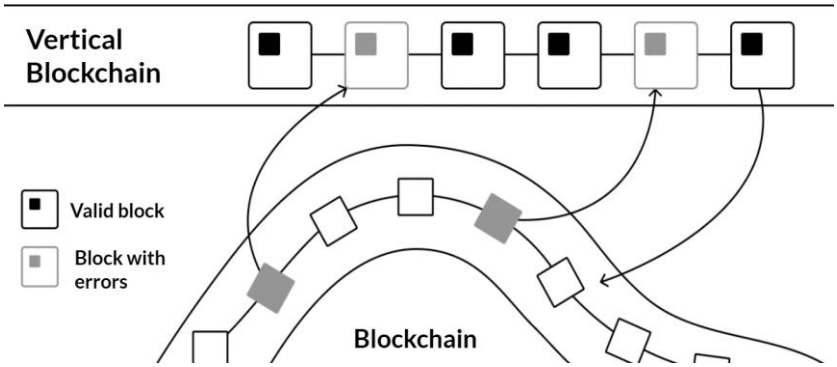

Рис. 1. Умовна схема роботи 2D-блокчейну

Кожен shardchain відповідає за підмножину облікових записів, що визначається за бітовим префіксом accound_id. Всі shardchains мають однаковий формат блоку та правила. Кожен shardchain ідентифікується shard_prefix – бітова послідовність довжиною від 0 до M. Цей префікс буде використовуватись для визначення підмножини облікових записів, що належать до даного шардчейну. Простими словами, будь-який обліковий запис, у якого бітове уявлення account_id починається з shard_prefix, вважається, що належить до даного шардчейну.

Спочатку, workchain складається тільки з одного shardchain, який відповідає за всю множину акаунтів. При цьому сценарії наш блокчейн мало відрізняється від “звичайного” одновимірного.

Але, як тільки кількість транзакцій в одному блоці помітно зростає, то наш шард розділяється (split) на два окремі shardchain, що розділяють між собою всю безліч акаунтів навпіл. При цьому перші блоки "нових" гілок ланцюжка будуть вказувати на останній блок початкового chardchain.

Аналогічно, якщо сумарне навантаження (кількість транзакцій у нових блоках) на два сусідні shardchains суттєво впало, то система може їх об'єднати (merge) в один. При цьому перший блок об'єднаного shardchain зберігатиме хеші останніх блоків з двох початкових шардів.

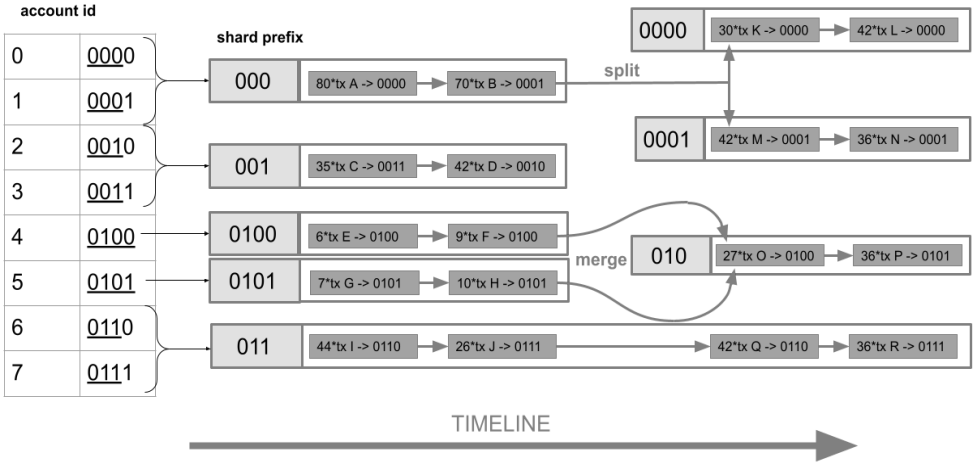

Рис. 2. Приклад split/merge операцій залежно від кількості транзакцій у блоках

Теоретично, workchain може прийти в такий стан, що на кожен обліковий запис виділено один shardchain, що містить історію змін тільки для одного облікового запису. Тож можемо вважати, що один workchain підтримує 2^M унікальних облікових записів (рис. 3).

