АНОТАЦІЯ

Грибняк С.С. Моделі та методи підвищення ефективності обробки транзакцій у розподілених реєстрах. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки. – Національний університет «Одеська політехніка», МОН України, Одеса, 2023.

У **вступі** показано актуальність та особливості застосування технології розподілених реєстрів (Distributed Ledger Technology (DLT) на основі блокчейну, яка стає все більш популярною завдяки прозорим транзакціям та відсутністю посередників або центральних керуючих органів.

Але незважаючи на потребу в застосуванні та на чисельні дослідження в галузі DLT, їх широкому розповсюдженню заважає недостатня ефективність існуючих рішень. Тому підвищення ефективності застосовуваних рішень є актуальною науково-технічною задачею, якій присвячено дане дослідження.

Визначено об'єкт, предмет, задачі та методи дослідження; наведено наукову новизну та практичне значення отриманих результатів; висвітлено особистий внесок здобувача.

В **першому розділі** дисертаційної роботи проведено аналіз існуючих технологій DLT, встановлені їх переваги та недоліки. Показано, що відомі системи, побудовані на DLT, мають ряд серйозних недоліків. Розподілена система повинна мати механізм масштабування для адаптації до зміни робочого навантаження у дуже широких межах. У той же час швидкість обробки даних у відомих популярних системах Bitcoin та Ethereum невисока – ці системи обробляють приблизно 7 та 15 транзакцій за секунду (tps) перша та до 119 tps друга. Ці показники незрівнянні з традиційними централізованими системами, що обробляють тисячі транзакцій на секунду.

Тобто виникає актуальне науково-практичне завдання підвищення ефективності обробки транзакцій в розподілених реєстрах, що передбачає

поєднання високої швидкості обробки транзакцій, високої масштабованості системи та достатньої криптозахищеності від маніпуляцій та атак.

Для вирішення цього завдання запропоновано шляхи підвищення ефективності обробки транзакцій та масштабованості розподіленого реєстру на основі двошарової моделі розподіленого реєстру.

У **другому розділі** дисертаційної роботи досліджено шляхи підвищення ефективності обробки транзакцій та масштабованості розподіленого реєстру.

Для прискорення обробки транзакцій з високим рівнем масштабованості запропоновано двошарову модель системи (рис. 1).

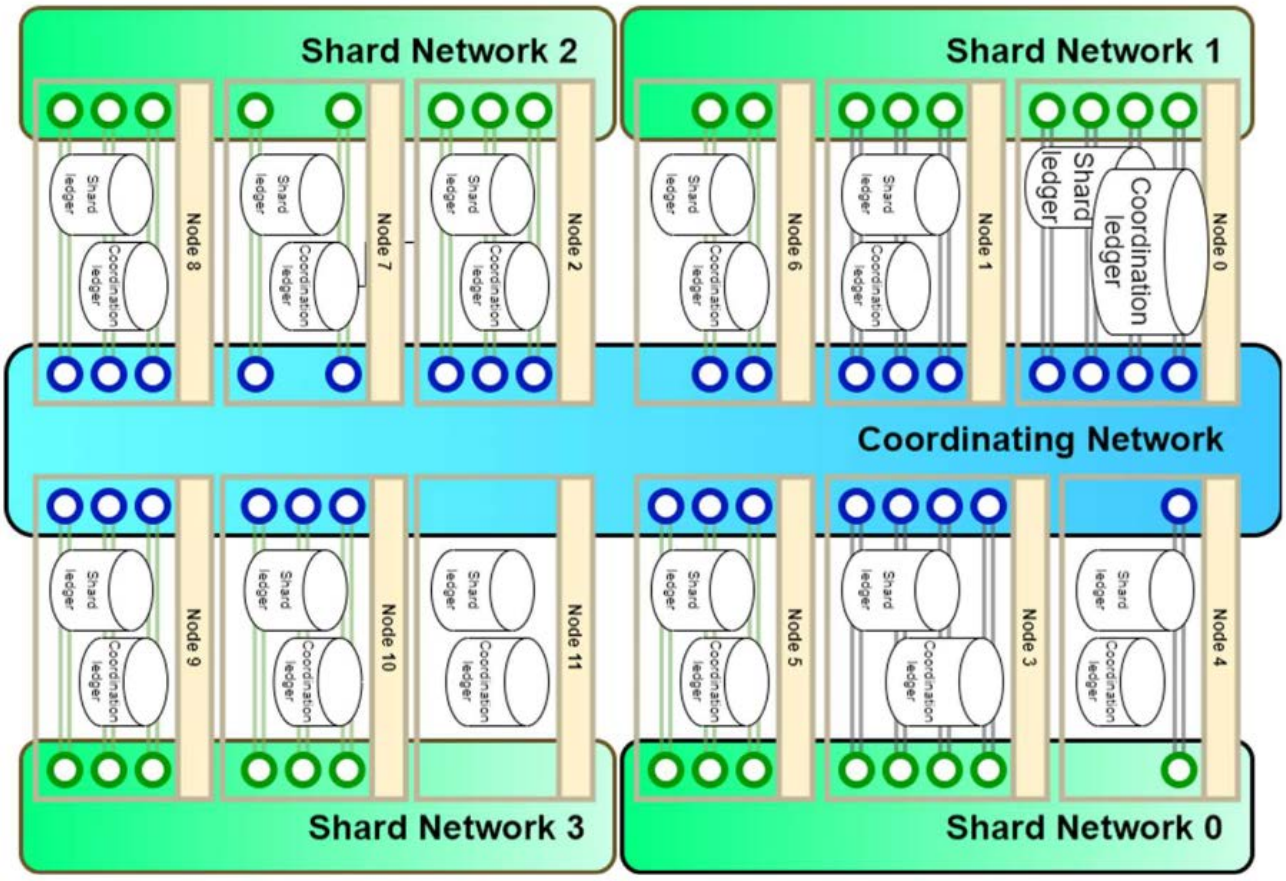

Рис. 1. Двошарова модель системи розподіленого реєстру

Основна мережа, яка призначена для формування та розповсюдження блоків, виконана за технологією BlockDAG (шар 1). Операції, пов'язані з верифікацією блоків на підставі протоколу консенсусу, винесені до координаційної мережі, що працює за технологією традиційного консенсусу (шар 2). Згідно із запропонованою моделлю всі вузли, що входять до системи і

називаються Worker'ами, отримують дві ролі – Утворювачів блоків в основній мережі та Координаторів у координаційній мережі. Таким чином розділені функції шарів мережі. В основній мережі виконуються функції формування блоків та їх поширення, що потребують операцій із об’ємними блоками. Побудова основної мережі за технологією BlockDAG суттєво прискорює процес попередньої обробки транзакцій за рахунок синхронного формування блоків. У координаційну мережу винесено операції з формування консенсусу відповідно до протоколу Proof of Stake (PoS), що вимагають великої кількості пересилань відносно коротких повідомлень. Тому робота координаційної мережі організована відповідно до традиційного блокчейн–протоколу, який виконується простіше, ніж BlockDAG .

Сформульовано перший пункт наукової новизни – вперше розроблено двошарову модель розподіленого реєстру, що поєднує в собі основну мережу, побудовану за технологією BlockDAG, та координаційну мережу, що базується на традиційній блокчейн технології, що дозволило підвищити швидкість обробки транзакцій покращило масштабованість системи.

Введено поняття хребетного блоку слота. Хребетний блок – це блок слота, якому притаманні наступні властивості:

1) має найбільшу висоту,

2) якщо таких блоків кілька, то береться блок, який посилається на більшу кількість попередніх блоків,

3) якщо таких блоків кілька, то береться той, у якого значення функції перемішування від хешу менше.

Оскільки кожен блок зберігає дерево Меркла, фактично хребетний блок зберігає в «упакованому» вигляді все «минуле» блоків даного слота. На цій підставі побудовано модель скороченого обміну інформацією між основною мережею та координаційною мережею, що зменшує інформаційне навантаження на систему в цілому та підвищує швидкість обробки транзакцій. Розроблено методику застосування обміну інформацією BlockDAG мережі з координаційною мережею на підставі моделі хребетних блоків.

Сформульовано другий пункт наукової новизни – набула подальшого розвитку модель скороченого обміну інформацією між BlockDAG мережею та координаційною мережею на основі поняття хребетного блоку, що дозволило скоротити обсяг трафіку між мережею BlockDAG та координаційною мережею і тим самим зменшити навантаження на систему загалом та підвищити швидкість обробки транзакцій.

На підставі двох запропонованих моделей сформульовано узгоджену послідовність виконання операцій в основній та координаційній мережах.

Проведено дослідження шляхом статистичного моделювання можливостей скороченої процедури ймовірнісного консенсусу у двошаровій моделі. Встановлено, що якщо початкова частина ланцюжка хребетних блоків повторилася k разів і за ці блоки проголосували більше половини атестаторів – учасників відповідних слотів, то цей ланцюжок є кандидатом на фіналізацію. Показано, що при k=3 дане впорядкування не зміниться з ймовірністю щонайменше 0,9. В результаті прогноз можливої фіналізації може бути отриманий за 3·4=12 секунд, в той час як очікування повного консенсусу становить 4 хвилини 16 секунд.

Сформульовано третій пункт наукової новизни – вперше розроблений метод прискореного PoS консенсусу в двошаровій моделі розподіленого реєстру на основі k-кратної перевірки повторення початкової частини ланцюжка хребетних блоків і голосування за ці блоки більше половини учасників відповідних слотів, що дозволило зменшити час отримання рішення до декількох секунд із ймовірністю, не меншою 0,9.

У третьому розділі дисертаційної роботи показано, що при формуванні PoS консенсусу квазівипадковим чином у кожному слоті епохи відбувається формування складу комітетів та ролей координаторів у них (утворювач блоків, атестатор, агрегатор). Далі атестатор підписує останній, на його думку, правильний блок у слоті, а агрегатор поєднує результати атестації в один мультіпідписом. При цьому не виключені атаки маніпуляцією як на формування складу комітетів, так і на вибір зі списку координаторів атестатора

або агрегатора. Тому важливим засобом захисту від таких можливих маніпуляцій є розробка методу квазівипадкового перемішування довільної числової множини, що реально гарантує захищеність від подібних маніпуляцій. Розділ присвячений дослідженню можливості застосування у комп'ютерній криптографії найпростіших положень теорії нелінійних дискретних динамічних систем, основною характеристикою яких є хаотичність.

