Одеський національний університет імені І. І. Мечникова
Факультет математики, фізики та інформаційних технологій
Кафедра оптимального керування та економічної кібернетики

Кваліфікаційна робота

на здобуття ступеня вищої освіти «магістр»

«Імітаційне моделювання та оптимізація ієрархічного консенсусу в блокчейнах контрольованого складу»

«Simulation Modeling and Optimization of the Hierarchical Consensus in Permissioned Blockchains»

Виконала: здобувачка денної форми навчання
спеціальності 113 Прикладна математика
Освітня програма «Прикладна математика»
Ворохта Аліса Юріївна

Керівник: канд. фіз.-мат. наук, доц. Страхов Є. М. _____
Рецензент: канд. техн. наук, доц. Мазурок І.Є.

Рекомендовано до захисту:

Протокол засідання кафедри

№ ___ від _____ 2022 р.

Завідувач кафедри

_____ _____

Захищено на засіданні ЕК № _____

Протокол № ___ від _____ 2022 р.

Оцінка _____ / _____ / _____

Голова ЕК

_____ _____

Одеса — 2022 р.

Odesa I. I. Mechnikov National University
Faculty of Mathematics, Physics and Information Technology
Department of optimal control and economical cybernetics

Diploma thesis

master

«Simulation Modeling and Optimization of the Hierarchical Consensus in Permissioned Blockchains»

Fulfilled by: full-time student
specialty 113 Applied Mathematics
Alisa Vorokhta

Supervisor: Ph. D. in physics and mathematics sciences, Associate Professor Yevhen Strakhov
Reviewer: Ph. D. in technical sciences, Associate Professor Igor Mazurok

Odesa — 2022

CONTENTS

Вступ 4

Introduction 6

1. Imitation Modeling and Optimization 7
- 1.1. What is Simulation Modeling? . . . 7
- 1.2. Optimization . . . 8
- 1.3. Python Programming Language . . . 8

2. Fundamentals of distributed systems and blockchain 9
- 2.1. Distributed Systems . . . 9
- 2.2. Blockchain and Consensus . . . 10

3. Modeling and Analyzing a Permissioned Blockchain with Hierarchical Consensus 13
- 3.1. Distributed Ledger Description . . . 13
  - 3.1.1. Terms . . . 13
  - 3.1.2. Description . . . 14
- 3.2. Hierarchical Consensus . . . 14
- 3.3. Committee Formation Problem . . . 16
  - 3.3.1. Minimizing the Number of Messages . . . 16
  - 3.3.2. Minimizing the Number of Missed Slots . . . 18
- 3.4. The Problem of Penalizing Faulty Coordinators . . . 27
  - 3.4.1. Types of Coordinators' Faultiness . . . 27
  - 3.4.2. Simulation Modeling . . . 27
- 3.5. Conclusion . . . 29

Висновки 30

Conclusion 31

Bibliography 32

Appendix A. Computer Code for the Partitioning algorithm 35

ВСТУП

Наразі до технології блокчейн [1] виникає інтерес у представників найрізноманітніших сфер: від банковського сектору до земельного реєстру. Деякі компанії навіть базують свої проекти на технології блокчейн. Блокчейн – це децентралізована база даних, у якій інформація зберігається у вигляді «ланцюжка блоків» певної кількості транзакцій. Децентралізація [2] означає відсутність вузлів або груп з винятковим доступом до певних ресурсів.

Серед особливостей блокчейну можна також зазначити, що дані зберігаються в учасників мережі. Оскільки блокчейн децентралізований, і дані в ньому не можуть бути змінені або скасовані завдяки системі криптографічного захисту, ця технологія вважається дуже безпечною.

Технології блокчейн можна знайти застосування практично у всіх сферах діяльності. У [3] досліджується застосування технології блокчейн у транспортній логістиці. А у [4] було досліджено особливості застосування блокчейн-технології у цифровій економіці.

Одним із засобів дослідження є імітаційне моделювання. Воно допомагає досліджувати реальну фізичну систему, не проводячи з нею безпосередніх експериментів. Наприклад, у [5] було побудовано моделі та імітації системи освіти на основі блокчейну, а [6] досліджує методи моделювання систем блокчейн за допомогою Anylogic.

Оптимізація - це процес пошуку розв'язку, який найкраще задовольняє заданому критерію. [7] показує приклад застосування оптимізації у блокчейну для вибору консенсусу. У статті [8] розглядаються результати застосування оптимізації в блокчейні та запропоновані більш розширені завдання оптимізації для майбутньої роботи.

Мета дослідження: побудування та оптимізація моделей блокчейну контрольованого складу для дослідження її особливостей.

Об'єкт дослідження: блокчейн контрольованого складу з ієрархічним консенсусом.

Предмет дослідження: блокчейн контрольованого складу.