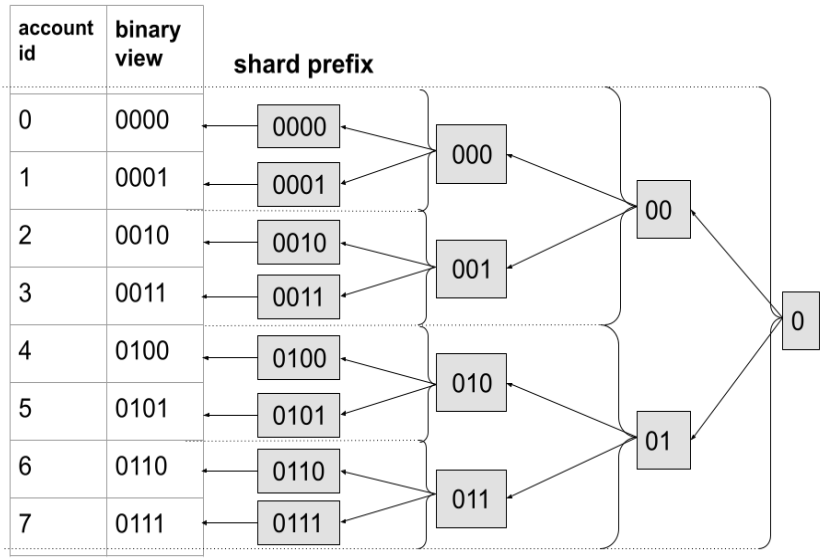

Рис. 3. Схематичний приклад максимального розшардування для M=3

Коли shardchain відповідає тільки за один аккаунт, то його називають account shard. Базуючись на інформації вище, можна скласти "ієрархію" блокчейнів у TON Blockchain (рис. 4).

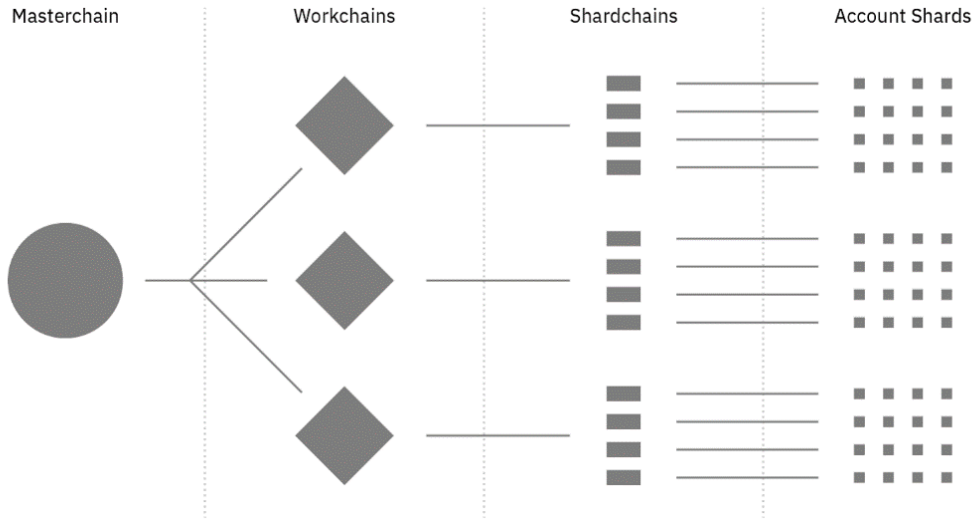

Рис. 4. Зв'язок між блокчейнами TON

Усі згадані елементи доповнюються та вкорінюються в механізм консенсусу. Механізм, який має підтримувати масштабування та, оскільки механізми синхронного консенсусу вимагають тимчасових запасів надійності, уповільнення угоди стану системи, повинен бути асинхронним. З цієї причини має бути розгорнутий асинхронний варіант Proof of Stake (PoS). У технічній документації TON [13] викладено процес прийняття рішення, що стоїть за вибором, і порівнюється делегований PoS з обраною Візантійською версією PoS з відмовос-

тійкістю (BFT). На жаль, у технічних документах бракує детального опису фактичної реалізації цього алгоритму.

Консенсусна мережа TON Blockchain складається з різних типів вузлів: валідатори, номінатори, фішери та коллатори (рис. 5).

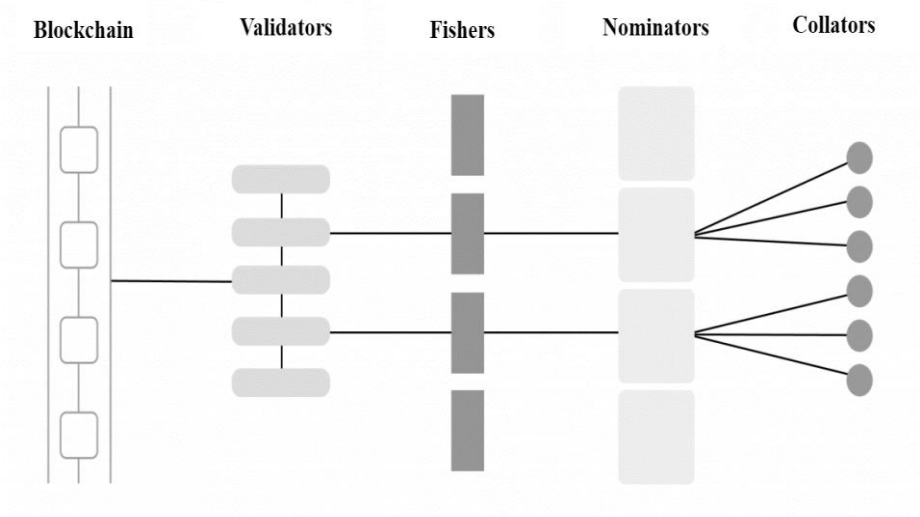

Рис. 5. Консенсусна мережа TON Blockchain

Валідаторами є вузли PoS та виробники блоків. Фішери стежать за консенсус-мережею з метою знайти помилку або виявити ймовірно зловмисний вузол консенсусу і у випадку, якщо фішер однозначно підтвердить, що вузол є таким, він отримує винагороду у вигляді конфіскації частини частки (stake) цього валідатора.

Завдання колаторів – підготовка блоків шардчейна та надання їх на валідацію PoS-вузлам, за що вони отримують свою частину винагороди за створення блоку. При цьому колатори є, по суті, додатковими учасниками консенсусу, оскільки валідатори майже завжди генерують блоки самостійно.

Номінатори надають свої активи (токени workchain) валідаторам у позику з метою отримання прибутку. Фактично, номінатори не входять до інфраструктури валідаторів, а лише поділяють свою велику початкову частку активу між ними в обмін на пропорційний відсоток від загальної винагороди. Таким чином, схема та розмір винагороди, яку отримують номінатори, повністю залежить від результатів роботи валідаторів, при цьому номінатори «голосують» за валідаторів, надаючи їм у позику свої токени. У ролі номінаторів можуть виступати як індивідуальні власники токенів, так і пули (pools), що управляють засобами окремих користувачів TON і одночасно виступають у ролі валідаторів, діючи як делегати за допомогою смарт-контракту TON. При цьому сумарна винагорода такого пулу розподіляється між його учасниками пропорційно до їхніх вкладів.

Сам процес генерації нових блоків відбувається наступним чином: деяка певна кількість валідаторів за спеціальним алгоритмом вибирають придатні для валідації блоки masterchain (шарди), потім для кожного такого шарда відбирається менше підмножини валідаторів в порядку, визначеному псевдовипадковим способом з інтервалом приблизно кожні 1024 блоки.