Досліджено можливість побудови якісних функцій перемішування на основі суперпозиції найпростіших лінійних та нелінійних відображень. Для лінійного відображення пропонується використовувати оператор перестановки, а для нелінійного – найбільш просте відображення, класичний q-Tent:

$$f_q(x) = 2\left(q/2 - \left|x - q/2\right|\right) = \begin{cases} 2x, x \le q/2 \\ 2(q-x), x > q/2 \end{cases}, \quad [0,q] \xrightarrow{f_q} [0,q] \ .$$

Проведено кореляційний аналіз побудованих відображень, аналіз їх чутливості, аналіз середніх довжин циклів цих відображень, розглянуто можливості узагальнення алгоритмів побудови функцій перемішування та застосування їх до захисту від маніпуляцій при квазівипадковому виборі. Підтверджено очікувані хороші дифузійні властивості цих функцій перемішування. Досліджена функція перемішування має наступні переваги: відсутність колізій; простота застосовуваних математичних операцій; злом її можливий тільки шляхом повного перебору.

Розроблено метод перемішування даних за допомогою бієктивного відображення, яке є суперпозицією лінійного та найпростішого нелінійного відображення q-Tent. Запропоновані функції перемішуванні дозволили здійснити процес якісного перемішування при формуванні PoS консенсусу, і тим самим захистити процес обробки транзакцій у розподілених реєстрах від можливих маніпуляцій шляхом суттєвого підвищення криптостійкості.

Сформульовано четвертий пункт наукової новизни: отримав подальший розвиток метод перемішування даних за допомогою бієктивного відображення, яке є суперпозицією лінійного та найпростішого нелінійного відображення q-Tent, що дозволило здійснити процес якісного перемішування при формуванні

PoS консенсус.

У четвертому розділі дисертаційної роботи розроблено експериментальну децентралізовану платформу Waterfall.

Розроблена платформа Waterfall успадковує основні принципи Ethereum 2.0 та розвиває їх. Завдяки розробленим моделям та методам платформа збільшує такі показники ефективності:

1. Висока швидкість обробки транзакцій при достатньому рівні масштабованості – масштабовані в системі блокові структури на основі DAG дозволяють одночасно публікувати кілька блоків. Це формує DAG та забезпечує завершеність всіх транзакцій за умови, що блоки не конфліктують один з одним. Тому Waterfall може одночасно обробляти об’єм транзакцій порівняний з тим що оброблюють Visa, MasterCard та UnionPay, але на децентралізованому рівні навіть у години пік. Згідно з останніми проміжними лабораторними тестами, система могла обробляти 3600 транзакцій в секунду. Для порівняння зазначимо, що Visa обробляє близько 1700 транзакцій на секунду.

2. Забезпечується висока захищеність платформи від можливих маніпуляцій при використанні операцій квазівипадкового вибору при здійсненні процедури консенсусу PoS за рахунок застосування розробленого методу перемішування.

Крім того, платформа Waterfall забезпечує наступні переваги, порівняно з аналогічними технічними рішеннями:

1. Низькі комісії за транзакції – архітектура спроектована таким чином, щоб підтримувати мінімальні комісії у різних сценаріях. Протокол динамічно масштабується зі зростанням навантаження на мережу. У той час, як продуктивність всієї системи збільшується, в тому самому слоті одночасно публікується більше блоків, а транзакційні збори знижуються в міру масштабування системи. Це знижує кількість операцій у пулі транзакцій навіть у години пік.

2. Низький фінансовий поріг входу – вузол із 6 Worker'ів коштує

приблизно 1 920 доларів США.

3. Платформа обслуговує вбудовані токени – випуск та обслуговування токенів (включно з NFT) не потребують спеціальних смарт-контрактів, а виконуються за допомогою звичайних транзакцій, що значно знижує накладні витрати. Крім того, це робить їх використання більш доступним для широкого кола користувачів.

4. Динамічні налаштування – платформа має механізми динамічної адаптації параметрів системи залежно від ситуації, що змінюється. зокрема, час слота, оптимальна кількість Worker'ів та деякі інші параметри налаштовуються автоматично.

Таким чином, платформа Waterfall забезпечує сприятливе середовище для надання та споживання широкого спектру послуг із ведення бізнесу та соціальної діяльності у зручному форматі загальнодоступного децентралізованого реєстру. Платформа призначена для обслуговування транзакцій з різними токенами, включаючи NFT, обслуговування смарт-контрактів і розробки розподілених додатків. Тестування системи показало, що вона може обробляти в середньому 2234 транзакції за секунду при досить високому рівні масштабованості.

Таким чином, підтверджено спроможність та правильність технічних рішень, заснованих на результатах дисертаційного дослідження.

Розроблені в роботі методи та інструментальні засоби отримали впровадження у діяльності Комунального підприємства «Теплопостачання міста Одеси» та знайшли відображення у навчальному процесі та науковій діяльності Національного університету «Одеська політехніка».

Ключові слова: розподілені системи, бази даних, технологія децентралізованих реєстрів, методи обробки інформації, операції з транзакціями, криптозахищеність, масштабованість, блокчейн-технології.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Grybniak S., Dmitrishin D. Basic principles for constructing mixing functions based on the simplest linear and nonlinear mappings. Proceedings of Odessa Polytechnic University. 2022. № 2(66). P. 100–109. DOI: 10.15276/opu.2.66.2022.12. (Реєстр наукових фахових видань України, категорія «Б»)

2. Mazurok I., Leonchyk Y., Grybniak S., Nashyvan O., Masalskyi R. AnincentivesystemfordecentralizedDAG-basedplatforms. *AppliedAspectsofInformationTechnology*. 2022. Vol. 5, № 3. P. 196–207. DOI: https://doi.org/10.15276/aait.05.2022.13. (Реєстр наукових фахових видань України, категорія «Б»)

3. Mazurok I., LeonchykY., GrybniakS., VorokhtaA., Nashyvan O. Multi-objective optimization of committee selection for hierarchical byzantine fault tolerance-based consensus protocols.*HeraldofAdvancedInformationTechnology*. 2023. Vol. 6, № 1. P. 39–53. DOI: https://doi.org/10.15276/hait.06.2023.3. (Реєстр наукових фахових видань України, категорія «Б»)

4. Грибняк С. С. Двошарова модель масштабуємого розподіленого децентралізованого реєстру. *Наукові праці Вінницького національного технічного університету*. 2023. № 2. С. 120–127. (Реєстр наукових фахових виданьУкраїни, категорія «Б»)

5. Грибняк С. С. Розробка платформи децентралізованого реєстру з покращеними характеристиками. Інформатика та математичні методи в моделюванні.2023. Т.13, №1-2, С.48–55.DOI: 10.15276/imms.v13.no1-2.48. (Реєстр наукових фахових виданьУкраїни, категорія «Б»).

Наукові праці, які засвідчують апробацію матеріалів дисертації:

6. Decentralized platforms: Goals, challenges, and solutions / S. Grybniak, Y. Leonchyk, R. Masalskyi, I. Mazurok, O. Nashyvan, R. Shanin.*2022 IEEE 7th Forum*

on Research and Technologies for Society and Industry Innovation (RTSI).24-26 August 2022. Paris, France. 2022. P. 62–67. DOI: https://doi.org/10.1109/RTSI55261.2022.9905225. Decentralized platforms express.pdf. (Indexed in SCOPUS)

7. Waterfall: A Scalable Distributed Ledger Technology / S. Grybniak, D. Dmytryshyn, Y. Leonchyk, I. Mazurok, O. Nashyvan, R. Shanin. In 2022 IEEE 1st Global Emerging Technology Blockchain Forum*: Blockchain & Beyond(iGETblockchain)*. November 2022. Irvine, CA, USA. 2022. P. 1–6. DOI: https://doi.org/10.1109/iGETblockchain56591.2022.10087112. Scalable Distributed Ledger express.pdf. (Indexed in SCOPUS)

8. Subnetworks in BlockDAG / O. Antonenko, S. Grybniak, D. Guzey, O. Nashyvan and R. Shanin. 2022 IEEE 1st Global Emerging Technology *Blockchain Forum: Blockchain& Beyond (iGETblockchain)*. November 2022. Irvine, CA, USA. 2022. P. 1–6. DOI: https://doi.org/10.1109/iGETblockchain56591.2022.10087101. Subnet works in BlockDAG (Final Version).pdf

9. Waterfall: Salto Collazo. Tokenomics / S. Grybniak, Y. Leonchyk, R. Masalskyi, I. Mazurok O. Nashyvan. 2022 IEEE International Conference on Blockchain, *Smart Healthcare and Emerging Technologies (SmartBlock4Health)*. 24-25 October 2022. Bucharest, Romania. 2022. P. 1-6. DOI: https://doi.org/10.1109/SmartBlock4Health56071.2022.10034521. Waterfall-Salto-Collazo express.pdf. (Indexed in SCOPUS)

10. Recurring Payments on EVM-based Platforms / S. Grybniak, N. Goga, O. Nashyvan, R. Mihai, I. Mazurok, Y. Leonchyk, G. Datta, O. F. Ozkul, C. V. Marian. 2022 IEEE 1st Global Emerging Technology Blockchain Forum: *Blockchain& Beyond (iGETblockchain)*. 07-11 November 2022. Irvine, CA, USA. 2022. P. 1–6. DOI: https://doi.org/10.1109/iGETblockchain56591.2022.10087077. Recurring Payments express.pdf. (Indexed in SCOPUS)

11. Blockchain-Enabled Economic Transactions: Recurring Financial Accruals and Payments / R. Mihai, O.F. Ozkul, G. Datta, S. Grybniak, C.V. Marian. 2022 IEEE 1st Global Emerging Technology Blockchain Forum: *Blockchain and Beyond,*

(iGETblockchain). 07-11 November 2022. Irvine, CA, USA. 2022.DOI: 10.1109/iGETblockchain56591.2022.10087074. (Indexed in SCOPUS)

12. Waterfall: Gozalandia. Distributed Protocol with Fast Finality and Proven Safety and Liveness / S. Grybniak, Y. Leonchyk, I. Mazurok, O. Nashyvan, R. Shanin. *IET Blockchain*. 2023. P. 1–12. DOI: https://doi.org/10.1049/blc2.12023.

