МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені І.І.МЕЧНИКОВА

(повне найменування вищого навчального закладу)

Факультет математики, фізики та інформаційних технологій

(повне найменування інституту, назва факультету (відділення))

Кафедра математичного забезпечення комп'ютерних систем

(повна назва кафедри (предметної, циклової комісії))

# Кваліфікаційна робота

на здобуття ступеня вищої освіти «магістр»

(освітньо-кваліфікаційний рівень)

на тему «Методи масштабування Блокчейн технологій»
«Blockchain technologies scalability methods»

Виконав: студент денної форми навчання
спеціальності 123 – Комп'ютерна інженерія
(шифр і назва напряму підготовки, спеціальності)
Гузей Денис Едуардович
(шифр і назва напряму підготовки, спеціальності)
Керівник к.ф.-м.н., доц. Антоненко О.С.
(науковий ступінь, вчене звання, прізвище та ініціали, підпис)
Рецензент к.ф.-м.н., доц. Петрушина Т.І.
(науковий ступінь, вчене звання, прізвище та ініціали)
Рецензент
(науковий ступінь, вчене звання, прізвище та ініціали)

Рекомендовано до захисту:
Протокол засідання кафедри
№___ від «___»_____ 2022 р.

Завідувач кафедри
_____ Є.В. Малахов
(підпис) (прізвище, ініціали)

Захищено на засіданні ЕК № ___
протокол № __ від «___» _____ 2022 р.
Оцінка _____/_____/_____
(за національною шкалою, шкалою ECTS, бали)

Голова ЕК
_____ _____
(підпис) (прізвище, ініціали)

Одеса – 2022

# АНОТАЦІЯ

У дипломній роботі розглядається тема «методи масштабування Блокчейн технологій».

Блокчейн технології набули великого розповсюдження. Основною галузю застосування цих технологій є фінансова галузь, проте вона також використовується в ігровій індустрії та IoT. Дані технології є децентралізованими, а також досить суттєво захищеними від внесення недійсної та підміни інформації, що дає більше впевненості у безпеці інформації на відміну від централізованих систем. Проте такі системи не зважаючи на їх переваги мають значний недолік, а саме невелику швидкість обробки транзакцій. Задля усунення цього недоліку використовуються різні методи масштабування, які мають свої переваги та недоліки.

Метою роботи є вдосконалення існуючих методів масштабування Блокчейн технологій.

В результаті проведених в роботі досліджень розглянуто методи усі популярні методи масштабування Блокчейн технологій, а також запропоновано використання ієрархічних дивізійних та агломеративних алгоритмів для реалізації побудови підмереж. Крім цього в роботі проведено моделювання різних методів та проведено їх аналіз.

У роботі сформовано ряд вимог до бібліотеки класів, яку можна використовувати у Блокчейн системах, а також для модельної системи, яка дозволила провести моделювання розглянутих методів. Обидві системи було реалізовано.

Використовуючи ієрархічні алгоритми для побудови підмереж у Блокчейн системах за допомогою критерія у агломеративних алгоритмах вдалось досягти прийнятної для практичних цілей кластеризації, дотримуючись умови, що підмережі за кількістю валідаторів будуть відрізнятися одна від одної менше ніж в два рази. У дивізійних алгоритмах розподілення мережі на підмережі вдалося досягти більш якісних результатів

кластеризації, а ще ряд дивізійних, які використовують алгоритми глобального пошуку найвіддаленіших вузлів, хоча і проявили себе як досить якісні, проте швидкість їх виконання досить слабка, тому вони не можуть бути використані в системах, де швидкість дуже критична, а також у системах, з малими розрахунковими потужностями. Дивізійні методи, які використовують алгоритми подвійного пошуку виконуються набагато швидше, але за якістю майже не поступаються тим, що базуються на алгоритмах глобального пошуку, тому їх можна використовувати в більшості випадкі.

# ABSTRACT

The topic of "Blockchain technology scaling methods" is considered in the thesis.

