МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ
ІНЖЕНЕРІЇ

**ДАРМОГРАЙ ВАСИЛЬ ОЛЕГОВИЧ**

УДК 004.62

# АЛГОРИТМІЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТЕХНОЛОГІЇ BLOCKCHAIN ПРИ ПОБУДОВІ МЕРЕЖЕВИХ IoT-ІНФРАСТРУКТУР

123 «Комп'ютерна інженерія»

**Автореферат**

дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль
2019

Роботу виконано на кафедрі комп’ютерних систем та мереж Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

**Керівник роботи:** кандидат технічних наук, доцент кафедри комп'ютерних систем та мереж
**Луцків Андрій Мирославович,**
Тернопільський національний технічний університет імені Івана Пулюя,

**Рецензент:** кандидат фізико-математичних наук, доцент, завідувач кафедри фізики
**Скоренький Юрій Любомирович,**
Тернопільський національний технічний університет імені Івана Пулюя,

Захист відбудеться 27 грудня 2019 р. о $9^{.00}$ годині на засіданні екзаменаційної комісії № 37 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, ауд.1-603

# ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

**Актуальність теми**: IoT з кожним днем все збільшується та отримує все більш вагомі позиції в світі. Незважаючи на свій бурхливий розвиток IoT-мережі пристроїв можна характеризувати, як невпорядкованістю так і відсутністю чітких стандартів. Завдяки цьому безпека даних користувачів є під небезпекою. Тому Blockchain технологія, яка є ланцюжком блоків транзакцій, й, водночас, розподілена база даних, що зберігає впорядкований ланцюжок записів являє собою сильним доповненням до стабільності та захищеності постійно зростаючої IoT-системі.

Тому технології Blockchain для IoT-інфраструктур є актуальним напрямком досліджень саме на сьогоднішній день, у час, коли технології швидко розвиваються, а єдиних стандартів не існує.

**Мета та задачі дослідження**: Метою даної роботи є розроблення архітектури IoT-інфраструктури з використанням технології Blockchain та аналіз її ефективності та стресостійкості. Для досягнення вказаної мети в рамках дипломної роботи було сформульовано та розв’язано наступні задачі:

- Проаналізовано сучасний стан технологій IoT та Blockchain.
- Розглянути предметну область та проаналізовано спільне застосування технології Blockchain та IoT.
- Визначити проблематику та галузі їх можливого застосування. Визначити основні небезпеки несанкціонованого доступу до мережі та протидію йому.
- Оцінити та провести тестування ефективності, продуктивності та можливості масштабування мережі.
- Проаналізувати технології Blockchain в мережевій інфраструктурі IoT. Визначити ключові елементи керування мережею та її можливості.
- Оцінити стресостійкість мережі та її захист від атак зловмисника.

**Предмет дослідження**: Однорангові IoT-інфраструктури та методи передавання даних у них.

**Об’єкт дослідження**: Технологія Blockchain як засіб забезпечення захищеності IoT-інфраструктури.

**Методи дослідження**: Одним із методів тестування технології є програма Cooja яка добре підходить для оцінки низькоресурсних пристроїв і надає перевагу доступності впровадження різних протоколів, відомих IoT. Використання програми NS3 дозволить оцінки продуктивність накладення, оскільки вона широко застосовується для аналізу однорангових мереж.

**Наукова новизна одержаних результатів**

Проведено аналіз використання технології Blockchain в IoT-інфраструктурах і показано можливості їх сумісного використання.

Узагальнено та сформовано рекомендації, які дають змогу спростити процес масштабування інфраструктури.

Проведено експеримент в ході якого було проведено тестування сумісності технологій та їх продуктивність.

**Практичне значення одержаних результатів**

Розроблені рекомендації та здійснені тестування дають змогу спростити IoT-інфраструктуру при її масштабуванні.

**Публікації**

Результати дослідження апробовано на II міжнародні студентські науково-технічні конференції «Природничі та гуманітарні науки. Актуальні питання» м. Тернопіль 25-26 квітня 2019 року та VIII Міжнародній науково-технічній конференції молодих учених та студентів «Актуальні задачі сучасних технологій» м. Тернопіль 27-28 листопада 2019 року.

**Структура роботи**

Робота складається з пояснювальної записки та графічної частини. Пояснювальна записка складається із вступу, 3 розділів, висновків, список використаних джерел та додатку. Обсяг роботи: пояснювальна записка – 118 аркушів формату А4, графічна частина – 10 аркушів формату А1.