13. Simulation Modelling of the Consensus Based on the Gozalandia / A. Vorokhta, I. Mazurok, Y. Leonchyk, S. Grybniak, and Y. Strakhov. *Adaptive Learning Management Technologies*. Kyiv. 2022. P. 31–33.

14. An Incentive System for Decentralized DAG-based Platforms / S. Grybniak, Y. Leonchyk, R. Masalskyi, I. Mazurok, O. Nashyvan. *IEEE Blockchain, Tech Breif*. 2022. URL: https://blockchain.ieee.org/images/files/pdf/techbriefs-2022-q4/an-incentive-system-for-decentralized-dag-based-platforms.pdf.

ABSTRACT

Grybniak S.S. Models and Methods for Improving Transaction Processing Efficiency in Distributed Ledgers. – Qualification scientific work in the form of manuscript.

Thesis for the Degree of Doctor of Philosophy in Computer Science, Specialization 122 – Computer Science. – Odessa Polytechnic National University, Ministry of Education and Science of Ukraine, Odesa, 2023.

The **introduction** shows the relevance and characteristics of Distributed Ledger Technology (DLT) based on blockchain. This technology is becoming increasingly popular due to its secure and transparent transactions, as well as its elimination of intermediaries and central governing authorities. Despite the growing demand for applications and research efforts in the field of DLT, its widespread adoption is hindered by the low efficiency of existing solutions. Therefore, enhancing the efficiency of applied solutions remains a proper scientific and technical challenge, to which this research is dedicated.The object, subject, tasks, and methods of the research have been defined. The scientific novelty and practical significance of the obtained results have been presented. The researcher's contribution has also been highlighted.

In the **first section** of the dissertation, an analysis of existing DLT technologies is conducted, identifying their advantages and disadvantages. It is demonstrated that well-known systems built on DLT suffer from several significant drawbacks. A distributed system should have a scalability mechanism to adapt to changing workloads within wide boundaries. However, the data processing speed in popular systems like Bitcoin and Ethereum is slow, processing approximately 7 and 15 transactions per second (tps) first one and up to 119 tps the second one, respectively. These figures are incomparable to traditional centralized systems, which can handle thousands of transactions per second.

There exist scientific and practical challenges to enhancing the efficiency of transaction processing in distributed ledgers, which requires combining high

transaction processing speeds, system scalability, and sufficient crypto security to prevent manipulations and attacks. The proposed ways to improve the efficiency of transaction processing and scalability of the distributed ledger are based on a two-layer model of the distributed ledger.

In the **second section** of the dissertation work, ways to improve the efficiency of transaction processing and scalability of the distributed ledger are investigated.

To accelerate transaction processing with high scalability, a two-layer model for the system is proposed (Fig. 1).