Blockchain technologies have become widespread. The main application of these technologies is the financial industry, but it is also used in the gaming industry and IoT. These technologies are decentralized, as well as quite significantly protected against entering invalid and changing information, which gives more confidence in the security of information, unlike centralized systems. However, despite their advantages, such systems have a significant drawback, namely the low speed of transaction processing. To overcome this drawback, various scaling methods are used, which have their own advantages and disadvantages.

The purpose of the work is to improve existing methods of scaling Blockchain technologies.

As a result of the research carried out in the work, all popular methods of scaling Blockchain technologies were considered, and the use of hierarchical divisional and agglomerative algorithms for the implementation of the construction of subnetworks was also proposed. In addition, the work carried out modeling of various methods and their analysis.

In the work, a number of requirements for the class library, which can be used in Blockchain systems, as well as for the model system, which made it possible to simulate the considered methods, were formed. Both systems were implemented.

Using hierarchical algorithms for building subnets in Blockchain systems with the help of a criterion in agglomerative algorithms, it was possible to achieve acceptable clustering for practical purposes, observing the condition that the subnets will differ from each other by less than two times in terms of the number of validators. In the divisional algorithms for dividing the network into subnets, it was possible to achieve higher quality clustering results, and a number of

divisional algorithms that use algorithms for the global search of the most distant nodes, although they proved to be quite high-quality, but their execution speed is quite weak, so they cannot be used in systems , where speed is very critical, as well as in systems with low computing power. Divisional methods that use double search algorithms are performed much faster, but the quality is almost not inferior to those based on global search algorithms, so they can be used in most cases.

**ЗМІСТ**

# ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ І ТЕРМІНІВ

PoW – алгоритм консенсусу Proof of Work

PoS – алгоритм консенсусу Proof of Stake

PoA – алгоритм консенсусу Proof of Authority

Леджер – бухгалтерська книга, історія фіналізованих транзакцій у Блокчейні

Tps – важливий показник, що визначає кількість оброблених транзакцій системою за секунду часу.

Розбиття мережі на підмережі/Кластеризація/Побудова топології мережі – процес, в результаті якого вузли отримають дані про те в якій підмережі вони будуть знаходитися в наступному раунді кластеризації.

Транзакція – це послідовність операцій, що виконується як одна одиниця роботи.

Блок – це базова складова Блокчейну, яка складається з транзакцій та має свій унікальних ідентифікатор, що генерується за допомогою хеш-суми.

Блокчейн/Blockchain – леджер, база даних або набір транзакцій, що представлені у вигляді пов’язаних блоків, дані в якому не змінні, зв’язок між якими криптографічно захищени.

ДАГ/DAG – ациклічний направлений граф, тобто направлений граф, який не має циклів.

Блок-ДАГ/Block-DAG – Блокчейнподібна система, яка має замість ланцюжку блоків використовує DAG подібну систему.

Пул транзакцій – місце де зберігаються транзакції від моменту їх публікації до потрапляння у блок.

Мемпул/mempool – назва пулу транзакцій, який використовується у Біткоїні та похідних від нього системах.

Транзакшнпул/transactionpool – назва пулу транзакцій, який використовується у Етеріумі та похідних від нього системах.

# ВСТУП

Технологія Блокчейн стала відома широкій публіці завдяки Сатоші Накомото, невідомому розробнику, орієнтовно китайського походження, що заснував найвідомішу криптовалюту Bitcoin. І хоча для загалу технологія Блокчейн та криптовалюта це тотожні поняття, проте криптовалюта – це лише один із аспектів даної технології. Найважливіший аспект Блокчейну – це нова віха розподіленого реєстру, що створила нові можливості для Інтернету. Завдяки цьому іноді в літературі, коли йдеться про Блокчейну, зустрічається таке поняття як Web 3.0. Може виникнути питання, що ж такого особливого в цій технології? Відповідь на це питання наступна – це розподілений реєстр, який одночасно є децентралізованим та захищеним.

Децентралізованість ґрунтується на тому, що весь реєстр зберігається одночасно на усіх вузлах мережі, а зміни внесені на одному з вузлів розсилаються лавинним шляхом на усі інші вузли. На відміну від звичайних розподілених систем тут не має декількох центральних вузлів, що виконують роль серверів, а інші вузли – роль клієнтів, в такій мережі усі вузли одночасно виконують роль і серверів, і клієнтів. Це дозволяє уникнути атаки захоплення серверних вузлів, бо для реалізації такої атаки необхідно захопити щонайменш половину усіх вузлів мережі.