Метод дослідження: аналітичний аналіз та експерименти з моделлю у Python.

INTRODUCTION

Currently, representatives of various fields are interested in blockchain technology [1]: from the banking sector to the land registry. Some companies even base their projects on blockchain technology. Blockchain is a decentralized database in which information is stored in the form of a "chain of blocks"of a certain number of transactions. Decentralization [2] refers to the absence of nodes or groups with exclusive access to certain resources.

Among the features of the blockchain, it can also be noted that the data is stored by the network participants. Since the blockchain is decentralized, and the data in it cannot be changed or reversed due to the cryptographic protection system, this technology is considered very secure.

Blockchain technology can be used in almost all fields of activity. [3] explores the application of blockchain technology in transport logistics. And in [4] the peculiarities of the application of blockchain technology in the digital economy have been studied.

One of the research tools is simulation modeling. It helps to study a real physical system without conducting direct experiments with it. For example, in [5] were built models and simulations of a blockchain-based education system, and [6] explores methods for modeling blockchain systems using Anylogic.

Optimization is the process of finding a solution that best satisfies a given criterion. [7] shows an example of applying optimization to the blockchain for consensus selection. The article [8] discusses the results of the application of optimization in the blockchain and proposes more advanced optimization problems for future work.

The purpose: to build and optimize models of a permissioned blockchain to study its features.

Object of study: permissioned blockchain with hierarchical consensus.

Subject of study: permissioned blockchain.

Research method: analytical analysis and experiments with the model in Python.

ВИСНОВКИ

Робота була присвячена дослідженню ієрархічного консенсусу в блокчейнах контрольованого складу за допомогою аналітичного аналізу та моделювання на мові програмування Python.

1) Було описано модель ієрархічного консенсусу на основі протоколу Gozalandia.
2) Було описано та вирішено проблему мінімізації числа повідомлень, якими обмінюються Координатори.
3) Було виявлено, що найбільший процент несправних Координаторів, при якому не відбувається великої затримки у фіналізації блоків - це 20%.
4) Було виявлено, що найкраще число для кількості Учасників Комітету та Комітетів має вигляд $3 \cdot f + 1$ для зменшення кількості пропущених слотів. При цьому кількість Комітетів має бути якомога меншою.
5) Було побудовано Алгоритм розбиття та виявлено, що кількість пропущених слотів є низькою при його застосуванні.
6) Було розглянуто проблему знаходження параметра масштабування λ, який відповідає за штрафи за атаки, роблячи їх недоцільними. Було рекомендовано значення цього параметру $\lambda = 100$.

Щоб краще дослідити цю тему, можна протестувати роботу такої децентралізованої системи.

Результати досліджень були представлені на науковій конференції [24].

CONCLUSION

The work was dedicated to the study of hierarchical consensus in permissioned blockchains using analytical analysis and modeling in the Python programming language.

1) A hierarchical consensus model based on the Gozalandia protocol was described.
2) The problem of minimizing the number of messages exchanged by Coordinators has been described and resolved.
3) It was found that the largest percentage of faulty Coordinators, at which there is no significant delay in block finalization, is 20%.
4) It was found that the best number for the number of Committee Members and Committees is $3 \cdot f + 1$ to reduce the number of missed slots. At the same time, the number of Committees should be as small as possible.
5) A Partitioning algorithm was built and the number of missed slots was found to be low when it was applied.
6) The problem of finding the scaling parameter λ, which is responsible for the penalties for the attacks, making them infeasible, was considered. The value of this parameter $\lambda = 100$ was recommended.

To better explore this topic, we should test the operation of such a decentralized system.

The research results were presented at the scientific conference [24].