Таким чином, для кожного блоку існує псевдовипадково обраний набір валідаторів для визначення того, чий кандидат у блок має найвищий пріоритет. Валідатори та інші вузли перевіряють достовірність запропонованих кандидатів у блоки. У випадку, якщо валідатор автоматично (не навмисно) підписує недійсного кандидата в блоки, він карається втратою частини або всієї своєї винагороди, або зовсім відстороненням від участі у відборі валідаторів на деякий час.

Далі валідаторам необхідно досягти консенсусу на основі алгоритму BFT. Потім після досягнення консенсусу створюється новий блок, при цьому комісії за транзакції розподіляються між валідаторами.

Необхідно зазначити, що кожен валідатор може бути обраний для участі в кількох підмножинах валідаторів, тому передбачається, що всі алгоритми валідації та консенсусу запущені паралельно.

Після того, як всі нові блоки шардів ланцюга згенеровані або тайм-аут закінчено, з'являється повідомлення про те, що створено новий блок у masterchain, що включає хеші останніх блоків всіх шардів на основі BFT-консенсусу всіх валідаторів.

Аналіз масштабування Telegram Open Network

Як зазначено на початку роботи, основні критерії, за якими оцінюється ефективність масштабування, – це пропускна здатність системи (transactions per second, скорочено TPS) та середній час появи нового блоку в мережі (average block time).

Для аналізу масштабування за критерієм average block time було вирішено порівняти показники найпопулярніших блокчейн платформ (Bitcoin, Ethereum) з реалізаціями TON Blockchain (The Open Network та Everscale).

Як джерело даних було обрано сервіси для аналітики блокчейн систем, такі як: Blockchair, Ever.live, Everscan, Tonscan та Blockchain.com. Основною причиною вибору є те, що ці сервіси надають змогу досліджувати метрики блокчейн систем у реальному часі.

На основі інформації, зібраної за допомогою цих сервісів, була зроблена порівняльна таблиця (табл. 1).

Таблиця 1

Середній час появи нового блоку в мережі

Блокчейн система	Average Block Time, *c*
Bitcoin	600
Ethereum	12-14
The Open Network	3-5 (невідома кількість шардів)
Everscale	0,3 (16 шардів)

За цими даними можна сказати, що застосування динамічного шардування значно прискорює середній час створення блоку. Особливо це видно на прикладі проєкту Everscale – у порівнянні з Bitcoin у 2000 разів швидше створюється новий блок. Однак слід зазначити, що показники для The Open Network є неточними, оскільки вони базувалися на замірах розробників, а інструментів для самостійного аналізу мережі у реальному часі знайти не вдалося. Тож реальний час створення блоку може бути навіть швидшим.

Що стосується показнику transactions per second, то потрібно оцінити два показники: прогнозована пропускна здатність та TPS системи у реальному часі.

За даними Binance Research [15], загальна архітектура TON унікальна і дуже орієнтована на підтримку масштабування. З поставленим завданням підтримки «мільйони транзакцій в секунду» TON не тільки ставить надзвичайно амбітну мету, але, здається, перевершує попит галузі на 1000 порядків. Для порівняння, одна з найбільш завантажених платіжних мереж у світі, Visa, складає в середньому 1700 TPS. Результати їх прогнозу можна побачити на рис. 6.

Однак варто зазначити, що система типу TON має намір масштабувати за запитом і не намагатиметься почати з мільйонів транзакцій. Базуючись на цьому, можна припустити, що при невеликій кількості активних користувачів показники TPS будуть достатньо помірними.

Це припущення було підтверджено у ході порівняння TPS тих самих систем за допомогою сервісів для моніторингу стану блокчейн систем, використаних раніше (табл. 2).

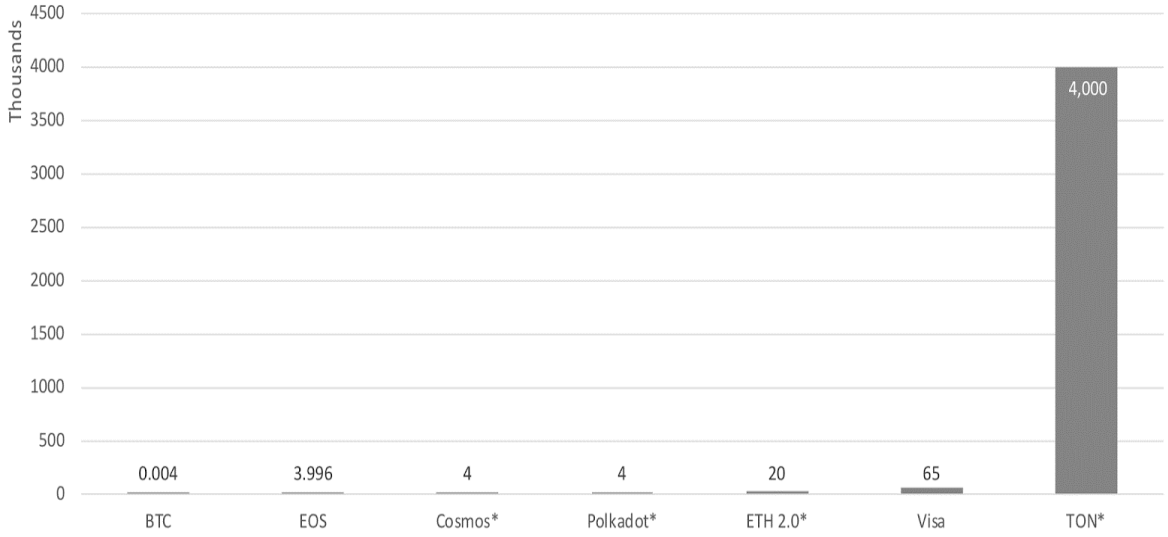

Рис. 6. Прогнозована пропускна здастність у TPS різних баз даних (у тисячах)

Таблиця 2

Реальні метрики систем станом на травень 2022

Блокчейн система	Transactions per second	Total number of transactions in last 24 hours	Total number of transactions
Bitcoin	1,98	247 680	742 642 891
Ethereum	10,21	1 056 240	1 611 997 470
The Open Network	2,02	180 738	218 035 610
Everscale	1,9	189 956	108 965 377

Як ми бачимо, за реальними показниками TPS системи-реалізації протоколу TON поки що поступаються навіть системі Bitcoin. Але варто зазначити загальне навантаження на системи TON та Everscale: кількість транзакцій за останній день та в цілому значно менші ніж у популярних систем. А базуючись на тому, що ці системи масштабуються динамічно, можна припустити, що ці показники TPS є оптимальними для користування при реальному навантаженні, оскільки ці системи ще не набули бажаної популярності у криптоспільноті.

Висновки

1. Зроблений порівняльний аналіз найпопулярніших блокчейн платформ (Bitcoin, Ethereum) з реалізаціями TON Blockchain (The Open Network та Everscale) за трьома показниками: пропускна здатність системи (transactions per second, скорочено TPS), середній час появи нового блоку в мережі (average block time) та прогнозована пропускна здатність у TPS. Для порівняння було використано сервіси аналізу блокчейн систем у реальному часі (так звані blockchain explorers) та відкрите дослідження Binance Research Group [14].

2. У ході порівняння average block time було виявлено, що застосування шардингу значно прискорює середній час появи нового блоку в мережі. Як приклад, система Everscale створює 3-4 блоки за секунду, коли Bitcoin створює один блок у середньому за 10 хвилин.

3. У ході порівняння показників TPS було виявлено, що показники TON та Everscale не є вражаючими. Однак слід зазначити, що ці системи є дуже молодими та не набули бажаної популярності серед користувачів щоб реалізувати свій потенціал у масштабуванні.