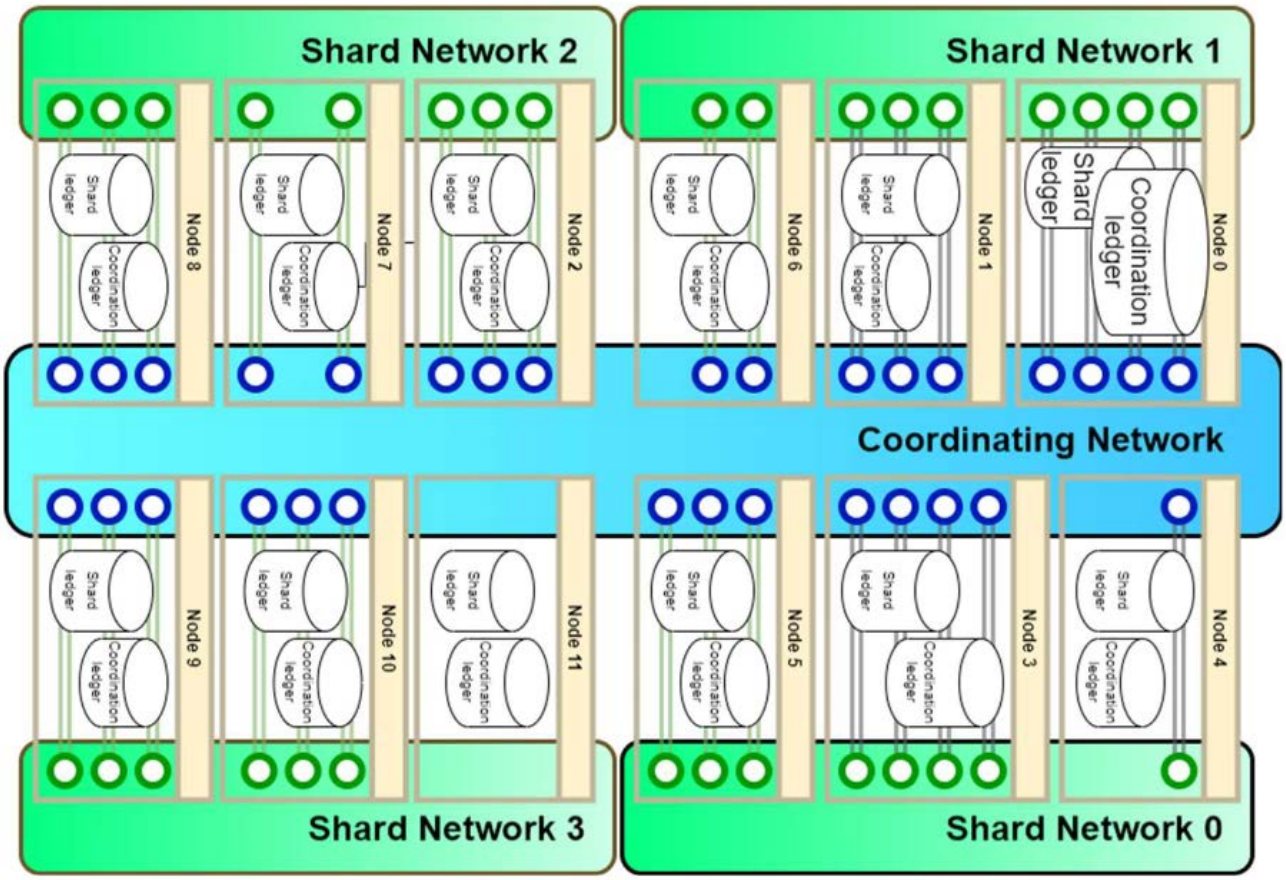

Fig. 1. Two-layer model of a distributed ledger

The main network is responsible for block formation and propagation, implemented using the BlockDAG technology (Layer 1). Operations related to block verification based on the consensus protocol are delegated to the coordination network, which operates using traditional consensus technology (Layer 2). According to the proposed model, all nodes in the system, called Workers, take on two roles – Block Producers in the main network and Coordinators in the coordination network.

With this approach, the functions of the network layers are separated. In the main network, block formation and propagation functions are executed, which require operations involving long blocks. Building the main network using BlockDAG technology significantly accelerates the process of pre-processing transactions due to asynchronous block formation. In the coordination network, operations related to forming consensus according to the Proof of Stake protocol are performed, which demand a large number of short message transmissions. Therefore, the operation of the coordination network is organized according to a traditional blockchain protocol, which is simpler than BlockDAG.

The first point of scientific novelty is formulated as follows: for the first time a two-layer model of a distributed ledger has been developed, which combines a main network built using BlockDAG technology and a coordination network based on traditional blockchain technology. This allows for an increased transaction processing speed while significantly scaling the system.

The concept of a “slot skeletal block” is introduced. A skeletal block is a slot block with the following properties:

1) It has the highest height,

2) If there are multiple such blocks, the one that references a larger number of previous blocks is chosen,

3) If there are multiple such blocks, the one with a lower hash value resulting from the mixing function is selected.

Since each block stores a Merkle tree, the skeletal block in fact stores in a “compressed” form all the “past” blocks of the same slot. Based on this, a model of efficient information exchange between the main network and the coordination network is built, reducing overall information overhead on the system and increasing transaction processing speed. A methodology for applying BlockDAG network information exchange with the coordination network is developed, based on the skeletal block model.

The second point of scientific novelty is formulated as follows: the model of efficient information exchange between the BlockDAG network and the coordination

network is further developed based on the concept of a skeletal block. This development leads to a reduction in the volume of traffic between the BlockDAG network and the coordination network, thereby decreasing the overall system load and increasing transaction processing speed.

Based on the two proposed models, a coordinated sequence of operations has been formulated in the main and coordination networks.

The research was conducted through statistical modeling of the possibilities of a shortened procedure for probabilistic consensus in a two-layer model. It has been established that if the initial part of the chain of skeletal blocks is repeated k times, and if more than half the attesters – participants of the corresponding slots – vote for these blocks, then this chain becomes a candidate for finalization. It has been shown that when $k = 3$, this ordering will not change with a probability of at least 0.9. As a result, a forecast of possible finalization can be obtained in $3 \cdot 4 = 12$ seconds, while the expected time for full consensus is 4 minutes and 16 seconds.

The third point of scientific novelty is formulated as follows: the first was developed as a method of accelerated PoS consensus in a two-layer model of a distributed ledger, based on k-fold verification of the initial part of the chain of skeletal blocks, and voting by more than half of the participants in the corresponding slots for those blocks. This allows for the time to obtain a decision to be reduced to just a few seconds, with a probability of at least 0.9.

In the **third section** of the dissertation, it is shown that in the formation of the PoS consensus, the composition of committees and coordinator roles (block proposer, attester, aggregator) is quasi-randomly determined in each epoch slot. Next, the attester signs the last valid (according to their judgment) block in the aggregator slot, combining the attestation results with a single signature. However, attacks on both the formation of committee compositions and the selection of coordinators as attesters and aggregators cannot be ruled out. Therefore, an important means of protection against such potential manipulations is the development of a method for quasi-random shuffling of an arbitrary numerical set, which can effectively guarantee protection against such manipulations. This chapter is dedicated to investigating the

possibility of applying the simplest principles of nonlinear discrete dynamic systems theory, characterized by chaos, in computer cryptography.

Research on the possibility of constructing qualitative mixing functions based on the superposition of the simplest linear and nonlinear transformations is investigated. As a linear transformation, the permutation operator is proposed to be used, and as a nonlinear transformation, the simplest classical q-Tent mapping is suggested:

$$f_q(x) = 2\left(q/2 - \left|x - q/2\right|\right) = \begin{cases} 2x, x \le q/2 \\ 2(q-x), x > q/2 \end{cases}, \quad [0,q] \xrightarrow{f_q} [0,q] \ .$$

Correlation analysis of the constructed mappings, sensitivity analysis, and analysis of the average cycle lengths of these mappings are conducted. The possibility of generalizing the algorithms for constructing mixing functions and their application for protection against manipulations in quasi-random selection is explored. The expected good diffusion properties of these mixing functions are confirmed. The investigated mixing function has the following advantages: absence of collisions; simplicity of the applied mathematical operations; its breaking is only possible through complete overrun.

A data mixing method using bijective mapping has been developed, which is a superposition of a linear and the simplest nonlinear mapping q-Tent. This method enables the process of qualitative mixing during the formation of PoS consensus, thereby protecting transaction processing in distributed ledgers from possible manipulations by significantly enhancing crypto security.

The fourth point of scientific novelty is formulated as follows: the data mixing method using a bijective mapping, which is a superposition of a linear and the simplest nonlinear q-Tent mapping, receives further development, enabling the process of qualitative shuffle during the formation of the PoS consensus.

In the **fourth section** of the dissertation, an experimental decentralized platform called "Waterfall" has been developed. The developed Waterfall platform inherits the main principles of Ethereum 2.0 and further expands them. Thanks to the developed models and methods, the platform increases the following efficiency indicators:

1. High transaction processing speed with sufficient scalability – Waterfall achieves scalability through block structures based on a directed acyclic graph (DAG). This allows multiple blocks to be published simultaneously, forming a DAG and ensuring the completion of all transactions, as long as the blocks do not conflict with each other. As a result, Waterfall can handle Visa, MasterCard, and Union Pay transactions simultaneously on a decentralized level, even during peak hours. According to recent intermediate laboratory tests, the system was able to process 3600 transactions per second. For comparison, Visa processes approximately 1700 transactions per second.

2. The platform ensures high security against potential manipulations by using operations of quasi-random selection during the Proof of Stake (PoS) consensus procedure, achieved through the application of the developed shuffling method.

In addition to the afore-mentioned advantages, the Waterfall platform provides the following benefits compared to similar technical solutions:

1. Low transaction fees – The architecture is designed to maintain minimal fees across various scenarios. The protocol dynamically scales with an increasing network load. As the overall system's performance improves, more blocks are simultaneously published in the same slot, leading to reduced transaction fees as the system scales. This reduces the number of operations in the transaction pool, even during peak hours.

2. Low financial entry barrier – A node with 6 Workers costs approximately 1,920 US dollars.

3. The platform serves built-in tokens – output and servicing tokens (including NFTs) do not require special smart contracts but are executed through regular transactions, significantly reducing overhead costs. Additionally, this makes their usage more accessible to a wide range of users.

4. Dynamic configuration – The platform incorporates mechanisms for dynamically adapting system parameters based on changing situations, such as the slot time, optimal number of Workers, and certain other parameters that are automatically adjusted as needed.

Thus, the Waterfall platform provides a favorable environment for the provision and consumption of a wide range of services in business and social activities through the convenient format of a publicly accessible decentralized ledger. The platform is designed to support transactions with various tokens, including NFTs, servicing smart contracts, and developing distributed applications. System testing has shown that Waterfall can process an average of 2.234 transactions per second at a high enough level of scalability.

As a result, the capability and correctness of the technical solutions based on the findings of the dissertation research have been confirmed.

The developed methods and tools in the research have been implemented in the activities of the Municipal enterprise “Heat supply of the city of Odesa” (Odesa) They have also been incorporated into the educational process and scientific activities of the National University "Odessa Polytechnic".

Key Words: distributed systems, databases, distributed ledger technology, information processing methods, transaction processing, crypto-security, scalability, blockchain technologies.