Проте у класичному представленні така система дуже не надійна тому, що не стійка до атаки «Людина посередині». Саме тому для уникнення такого роду атаки в технології Блокчейн і реалізовано захист за допомогою ЄЦП, що унеможливлює підміну зловмисником інформації, що вніс певний вузол у реєстр. Крім того для захисту інформації використовується ланцюжок блоків, що посилаються один на одного (наступний на попередній), при чому усі блоки зберігаються на всіх вузлах мережі. Реалізовано це наступним чином: Існує Перший блок G, в цей блок записується певна інформація доти поки об’єм цієї інформації не почне перевищувати порогове значення. Після чого розраховується контрольна

сума цього блоку на основі контрольної суми інформації, що записана у ньому, його ідентифікатора та хеш-суми попереднього вузла (так як блок є першим і він не посилається ні на який блок, то значення хеш-суми пусте, чи записане нулями, що тотожно), після чого змінити інформацію в цьому блоці не можливо, а нова інформація записується у новий блок, який має свій ідентифікатор, та який посилається на перший блок, далі інформація записується аналогічним чином, а вже потім блок також фіналізується та підписується хеш-сумою. І так до безкінечності.

Ця система досить надійна, хоча і є певні недоліки. Першим недоліком є великий об’єм ланцюжка блоків, який на момент серпня 2022 року складає більше аніж 414 Гігабайт і це значення безперервно зростає, в наслідок чого для того, щоб приймати участь у генерації блоків, необхідно мати накопичувач об’ємом більшим за це значення. Другий недолік випливає з концепції системи захисту мережі від підміни блоків. Яка ґрунтується на тому, що певний блок можливо підмінити лише за умови, якщо є повністю перерахована хеш-сума ланцюжка блоків, що посилаються на цільовий блок і для того, щоб позбавити зловмисників можливості легкої підміни блоків, в блоки інтегровано деяке числове значення, яке майнер повинен вгадати шляхом перебору для того, щоб сформувати валідний блок. Це значення вгадати дуже складно і складність такого розрахунку зростає пропорційно до розвитку комп’ютерної техніки. А чим вище розрахункова потужність, тим більше необхідно витрачати енергії на розрахунки. Тобто другим недоліком є велика затрата енергії на генерацію блоків, тобто на підтримку життєдіяльності системи. Враховуючи факт значної складності розрахунків, а також обмеження у вигляді максимального об’єму блоку виходить ще один недолік – невелика кількість транзакцій за певний проміжок часу.

Для уникнення цих недоліків існує багато методів масштабування блокчейн-мереж, кожна з них має свої переваги та недоліки. Саме тому метою даного дослідження є вдосконалення існуючих методів

масштабування Блокчейн систем та оптимальне їх поєднання для підвищення їх пропускної спроможності.

Об’єкт дослідження – технологія Блокчейн.

Предмет дослідження – алгоритми, методи та підходи масштабування блокчейн-мереж.

Для досягнення мети треба виконати наступні задачі:

– огляд алгоритмів, методів та підходів до масштабування блокчейн-мереж;

– аналіз ефективності популярних методів;

– огляд можливостей поєднання цих методів;

– перевірка можливості перенесення методів масштабування із інших областей комп’ютерних наук

– запропонувати нові підходи до масштабування блокчейн-мережі;

– промоделювати запропоновані методи;

– зробити аналіз запропонованих методів, ґрунтуючись на дані, отримані з розробленої моделі.

# ВИСНОВКИ

Під час виконання даної роботи було проаналізовано більшість існуючих методів, що дозволяють масштабувати Блокчейн технології. Також були зібрані усі відомі класифікації цих методів. Зважаючи той факт, що усі відомі методи зазвичай діють при різних умовах та в різних площинах, а також те що поточна робота пов'язана з проектом Waterfall було запропоновано новий метод горизонтального масштабування, який буде діяти сумісно з алгоритмом консенсусу PoS та Block-DAG системою. В процесі виконання роботи було запропоновано метод розподілення усієї мережі на підмережі, використовуючи ієрархічні алгоритми кластеризації – агломеративні та дивізійні.

Резюмуючи поточну роботу можна зробити висновки, що запропонований у поточній роботі та у статті [66], що з нею пов'язана є інноваційним рішенням поставленої задачі, тобто робота відповідає критерію наукової новизни.

Також в процесі виконання роботи було розроблено бібліотеку, яку можна підключати до Block-DAG проекту, клієнти якого написані на мові програмування C#. Ця бібліотека містить все необхідне для виконання задачі розділення мережі на підмережі. Крім того було розроблено модельну систему, яка дозволяє проаналізувати ефективність кожного розробленого методу. А також декілька малих супутніх проектів, що дозволяють генерувати віртуальні набори даних, а також спрощують читання коду та роблять архітектуру модельного проекту більш зрозумілою.

В ході роботи було проаналізовано усі методи ієрархічної кластеризації та зроблено висновки про те які з методів є найефективнішими. З точки зору якості результатів найкраще проявили себе дивізійні методи, найкращі результати надали алгоритми де найвіддаленіші вузли знаходилися серед усіх вузлів, проте вони були найповільнішими. Серед агломеративних алгоритмів краще за все проявили себе алгоритми із рорахунком відстаней за

найближчими вузлами. Дивізійні алгоритми проявили себе більш ефективно зі сторони якості кластеризації, при чому алгоритми з дивізійні алгоритми з використанням двійного обходу пошуку найвіддаленіших виявилися більш швидкими.

Результат роботи дозволяє значно підвищити головний показник в контексті масштабування Блокчейн технологій, а саме tps. І хоча без реальних даних роботи мережі отримати конкретні цифри не можливо, проте можна сказати заздалегідь, що завдяки тому, що транзакції не дублюються у різних підмережах, а також те, що транзакція розсилається лише в межах однієї підмережі цей показник виросте пропорційно тому на скільки підмереж буде розподілена мережа.

Таке підвищення результатів дозволить інтегрувати Блокчейн системи в галузь IoT, у галузь військових та медичних досліджень, а також у інші вузькі галузі, в яких звичайний Блокчейн не може використовуватися з-за поганої масштабованості.

У наступних роботах планується зробити перевірку надійність цих метоів з боку безпеки, перевірити їх стійкість при різних родах атак та кількості атакуючих. Перевірка планується зі сторони стійкості алгоритмів до атак, під атаками мається на увазі публікація вузлами не правдивих даних стосовно відстаней. Крім того планується запропонувати метод, який дозволить захиститися від такого роду атак.

Також у наступних роботах планується промоделювати метод самоорганізації вузлів у кластери, який було розглянуто у поточній статті, та який не увійшов до неї так як він не підходить до систем, що використовують алгоритм консенсусу PoS, якою і є проект Waterfall. Проте цей метод може підійти до систем, що використовують алгоритм консенсусу PoW.

Також у наступних роботах планується зробити опис роботи реальної системи, що буде розгорнута та використовуватиме запропонований у поточній статті методи.

# ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Haber Stuart, How To Time-Stamp a Digital Document / Stuart Haber and W. Scott Stornetta // Journal of Cryptology, Vol. 3, No. 2, 1991. – PP. 99-111.

2. Cynthia Dwork, Pricing via Processing or Combatting Junk Mail / Cynthia Dwork, Moni Naor // Brickell, E.F. (eds) Advances in Cryptology – CRYPTO' 92. CRYPTO 1992. – PP.139-147.

3. Hashcash. Hashcash.org [Електронний ресурс] – Режим доступу: http://www.hashcash.org/

4. Markus Jakobsson, Proofs of work and bread pudding protocols (extended abstract)/ Markus Jakobsson, Ari Juels// Part of the IFIP — The International Federation for Information Processing book series. September, 1999. – PP. 15. – Access mode: http://www.arijuels.com/wp-content/uploads/2013/09/PoW.pdf

5. RPOW - Reusable Proofs of Work. Cryptome. [Електронний ресурс] – Режим доступу: https://cryptome.org/rpow.htm

6. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. – 2008. – PP. 9. – Access Mode: https://bitcoin.org/bitcoin.pdf

7. Ethereum. ethereum.org. [Електронний ресурс] – Режим доступу: https://ethereum.org/en/

8. Ethereum Whitepaper. ethereum.org. – PP. 36. – Access Mode: https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf

9. Ethereum virtual machine (evm). ethereum.org. [Електронний ресурс] – Режим доступу: https://ethereum.org/en/developers/docs/evm/

10. A. M. Turing, On computable numbers, with an application to the entscheidungsproblem // Proceedings of the London Mathematical Society. January 01, 1937. – PP. 230-265. – Access Mode: https://www.cs.virginia.edu/~robins/Turing_Paper_1936.pdf

11. Повний по Тьюрінгу. neerc.ifmo. [Електронний ресурс] – Режим доступу: https://neerc.ifmo.ru/wiki/index.php?title=Тьюринг-полнота

12. Turing completeness. Wikipedia. [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Turing_completeness#cite_note-1

13. Gavin Wood, Ethereum: A secure decentralised generalised transaction ledger. gavwood.com. [Electronic book]. – Access Mode: http://gavwood.com/Paper.pdf

14. b-money. weidai.com. [Електронний ресурс] – Режим доступу: https://www.webcitation.org/62ArKBIqT?url=http://www.weidai.com/bmoney.txt

15. N. Szabo, Secure property titles with owner authority. 1998. Access Mode: http://unenumerated.blogspot.com/2005/12/bit-gold.html

16. Leslie Lamport, The Byzantine Generals Problem / Leslie Lamport, Robert Shostak, Marshall Pease // ACM Transactions on Programming Languages and Systems. July, 1982. – PP. 382-40. – Access Mode http://lamport.azurewebsites.net/pubs/pubs.html#byz

17. Advanced Peer-to-Peer Networking. ibm..com. [Електронний ресурс] – – Режим доступу: https://www.ibm.com/docs/en/i/7.3?topic=concepts-advanced-peer-peer-networking

18. Karl Aberer, Advanced Peer-to-Peer Networking: The P-Grid System and its Applications / Karl Aberer, Anwitaman Datta, Zoran Despotovic // https://www.researchgate.net/publication/2556132_Advanced_Peer-to-Peer_Networking_The_P-Grid_System_and_its_Applications

19. IBM Advanced Peer-to-Peer Networking. Wikipedia. [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/IBM_Advanced_Peer-to-Peer_Networking

20. ARPANET. developer.mozilla. [Електронний ресурс] – Режим доступу: https://developer.mozilla.org/ru/docs/Glossary/Arpanet

21. ОДАС В. М. Глушкова: Історія проекту побудови інформаційного суспільства. Суспільне. [Електронний ресурс] – Режим доступу: https://commons.com.ua/uk/ogas-v-m-glushkova-istoriya-proekta-postroeniya-informatsionnogo-obshhestva/

22. uTorrent. [Електронний ресурс] – Режим доступу: https://www.utorrent.com/

23. BitTorrent. [Електронний ресурс] – Режим доступу: https://www.bittorrent.com/

24. Малахов Є.В, Організація баз даних. Конспект лекцій. / Одеса. – 169с. [Електронний ресурс] – Режим доступу: http://computer-science.onu.edu.ua/Малахов%20Организация%20баз%20данных.pdf

25. Genesis block. Bitcoin Wiki [Електронний ресурс] – Режим доступу: https://en.bitcoin.it/wiki/Genesis_block

26. Mercle Tree. USA Patent 4,309,569 [Електронний ресурс] – Режим доступу: https://patentimages.storage.googleapis.com/69/ab/d9/2ff9f94fada6ea/US4309569.pdf