4. Базуючись на дослідженні прогнозованої пропускної здатності, можна зробити висновок, що TON та Everscale, здається, перевершують попит галузі на 1000 порядків. Тож, щоб реалізувати їхній потенціал, потрібна багатомільйонна аудиторія активних користувачів. Гарними напрямками для цього є сфера Вільного Інтернету та конкуренція з міжнародними платіжними системами типу MasterCard та Visa.

Список літератури:

1. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Working Paper, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.
2. V. Buterin. Ethereum Sharding FAQ. Accessed: Jan. 28, 2020. [Online]. Available: https://github.com/ethereum/wiki/wiki/Sharding-FAQ.
3. F. Gai, J. Niu, S. Ali Tabatabaee, C. Feng and M. Jalalzai. Cumulus: A Secure BFT-based Sidechain for Off-chain Scaling // 2021 IEEE/ACM 29th International Symposium on Quality of Service (IWQOS), 2021, pp. 1-6, doi: 10.1109/IWQOS52092.2021.9521363.
4. J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll and E. W. Felten. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies // 2015 IEEE Symposium on Security and Privacy, 2015, pp. 104-121, doi: 10.1109/SP.2015.14.
5. H. Moudoud, S. Cherkaoui, and L. Khoukhi. An IoT Blockchain Architecture Using Oracles and Smart Contracts: the Use-Case of a Food Supply Chain // IEEE Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2019.
6. C. Profentzas, M. Almgren and O. Landsiedel. TinyEVM: Off-Chain Smart Contracts on Low-Power IoT Devices // 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), 2020, pp. 507-518, doi: 10.1109/ICDCS47774.2020.00025.
7. Singh, Amritraj & Click, Kelly & Parizi, Reza & Zhang, Qi & Dehghantanha, Ali & Choo, Kim-Kwang Raymond. Sidechain technologies in blockchain networks: An examination and state-of-the-art review // Journal of Network and Computer Applications. 149. 102471. 10.1016/j.jnca.2019.102471.
8. A. Hafid, A. S. Hafid, and M. Samih. A methodology for a probabilistic security analysis of sharding-based blockchain protocols // Proc. Int. Congr. Blockchain Appl. Cham, Switzerland: Springer, 2019, pp. 101–109.
9. L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena. A secure sharding protocol for open blockchains // Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Oct. 2016, pp. 17–30.
10. G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang, and R. P. Liu. Survey: Sharding in blockchains // IEEE Access, vol. 8, 2020, pp. 14155–14181.
11. C. Huang, Z. Wang, H. Chen, Q. Hu, Q. Zhang, W. Wang, and X. Guan, RepChain: A reputation-based secure, fast and high incentive blockchain system via sharding, 2019, arXiv:1901.05741. [Online]. Available: http://arxiv.org/abs/1901.05741.
12. Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou. A survey of distributed consensus protocols for blockchain networks // IEEE Commun. Surveys Tuts., vol. 22, no. 2, pp. 1432–1465, 2nd Quart., 2020, doi: 10.1109/COMST.2020.2969706.
13. The Open Network / N. Durov. Режим доступу: https://ton.org/ton.pdf. Дата звернення: 24.05.2022.
14. Everscale Whitepaper / Mitja Goroshevsky. Режим доступу: https://everscale.network/docs/everscale-whitepaper.pdf. Дата звернення: 24.05.2022.
15. Exploring Telegram Open Network / Binance Research Group. Режим доступу: https://research.binance.com/en/analysis/telegram-open-network. Дата звернення: 24.05.2022.

Надійшла до редколегії 07.06.2022

Відомості про авторів:

Юхименко Валентин Ігорович – студент 4-го курсу спеціальності 125 Кібербезпека кафедри безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Україна; e-mail: valentin.yukhymenko@gmail.com; ORCID: http://orcid.org/0000-0002-7191-2969

Федюшин Олександр Іванович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, Україна; e-mail: oleksandr.fediushyn@nure.ua; ORCID: http://orcid.org/0000-0002-3600-405X