BIBLIOGRAPHY

1. Wright C. Bitcoin: A Peer-to-Peer Electronic Cash System // University of Southern Queensland. — August, 2008. — DOI: http://dx.doi.org/10.2139/ssrn.3440802
2. Anderson M. Exploring Decentralization: Blockchain Technology and Complex Coordination // Anderson M. — Journal of Design and Science. — 2019. — Resource access mode: https://jods.mitpress.mit.edu/pub/7vxemtm3/release/2
3. Корнага Я. І. Дослідження та застосування технології блокчейн у транспортній логістиці / Корнага Я. І., Тільняк Ю. Я. — ВІСНИК ЖДТУ. — 2019. – № 1 (83). — DOI: https://doi.org/10.26642/tn-2019-1(83)-12-17
4. Жмуркевич А. Є. Особливості застосування блокчейн-технології у цифровій економіці / Жмуркевич А. Є., Вакулін Р. С. — Міжнародний науковий журнал "Інтернаука". — 2018. — № 6(2). — С. 14-17. — Режим доступу: http://nbuv.gov.ua/UJRN/mnj_2018_6(2)__5
5. Bajwa N. K. Modelling and Simulation of Blockchain based Education system / Bajwa N. K. —- Masters thesis, Concordia University. — 2018. — Resource access mode: https://spectrum.library.concordia.ca/984170/1/Bajwa_MASc_S2018.pdf
6. Spirkina A. Approaches to Modeling Blockchain Systems / [Spirkina A., Aptrieva E., Elagin V. et al.] — 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). — 2020. — DOI: 10.1109/ICUMT51630.2020.9222437
7. Золотарьова І. О. Інформаційні технології оптимізації роботи приватного блокчейн за допомогою вибору алгоритму консенсусу / Золотарьова І. О., Плеханова Г. О. — Системи обробки інформації. — 2020. — № 1(160). — С. 107-14. — DOI: https://doi.org/10.30748/soi.2020.160.14
8. Antwi R. A Survey on Network Optimization Techniques for Blockchain Systems / [Antwi R., Gadze J., Tchao E. et al.] — Algorithms 2022. — 15. — 193. — DOI: https://doi.org/10.3390/a15060193
9. Anu M. Introduction to modeling and simulation / Anu M. — WSC '97: Proceedings of the 29th conference on Winter simulation. — December, 1997.

— p. 7-13. — DOI: https://doi.org/10.1145/268437.268440

10. Downey A. Modeling and Simulation in Python / Downey A. — Green Tea Press. — 2017. — Resource access mode: https://greenteapress.com/modsimpy/ModSimPy3.pdf
11. Why use simulation modeling? // Anylogic: web site. — URL: https://www.anylogic.com/use-of-simulation/ (date of application: 05.12.2022)
12. Mathematical optimization / Wikipedia, the free encyclopedia: web site. — URL: https://en.wikipedia.org/wiki/Mathematical_optimization (date of application: 05.12.2022)
13. Rossum G. Python tutorial / Rossum G. — Technical Report CS-R9526. — Centrum voor Wiskunde en Informatica (CWI) Amsterdam. — May, 1995. — Resource access mode: https://ir.cwi.nl/pub/5007/05007D.pdf
14. Brewer E. Towards robust distributed systems / Brewer E. — Proceedings of the XIX annual ACM symposium on Principles of distributed computing. — Portland, OR: ACM, 2000. — Vol. 19, no. 7. — DOI: doi:10.1145/343477.343502
15. Grybniak S. Decentralized platforms: Goals, challenges, and solutions / [Grybniak S., Leonchyk Y., Masalskyi R. et al] — 2022 IEEE 7th Forum on Research and Technologies for Society and Industry Innovation (RTSI). — 2022. — pp. 62-67. — DOI: 10.1109/RTSI55261.2022.9905225
16. Distributed Systems - The Complete Guide / Confluent: web site. — URL: https://www.confluent.io/learn/distributed-systems/
17. Blockchain / Wikipedia, the free encyclopedia: web site. — URL: https://en.wikipedia.org/wiki/Blockchain (date of application: 05.12.2022)
18. Types of Blockchain / Geeks for Geeks: web site. — URL: https://www.geeksforgeeks.org/types-of-blockchain/ (date of application: 05.12.2022)
19. Frankenfield J. Consensus Mechanism (Cryptocurrency) / Frankenfield J. — Investopedia: web site. — URL: https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp (date of application: 30.11.2022)
20. Lamport L., Shostak R., Pease M. C. The Byzantine Generals Problem /

ACM Transactions on Programming Languages and Systems. — Vol. 4. — No. 3. — July 1982. — DOI: 10.1145/357172.357176

21. Castro M. Practical Byzantine Fault Tolerance / Castro M., Lickov B. — OSDI '99: Proceedings of the third symposium on Operating systems design and implementation. — February 1999. — p. 173–186. — DOI: 10.1002/9781119682127.ch7
22. Grybniak S., Dmytryshyn D., Leonchyk Y., Mazurok I., Nashyvan O., Shanin R. Waterfall: A Scalable Distributed Ledger Technology // IEEE 1st GET Blockchain Forum, California. — United States. — 2022. — In press.
23. Grybniak S. Waterfall: Salto Collazo. Tokenomics / [Grybniak S., Leonchyk Y., Masalskyi R. et al.] — IEEE International Conference on Blockchain, Smart Healthcare and Emerging Technologies. — Bucharest, Romania. — 2022. — In press.
24. Vorokhta A. Simulation Modelling of the Consensus Based on the Gozalandia / [Vorokhta A., Mazurok I., Leonchyk Y. et al.] — Adaptive Learning Management Technologies. — Kyiv. — 2022. — p. 31-33.
25. Mazurok I. An incentive system for decentralized DAG-based platforms / [Mazurok I., Leonchyk Y., Grybniak S. et al.] — Applied Aspects of Information Technology. — vol. 5(3). — 2022. — pp. 196–207.