## ОСНОВНИЙ ЗМІСТ РОБОТИ

**У вступі** обґрунтовано актуальність дослідження, мету роботи, задачі, об’єкт, предмет, наукову новизну, практичне значення та публікації дипломних досліджень.

**У першому розділі роботи «Огляд предметної області»** описується спільне застосування технології Blockchain та IoT, їх можливе застосування у різноманітних сферах. Основну проблематику їх застосування, та забезпечення безпеки та конфіденційності.

**У другому розділі «Аналіз технології Blockchain в контексті IoT»** проаналізовано ключові елементи шифрування в технології Blockchain, PoW та PoS. Обґрунтовано використання алгоритму консенсусу на основі часу, та описано його оптимальність використання для мережі IoT-інфраструктур. Описано роботу менеджера блоків накладання, взаємодію його з низькоресурсними пристроями та іншими менеджерами.

**У третьому розділі «Апробація запропонованого підходу»** здійснено симуляцію IoT-інфраструктури з використанням технології Blockchain. Проведено їх тестування та оцінку на стресостійкість. Проаналізовано вплив розподілу потоків даних і транзакцій на мережу, та середній час обробки ОВМ для перевірки нових блоків.

**У четвертому розділі «Обґрунтування економічної ефективності»** зроблено обчислення показників економічної ефективності від застосування технології Blockchain в мережевих IoT-інфраструктурах.

**П’ятий розділ роботи «Охорона праці та безпека в надзвичайних ситуаціях»** проведено аналіз вимог з охорони праці і техніки безпеки при використання комп’ютерної техніки. Розглянуто небезпечні і шкідливі фактори при роботі з комп’ютерними системами, а також наслідки їх дії.

**Шостий розділ роботи «Екологія»** В розділі екології було проаналізовано методи визначення якості і обсягу забруднення. Визначено основну мету та методи дисперсійного аналізу в екології.

## ВИСНОВКИ

В першому розділі було розглянуто предметну область та проаналізовано спільне застосування технології Blockchain в IoT та можливості використання в різних сферах нашого життя. Визначено проблематику використання Blpckchain разом з IoT-пристроями, зокрема проблему безпеки. Проаналізовано галузі їх можливого застосування й проблеми.

В другому розділі було розроблено функціональну структуру та архітектуру IoT - інфраструктури з використанням ключових елементів, таких як LBM та OBM.

На основі ключових елементів LBM та OBM розроблено мережу накладення, яка потенційно може складатися з великої кількості вузлів.

Обґрунтовано використання алгоритму консенсусу на основі часу, замість більш ресурсомістких альтернатив, таких як PoW та PoS. Таким чином, завдяки алгоритму перевірки транзакцій кожен OBM перевіряє всі нові блоки, які отримує від пристроїв, та інших OBM.

В третьому розділі проаналізовано ключові оцінки різних аспектів діяльності LSB.

Проаналізовано програми для визначення ефективності низькоресурсних пристроїв та оцінено продуктивність накладення за допомогою них.

Проведено моделювання роботи таких мереж з метою оцінювання накладних витрат у LBM та споживання енергії.

Проаналізовано вплив розподілу потоків даних і транзакцій на мережу, та середній час обробки OBM для перевірки нових блоків.

При аналізі безпеки та конфіденційності було проаналізовано вимоги безпеки та основні можливі атаки на Blockchain та способи їх уникнення.

Здійснено тестування й визначено вплив кількості OBM на безпеку та пакетні накладні витрати, а також визначено відсоток транзакцій, який потрібно підтвердити для забезпечення максимальної стійкості до атак.

В четвертому розділі завдяки результату проведених розрахунків отриманий результат показує, що розробка матиме оптимальну економічну ефективність 0,56 і термін окупності становитиме майже два роки (1,79 року). Варто зазначити, що дані розрахунки носять номінальний характер і основна їх мета оцінити приблизну вартість дослідження та створення даного продукту. Номінальний характер розрахунків зумовлений тим, що даний програмний продукт має дослідницьке призначення.

В розділі охорони праці та безпеки в надзвичайних ситуаціях було визначено, що технологія IoT дозволяють зібрати інформацію для оцінки шкідливості і небезпечності умов праці персоналу в ході провадження виробничої діяльності суб’єктами господарювання. Завдяки доповненню IoT-

інфраструктури технологією Blockchsin, можна збирати, записувати та передавати необхідну інформацію, для своєчасної реакції на виникнення небезпечної ситуації. Симбіоз цих технологій дозволяє записувати зібрану інформацію в своєрідну базу даних для статистики та виявлення причинно-наслідкового зв'язку при виникненні небезпечної ситуації.

В розділі екології було проаналізовано методи визначення якості і обсягу забруднення. Визначено основну мету та методи дисперсійного аналізу в екології.

## СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Дармограй В. О. Застосування технології блокчейн в IoT / В. О. Дармограй, А. М. Луцків// Матеріали II міжнародної студентської науково-технічної конференції «Природничі та гуманітарні науки. Актуальні питання» (25-26 квітня 2019 року) – Тернопіль, ТНТУ – 2019 – с. 52

2. Дармограй В. О., Луцків А. М. к.т.н., доц. Аналіз бібліотек для реалізації Blockchain-інфраструктури для систем IoT / В. О. Дармограй, А. М. Луцків// Матеріали VIII міжнародної науково-технічної конференції молодих учених та студентів «Актуальні задачі сучасних технологій» (27-28 листопада 2019 року) – Тернопіль, ТНТУ – 2019 – с. 96

# АНОТАЦІЯ

Дипломна робота // Алгоритмічне та програмне забезпечення технології Blockchain при побудові мережевих IoT-інфраструктур // Дармограя Василя Олеговича // Тернопільський національний технічний університет імені Івана Пулюя. Факультет комп'ютерно - інформаційних систем та програмної інженерії. Кафедра комп'ютерних систем та мереж // група СІм-62 // Тернопіль, 2019 р. // с. - 118, рис. - 14, бібліогр. - 33.

Ключові слова: БЛОКЧЕЙН, ІНТЕРНЕТ РЕЧЕЙ.

Темою даної дипломної роботи є «Алгоритмічне та програмне забезпечення технології Blockchain при побудові мережевих IoT-інфраструктур».

Мета роботи полягає у розробці архітектури IoT-інфраструктури з використанням технології Blockchain.

У дипломній роботі проаналізовано сучасний стан технологій Blockchain та IoT, та визначено основну проблематику їх застосування; оцінено та проведено тестування ефективності, продуктивності та можливості масштабування.

Розроблено функціональну структуру та архітектуру IoT- інфраструктури з використанням ключових елементів LBM та OBM. За допомогою цих елементів розроблено мережу накладення, яка потенційно може складатися з великої кількості вузлів.

Обґрунтовано використання алгоритму консенсусу на основі часу, замість більш ресурсоміських альтернатив, таких як PoW та PoS. Таким чином, завдяки алгоритму перевірки транзакцій кожен OBM перевіряє всі нові блоки, які отримує від пристроїв, та інших OBM.

Проведено моделювання роботи ресурсоміських мереж з метою оцінювання накладних витрат у LBM та споживання енергії. При аналізі безпеки та конфіденційності було проаналізовано вимоги безпеки та основні можливості атаки на Blockchain та способи їх уникнення.

# ANNOTATION

Graduate thesis // Algorithms and software of Blockchain technology at network IoT-infrastructures development // Darmohrai Vasyl Olehovych // Ternopil Ivan Puluj National Technical University. Faculty of Computer Information Systems and Software Engineering. Computer Systems and Networks Department // group СІм-62 // Ternopil, 2019 y. // pages - 118, imges - 14, bibliography - 33.

Keywords: BLOCKCHAIN, INTERNET OF THINGS.

The topic of this thesis is "Algorithms and software of Blockchain technology at network IoT-infrastructures development".

The purpose of the work is to develop an architecture of IoT infrastructure using Blockchain technology.

The diploma thesis analyzes the current state of Blockchain and IoT technologies and identifies the main problems of their application; Performance, productivity and scalability testing and evaluation.

The functional structure and architecture of the IoT infrastructure using key LBM and OBM elements has been developed. These elements create an overlay network that can potentially consist of a large number of nodes.

Using a time-based consensus algorithm is justified instead of more resource-intensive alternatives such as PoW and PoS. Thus, thanks to the transaction verification algorithm, each OBM checks all new units it receives from devices and other OBMs.

Resource network modeling is simulated to estimate LBM overhead and energy consumption. Security and privacy analyzes have analyzed the security requirements and key capabilities of an attack on Blockchain and how to avoid them.