LIST OF PUBLISHED PAPERS ON THE TOPICS OF THE DISSERTATION

Papers in which the main scientific results of the dissertation are published:

1. Grybniak, S., & Dmitrishin, D. (2022). Basic principles for constructing mixing functions based on the simplest linear and nonlinear mappings. *Proceedings of Odessa Polytechnic University,* 2(66), 100–109. DOI: 10.15276/opu.2.66.2022.12. (Register of scientific and professional publications of Ukraine, category "B")

2. Mazurok, I., Leonchyk, Y., Grybniak, S., Nashyvan, O., & Masalskyi, R. (2022).AnincentivesystemfordecentralizedDAG-basedplatforms. *AppliedAspectsofInformationTechnology,* 5, 3, 196–207. DOI: https://doi.org/10.15276/aait.05.2022.13. (Register of scientific and professional publications of Ukraine, category "B")

3. Mazurok, I., Leonchyk,Y., Grybniak,S., Vorokhta,A., & Nashyvan, O. (2023). Multi-objective optimization of committee selection for hierarchical byzantine fault tolerance-based consensus protocols.*HeraldofAdvancedInformationTechnology*, 6, 1, 39–53. DOI: https://doi.org/10.15276/hait.06.2023.3. (Register of scientific and professional publications of Ukraine, category "B")

4. Grybniak, S.S. (2023). Two-layer model of scalable distributed decentralized registry. *Scientific works of Vinnytsia National Technical University*, 2, 120–127. (Register of scientific and professional publications of Ukraine, category "B")

5. Grybniak,S.S. (2023). Development of a decentralized registry platform with improved characteristics. *Informatics and Mathematical Methods in Simulation,* 13, 1-2, 48–55. DOI: 10.15276/imms.v13.no1-2.48. (Register of scientific and professional publications of Ukraine, category "B").

Papers certifying the approbation of the dissertation materials:

6. Grybniak, S.,Leonchyk, Y.,Masalskyi, R.,Mazurok, I.,Nashyvan, O.,& Shanin, R. (2022).Decentralized platforms: Goals, challenges, and solutions. *2022 IEEE 7th Forum on Research and Technologies for Society and Industry Innovation*

(RTSI),24-26 August 2022, Paris, France, 62–67. DOI: https://doi.org/10.1109/RTSI55261.2022.9905225. Decentralized platforms express.pdf. (Indexed in SCOPUS)

7. Grybniak, S., Dmytryshyn, D., Leonchyk, Y., Mazurok, I., Nashyvan, O., & Shanin, R. (2022). Waterfall: A Scalable Distributed Ledger Technology. *In 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain),* November 2022, Irvine, CA, USA, 1–6. DOI: https://doi.org/10.1109/iGETblockchain56591.2022.10087112. Scalable Distributed Ledger express.pdf. (Indexed in SCOPUS)

8. Antonenko, O., Grybniak, S., Guzey, D., Nashyvan, O., & Shanin, R. (2022). Subnetworks in BlockDAG. *2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain& Beyond (iGETblockchain),* November 2022, Irvine, CA, USA, 1–6. DOI: https://doi.org/10.1109/iGETblockchain56591.2022.10087101. Subnet works in BlockDAG (Final Version).pdf

9. Grybniak, S., Leonchyk, Y., Masalskyi, R., Mazurok, I., & Nashyvan, O. (2022). Waterfall: Salto Collazo. Tokenomics. *2022 IEEE International Conference on Blockchain, Smart Healthcare and Emerging Technologies (SmartBlock4Health),*24-25 October 2022, Bucharest, Romania, 1–6. DOI: https://doi.org/10.1109/SmartBlock4Health56071.2022.10034521. Waterfall-Salto-Collazo express.pdf. (Indexed in SCOPUS)

10. Grybniak, S., Goga, N., Nashyvan, O., Mihai, R., Mazurok, I., Leonchyk, Y., Datta, G., Ozkul, O. F., & Marian, C. V. (2022). Recurring Payments on EVM-based Platforms. *2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain& Beyond (iGETblockchain)*, 07-11 November 2022, Irvine, CA, USA, 1–6. DOI: https://doi.org/10.1109/iGETblockchain56591.2022.10087077. Recurring Payments express.pdf. (Indexed in SCOPUS)

11. Mihai, R., Ozkul, O.F., Datta, G., Grybniak, S., &Marian, C.V. (2022).Blockchain-Enabled Economic Transactions: Recurring Financial Accruals and Payments. *2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain and Beyond, (iGETblockchain),* 07-11 November 2022, Irvine, CA, USA.

DOI: 10.1109/iGETblockchain56591.2022.10087074. (Indexed in SCOPUS)

12. Grybniak, S., Leonchyk, Y., Mazurok, I., Nashyvan, O., & Shanin, R. (2023). Waterfall: Gozalandia. Distributed Protocol with Fast Finality and Proven Safety and Liveness. *IET Blockchain*, 1–12. DOI: https://doi.org/10.1049/blc2.12023.

13. Vorokhta, A., Mazurok, I., Leonchyk, Y., Grybniak, S., & Strakhov, Y. (2022). Simulation Modelling of the Consensus Based on the Gozalandia. *Adaptive Learning Management Technologies*, Kyiv, 31–33.

14. Grybniak, S., Leonchyk, Y., Masalskyi, R., Mazurok, I., Nashyvan, O. (2022). An Incentive System for Decentralized DAG-based Platforms. *IEEE Blockchain, Tech Breif.* URL: https://blockchain.ieee.org/images/files/pdf/techbriefs-2022-q4/an-incentive-system-for-decentralized-dag-based-platforms.pdf.