27. Mempool. Binance Academy [Електронний ресурс] – Режим доступу: https://academy.binance.com/en/glossary/mempool

28. Ethereum Transaction Pool. Geth. [Електронний ресурс] – Режим доступу: https://geth.ethereum.org/docs/rpc/ns-txpool

29. Що таке гроші? Binance Academy. [Електронний ресурс] – Режим доступу: https://academy.binance.com/uk/articles/what-is-money

30. Sergi Delgado-Segura, Analysis of the Bitcoin UTXO Set / Sergi Delgado-Segura, Cristina Pérez-Solà, Guillermo Navarro-Arribas // Financial Cryptography and Data Security. 2018. – PP. 15. – Access Mode: https://link.springer.com/chapter/10.1007/978-3-662-58820-8_6

31. Аккаунты ethereum. ethereum.org.[Електронний ресурс] – Режим доступу: https://ethereum.org/ru/developers/docs/accounts/

32. Jean-Paul Delahaye, L’attaque Goldfinger d’une blockchain. [Електронне видання] – Режим доступу: https://scilogs.fr/complexites/lattaque-goldfinder-dune-blockchain/

33. Greg Walker, Longest Chain. [Електронне видання] – Режим доступу: https://learnmeabitcoin.com/technical/longest-

chain#:~:text=The%20longest%20chain%20is%20what,on%20the%20same%20transaction%20history

34. Ethereim GHOST protocol. Github. [Електронний ресурс] – Режим доступу: https://github.com/lukepark327/eth-ghost-sol

35. Mining Farm. Binance Academy [Електронний ресурс] – Режим доступу: https://academy.binance.com/en/glossary/mining-farm

36. What is an ASIC miner farm? Quora. [Електронний ресурс] – Режим доступу: https://www.quora.com/What-is-an-ASIC-miner-farm

37. Proof-Of-Stake (Pos). ethereum.org. [Електронний ресурс] – Режим доступу: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

38. Proof of Authority Explained. Binance Academy. [Електронний ресурс] – Режим доступу: https://academy.binance.com/en/articles/proof-of-authority-explained

39. Networking layer. ethereum.org. [Електронний ресурс] – Режим доступу: https://ethereum.org/en/developers/docs/networking-layer/

40. Ingmar Baumgart, S/Kademlia: A practicable approach towards secure key-based routing / Ingmar Baumgart, Sebastian Mies // 2007 International Conference on Parallel and Distributed Systems. December 05-07, 2007. – PP. 5. – Access Mode: https://ieeexplore.ieee.org/document/4447808

41. Antonio Delgado Peris, Evaluation of the Broadcast Operation in Kademlia / Antonio Delgado Peris, José M. Hern'ndez, Eduardo Huedo // 2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems. June 25-27, 2012. – PP. 12. – Access Mode: https://ieeexplore.ieee.org/document/6332245 .

42. S. Au, Th. Power, Tokenomics: The Crypto Shift of Blockchains, ICOs, and Tokens // Packt Publishing Ltd, 2018.

43. К. М. Краус, blockchain як новітній фінансовий інститут: процеси, стратегії, технології та практика застосування в умовах цифровізації

економіки / К. М. Краус, Н. М. Краус, О. В. Манжура. [Електронний ресурс] – Режим доступу: http://www.economy.nayka.com.ua/pdf/1_2022/76.pdf

44. Введение в умные контракты. ethereum.org. [Електронний ресурс] – Режим доступу: https://ethereum.org/ru/smart-contracts/

45. Introduction to dapps. ethereum.org. [Електронний ресурс] – Режим доступу: https://ethereum.org/en/developers/docs/dapps/

46. Eric A. Brewer, Towards robust distributed systems (abstract) [Electronic book] // Proceedings of the nineteenth annual ACM symposium on Principles of distributed computing. July 2000. – Access Mode: https://dl.acm.org/doi/10.1145/343477.343502

47. Scalability. Bitcoin Wiki. [Електронний ресурс] – Режим доступу: https://en.bitcoin.it/wiki/Scalability

48. Layer-1 and Layer-2 Blockchain Scaling Solutions. Cryptopedia. Gemini. [Електронний ресурс] – Режим доступу: https://www.gemini.com/cryptopedia/blockchain-layer-2-network-layer-1-network

49. Wenting Wang, Scale Up vs. Scale Out in Cloud Storage and Graph Processing Systems / Wenting Wang, Le Xu // 2015 IEEE International Conference on Cloud Engineering. March 09-13. – PP. 6. – Access Mode: https://ieeexplore.ieee.org/document/7092956

50. Kai Hwang, Scale-Out vs. Scale-Up Techniques for Cloud Performance and Productivity / Kai Hwang, Yue Shi, Xiaoying Bai // 2014 IEEE 6th International Conference on Cloud Computing Technology and Science. December 15-18, 2014. – PP. 858-865. – Access mode: https://ieeexplore.ieee.org/document/7037758

51. Shafi Goldwasser, The knowledge complexity of interactive proofs system / Shafi Goldwasser, Silvio Micali, Charles Rackoff // SIAM Journal on Computing. 1989. – PP. 186-208. – Access Mode: http://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf

52. What are zero-knowledge proofs? ethereum.org.[Електронний ресурс] – Режим доступу: https://ethereum.org/en/zero-knowledge-proofs/ нулевое разглашение

53. Платіжні канали. ethhub.io. [Електронний ресурс] – Режим доступу: https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/payment-channels/

54. Payment Channel. Електронний ресурс] – Режим доступу: https://research.csiro.au/blockchainpatterns/general-patterns/blockchain-payment-patterns/payment-channel/

55. Bahaa Mahmoud Abdelhafiz, Sharding Database for Fault Tolerance and Scalability of Data / Bahaa Mahmoud Abdelhafiz, Mourad Elhadef // 2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM). January 2021. – PP. 23. – Access mode: https://ieeexplore.ieee.org/document/9357711

56. Sharding. ethereum.org. [Електронний ресурс] – Режим доступу: https://ethereum.org/en/upgrades/sharding/ шардинг в блокчейне

57. Шардінг у Блокчейні. ethhub.io. [Електронний ресурс] – Режим доступу: https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/sharding/

58. Банг-Дженсен Йорген, Ациклические орграфы, орграфы: теория, алгоритмы и приложения, Монографии Springer по математике, 2-е, Springer-Verlag: 32–34, 2008 г., ISBN 978-1-84800-997-4 .

59. Y. Sompolinsky, Y. Lewenberg, and A. Zohar. SPECTRE: Serialization of Proof-of-work Events: Confirming Transactions via Recursive Elections, 2017.

60. Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich. Algorand: Scaling byzantine agreements forcryptocurrencies. In Proc. the 26th Symposium on Operating Systems Principles, pages 51–68. ACM, 2017.

61. S. S. Grybniak, D. Dmytryshyn, Y. Leonchyk, I. Mazurok, O. Nashyvan, and R. Shanin, “Waterfall: Gozalandia. Distributed protocol with fast finality and proven safety and liveness,” In press. Какая-то ссылка на Ватерфол

62. Y. Sompolinsky, “PHANTOM and GHOSTDAG: A Scalable Generalization of Nakamoto Consensus” / Y. Sompolinsky, S. Wyborski, and A.

Zohar // Cryptology ePrint Archive, Paper 2018/104, 2018. [Online]. Available: https://eprint.iacr.org/2018/104

63. Ethereum2.-Github [Електронний ресурс] – Режим доступу: https://github.com/ethereum/consensus-specs/blob/dev/specs/phase0/p2p-interface.md#topics-and-messages

64. Kaspa. Subnetworks. [Online]. Available: https://kaspa.gitbook.io/kaspa/archive/archive/components/kaspad-full-node/reference/subnetworks-1

65. N. Durov. (2019) Telegram Open Network. [Online]. Available: https://ton.org/ton.pdf

66. Oleksandr Antonenko, Subnetworks in Block-DAG / Oleksandr Antonenko, Sergii Grybniak, Denis Guzey et al. // IEEE 1st GET Blockchain Forum, California, United States, 2022. In press.

67. Lightweight node. Bitcoin Wiki. [Електронний ресурс] – Режим доступу: https://en.bitcoin.it/wiki/Lightweight_node

68. Grybniak, Y. Leonchyk, R. Masalskyi, I. Mazurok, O. Nashyvan, and R. Shanin, "Decentralized platforms: Goals, challenges, and solutions," 2022 IEEE 7th Forum on Research and Technologies for Society and Industry Innovation (RTSI), 2022, pp. 62-67, doi: 10.1109/RTSI55261.2022.9905225

69. Gerardo Beni, Swarm Intelligence in Cellular Robotic Systems / Gerardo Beni, Jing Wang // Part of the NATO ASI Series book series. – PP.703-712. – Access Mode: https://link.springer.com/chapter/10.1007/978-3-642-58069-7_38

70. M. Dorigo, Optimization, Learning and Natural Algorithms, PhD thesis, Politecnico di Milano, Italie, 1992. Муравьиные алгоритмы

71. L. Hubert, Monotone invariant clustering procedures // Psychometrika, vol. 38, no. 1, 1973. – PP. 47-62.

72. M. Roux, A comparative study of divisive and agglomerativehierarchical clustering algorithms // Journal of Classification, 2018, PP. 345-366.

73. Stuart P. Lloyd, Least Squares Quantization in PCM // EEE TRANSACTIONS ON INFORMATION THEORY, MARCH 1982. – PP. 28. – Access mode: https://cs.nyu.edu/~roweis/csc2515-2006/readings/lloyd57.pdf

74. Dan Simovici, The PAM Clustering Algorithm. PP. 4. – Access mode: https://www.cs.umb.edu/cs738/pam1.pdf неиерарх(пам алгоритм)

75. Johann Bacher, SPSS TWOSTEP CLUSTER – A FIRST EVALUATION / Johann Bacher, Knut Wenzig, Melanie Vogler // Universität Erlangen-Nürnberg, Sozialwissenschaftliches Institut, Lehrstuhl für Soziologie, February 2004. – PP. 23. – Access mode: https://www.statisticalinnovations.com/wp-content/uploads/Bacher2004.pdf

76. Douglas H. Fisher, Knowledge Acquisition Via Incremental Conceptual Clustering // Kluwer Acadenfic Publishers, Boston Manufactured in The Netherlands 1987. – PP. 139-172 – Access mode: https://link.springer.com/content/pdf/10.1007/BF00114265.pdf

77. Matthaios Theodorakis, Using Hierarchical Clustering to Enhance Classification Accuracy / Matthaios Theodorakis, Andreas Vlachos, Theodore Z. Kalamboukis. PP. 10. – Access mode: https://www.cl.cam.ac.uk/~av308/cobweb.pdf

78. М. А. Рожков, Методы самоорганизации роя беспилотных летательных средств. / М. А. Рожков, Р. В. Киричек. [Електронний ресурс] – Режим доступу: https://conf-ntores.etu.ru/assets/files/2020/cp/papers/143.pdf

79. The Raft Consensus Algorithm. Github.io. [Електронний ресурс] – Режим доступу: https://raft.github.io/

80. Lakshmish Ramaswamy, A Distributed Approach to Node Clustering in Decentralized Peer-to-Peer Networks / Lakshmish Ramaswamy, Bu gra Gedi, Ling Li // IEEE Transactions on Parallel and Distributed Systems, September 2005. – PP. 814-829 http://cobweb.cs.uga.edu/~laks/papers/tpds_cdc.pdf

81. Документация по C#. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/ru-ru/dotnet/csharp/

82. Overview of .NET Framework. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/dotnet/framework/get-started/overview

83. T. H. Cormen, C. E. Leiserson, R. L. Rivest, C. Stein. Introduction to Algorithms. – 3rd edition. – The MIT Press, 2009.

84. R. C. Prim: Shortest connection networks and some generalizations. In: Bell System Technical Journal, 36 (1957), PP. 1389-1401. – Access mode: https://archive.org/details/bstj36-6-1389

85. Dijkstra E. W. A note on two problems in connexion with graphs (англ.) // Numer. Math / F. Brezzi – Springer Science+Business Media, 1959. – PP. 269–271. – Access mode: http://www.m3.ma.tum.de/foswiki/pub/MN0506/WebHome/dijkstra.pdf