Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U000478

Особливі позначки: відкрита

Дата реєстрації: 10-02-2025

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Грибняк Сергій Сергійович
2. Serhii Grybniak

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 122

Назва наукової спеціальності: Комп'ютерні науки

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Комп'ютерні науки

Дата захисту: 18-12-2023

Спеціальність за освітою: Менеджмент організацій

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 2977

Повне найменування юридичної особи: Національний університет "Одеська політехніка"

Код за ЄДРПОУ: 43861328

Місцезнаходження: пр. Шевченка, буд. 1, Одеса, 65044, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Національний університет "Одеська політехніка"

Код за ЄДРПОУ: 43861328

Місцезнаходження: пр. Шевченка, буд. 1, Одеса, 65044, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.54.03

Тема дисертації:

1. Моделі та методи підвищення ефективності обробки транзакцій у розподілених реєстрах.

2. Models and Methods for Improving Transaction Processing Efficiency in Distributed Ledgers.

Реферат:

1. 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. 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. У другому розділі дисертаційної роботи досліджено шляхи підвищення ефективності обробки транзакцій та масштабованості розподіленого реєстру. 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 мультипідписом. 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. У четвертому розділі дисертаційної роботи розроблено експериментальну децентралізовану платформу Waterfall. Підтверджено спроможність та правильність технічних рішень, заснованих на результатах дисертаційного дослідження.

2. 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. In the second section of the dissertation work, ways to improve the efficiency of transaction processing and scalability of the distributed ledger are investigated. 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. The capability and correctness of the technical solutions based on the findings of the dissertation research have been confirmed.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- 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.

- 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.
- Mazurok I., LeonchykY., GrybniakS., VorokhtaA., Nashyvan O. Multiobjective 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.
- Грибняк С. С. Двошарова модель масштабуємого розподіленого децентралізованого реєстру. Наукові праці Вінницького національного технічного університету. 2023. № 2. С. 120–127.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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-2022q4/an-incentive-system-for-decentralized-dag-based-platforms.pdf.

Наукова (науково-технічна) продукція: програмні продукти, програмно-технологічна документація

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Дмитришин Дмитро Володимирович
2. Dmytro Dmytryshyn

Кваліфікація: д. т. н., професор, 05.13.03

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Одеська політехніка"

Код за ЄДРПОУ: 43861328

Місцезнаходження: пр. Шевченка, буд. 1, Одеса, 65044, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Яцків Василь Васильович
2. Vasyl Yatskiv

Кваліфікація: д. т. н., професор, 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Західноукраїнський національний університет

Код за ЄДРПОУ: 33680120

Місцезнаходження: вул. Львівська, буд. 11, Тернопіль, Тернопільський р-н., 46009, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Шаховська Наталія Богданівна

2. Natalia Shakhovska

Кваліфікація: д.т.н., професор, 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Арсірій Олена Олександрівна

2. Olena Arsirii

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Одеська політехніка"

Код за ЄДРПОУ: 43861328

Місцезнаходження: пр. Шевченка, буд. 1, Одеса, 65044, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Годовиченко Микола Анатолійович

2. Mykola A. Hodovychenko

Кваліфікація: к. т. н., доц., 05.13.23

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Одеська політехніка"

Код за ЄДРПОУ: 43861328

Місцезнаходження: пр. Шевченка, буд. 1, Одеса, 65044, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Антощук Світлана Григорівна
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Антощук Світлана Григорівна
Відповідальний за підготовку облікових документів	Кривда Вікторія Ігорівна
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна