

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))

Дипломна робота

на здобуття освітньо-кваліфікаційного рівня «бакалавр»

(освітньо-кваліфікаційний рівень)

на тему «Розробка програмної системи моделювання та верифікації протоколів

консенсусу в розподілених системах»

«Development of software system for modeling and verification of consensus
protocols in distributed systems»

Виконала: студентка денної форми навчання

напряму підготовки 6.050102 – Комп'ютерна інженерія

(шифр і назва напряму підготовки, спеціальності)

Беляєва Крістіна Сергіївна

(прізвище, ім'я, по-батькові)

Керівник

к.ф.- м.н., доцент Пенко В.Г.

(науковий ступінь, вчене звання, прізвище та ініціали, підпис)

Рецензент

ст. викладач Берков Ю. М.

(науковий ступінь, вчене звання, прізвище та ініціали)

Рекомендовано до захисту:

Протокол засідання кафедри

№ ____ від « ____ » ____ 2019 р.

Завідувач кафедри

(підпис)

Є.В. Малахов
(прізвище, ініціали)

Захищено на засіданні ЕК № ____

протокол № ____ від « ____ » ____ 2019 р.

Оцінка ____ / ____ / ____
(за національною шкалою, шкалою ECTS, бали)

Голова ЕК

(підпис)

О.О. Арсірій
(прізвище, ініціали)

АННОТАЦИЯ

Важной тенденцией развития современных информационных систем является использование децентрализованного подхода к построению физической и алгоритмической структуры систем. Это позволяет обеспечить ряд положительных свойств, критически важных во многих предметных областях: масштабируемость, надежность от отказов и угроз различных типов, криптостойкость и др.

Одним из ведущих элементов таких систем является алгоритм консенсуса, позволяющий обеспечить принятие согласованных решений всеми узлами сети. Существующие и вновь разрабатываемые алгоритмы консенсуса далеко не всегда подтверждены аналитическим доказательством их корректности. В этих условиях актуальной является цель данной работы – разработка системы программного моделирования поведения децентрализованной системы, предназначенной для доказательства требуемых свойств алгоритма консенсуса.

Для этого в работе был представлен анализ предметной области децентрализованных систем, рассмотрены несколько популярных и перспективных алгоритмов консенсуса, изучены несколько подходов к доказательству и моделированию свойств консенсуса. На этой основе была спроектирована и разработана базовая программная система моделирования поведения децентрализованных систем.

Данная система позволяет осуществлять передачу сообщений между узлами сети по протоколу Gossip и расширять функциональность программных классов с учетом требований конкретных протоколов консенсуса.

АНОТАЦІЯ

Важливою тенденцією розвитку сучасних інформаційних систем є використання децентралізованого походу до побудови фізичної та алгоритмічної структури цих систем. Це дозволяє забезпечити ряд позитивних властивостей, критично важливих у багатьох предметних областях: масштабованість, надійність від відмов та загроз різних типів, криптостойкість і ін.

Одним з провідних елементів таких систем є алгоритм консенсусу, що дозволяє забезпечити прийняття узгоджених рішень усіма вузлами мережі. Існуючі та ті, що розробляються, алгоритми консенсусу не завжди підтверджені аналітичним доказом їх коректності. У цих умовах актуальною є мета даної роботи – розробка системи програмного моделювання поведінки децентралізованої системи, призначеної для доказу необхідних властивостей алгоритму консенсусу.

Для цього в роботі був представлений аналіз предметної області децентралізованих систем, розглянуті кілька популярних і перспективних алгоритмів консенсусу, вивчені кілька підходів для доведення і моделювання властивостей консенсусу. На цій основі була спроектована і розроблена базова програмна система моделювання поведінки децентралізованих систем.

Дана система дозволяє здійснювати передачу повідомлень між вузлами мережі по протоколу Gossip і розширювати функціональність програмних класів з урахуванням вимог конкретних протоколів консенсусу.

ABSTRACT

The important trend of the modern informative systems development is the use of the decentralized approach to the construction of physical and algorithmic structure of the systems. It allows to provide several of positive properties critically important in many subject domains : scalability, reliability from faults and threats of different types, cryptofirmness and other.

The critically important element of such systems is an consensus algorithm, allowing to provide the acceptance of the approved decisions by all nodes of the network. The existing and new developed algorithms of consensus are not always confirmed by analytical proof of their correctness. Under this conditions the purpose of the given work is relevant. It is the development of software system for modeling and verification of consensus protocols in distributed systems.

For these purposes analysis of data domain of decentralized systems was presented in given work, a few popular and promising consensus algorithms are considered, a few approaches to the proof and simulation of properties of the consensus are investigated. On this base program system of simulation of behavior of decentralized systems was designed and developed.

Given system implements message transfer between units of the network by protocol Gossip and allows to expand functionality of program classes in view of requirements of particular consensus protocols.

ЗМІСТ

ВСТУП.....	7
1 ЗАГАЛЬНІ ВІДОМОСТІ ПРО ДЕЦЕНТРАЛІЗОВАНІ СИСТЕМИ..	9
1.1 Мережа P2P	9
1.2 Протокол Gossip.....	10
1.3 Зберігання даних.....	11
1.4 Блокчейн.....	12
2 ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ТА ВИДІВ КОНСЕНСУСУ ..	17
2.1 Визначення консенсусу	17
2.2 CAP теорема.....	18
2.3 Класи консенсусу.....	21
2.3.1 Загальна класифікація консенсусу.....	21
2.3.2 Візантійський консенсус	22
2.3.3 Консенсус Proof-of-Work.....	23
2.3.4 Консенсус Proof-of-Stake	25
2.4 Загрози консенсусу	26
2.4.1 «Атака 51%» і Double-spending	26
2.4.2 Атака Сибілли	28
2.4.3 DDoS атаки.....	29
2.4.4 Злом криптографії.....	30
2.5 Алгоритм Algorand	30
2.6 Протокол HashGraph.....	32
3 МОДЕЛЮВАННЯ КОНСЕНСУСУ	34
3.1 Необхідність в моделюванні складних систем	34
3.2 Системи моделювання.....	35

3.3	Аналітичний підхід.....	35
3.4	Імітаційне моделювання.....	37
4	РЕАЛІЗАЦІЯ СИСТЕМИ МОДЕЛЮВАННЯ ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМ НА ОСНОВІ КОНСЕНСУСУ	39
4.1	Потреба у створенні власної системи для моделювання консенсусу	39
4.2	Аналіз проблематики моделювання комунікаційних процесів в децентралізованій системі	40
4.3	Опис реалізації бібліотеки класів і експериментів з мережею	42
4.4	Реалізація інтерактивної взаємодії з моделлю мережі.....	46
	ВИСНОВОК	54
	СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	55
	ДОДАТОК А.....	56

ВСТУП

Однією з характерних рис сучасного постіндустріального суспільства є глобалізація економіки. Географічне розташування перестає мати принципове значення в формуванні зв'язків між господарюючими суб'єктами. Розвиток мережевих технологій, електронної комерції, систем віддаленої роботи передбачає можливість і необхідність комунікації з великим числом підприємств зовнішнього середовища для вибору оптимальних партнерів.

Розвиток інформаційних мереж, запровадив технічні потужності сучасних комп'ютерів, бурхливий розвиток потужних і гнучких інтелектуальних програмних систем, здатних безперервно здобувати нові знання і змінювати свою структуру і функції. Розвиваючись і адаптуючись до важливих справ і умов зовнішнього середовища, створюють необхідні умови для трансформації сучасних технологій і методів роботи з інформацією.

Зі збільшенням масштабів і зростанням складності в централізованих системах падає надійність, тому з'являються технології і системи, побудовані на принципах децентралізації управління та автономності окремих елементів. В сучасних умовах компанії витрачають дуже багато коштів на створення та модернізацію своїх систем, ці витрати трансформуються в додаткові витрати, які лягають на плечі кінцевих споживачів.

Як правило, такі системи будуються на основі пірінгових комп'ютерних систем, що складається з рівноправних вузлів. Структура зв'язків між вузлами такої мережі досить довільна. Для забезпечення пересилання інформації між усіма вузлами мережі часто використовується простий протокол gossip.

Принципово важливою вимогою до роботи такої мережі є необхідність забезпечення однакового інформаційного стану на всіх вузлах мережі в умовно один момент часу. В таких випадках часто використовують таку інформаційну структуру як блокчейн – ланцюгова структура, що забезпечує додаткову властивість – захист від підробок, що забезпечується спеціальними криптографічними прийомами. На основі цього підходу працюють багато

сучасних криптовалют і розподілені системи з більш широкою функціональністю. У цих умовах центральною вимогою до роботи системи є досягнення консенсусу – досягнення усіма (або більшістю) вузлами мережі спільної думки і запис його результатів у власну копію блокчейну.

Найбільш популярними типами алгоритмів консенсусу є Proof of Work і Proof of Stake. Ще до появи сучасних криптовалют дослідники цікавилися питаннями організації обчислень в розподілених системах і формулювали різні варіанти алгоритмів консенсусу. Першоосновою багатьох таких алгоритмів є завдання про Візантійських генералів. Для опису алгоритмів консенсусу часто використовують спеціальні діаграми, де одночасно демонструється обмін вузлів інформаційними повідомленнями і перехід їх зі стану в стан.

Недоліками таких систем є: висока вартість в обслуговуванні і менша ефективність через проблеми з масштабуванням, а також складності у використанні для кінцевого користувача.

Для досягнення поставленої мети – створення базової архітектури програмних класів, які моделюють процеси інформаційного обміну між мережами P2P з урахуванням розумного узгодження за часом:

- 1) провести дослідження предметної області;
- 2) вивчити поняття консенсусу, класифікувати алгоритми консенсусу та визначити його властивості;
- 3) сформулювати вимоги до створюваної системи;
- 4) спроектувати та реалізувати систему, відповідну даним вимогам;
- 5) перевірити коректність реалізації декількома клієнтськими додатками.

ВИСНОВОК

У результаті виконаної дипломної роботи був представлений аналіз предметної області децентралізованих систем.

На основі цього аналізу було розглянуто ряд перспективних алгоритмів консенсусу. Це, у свою чергу, дозволило визначити основні вимоги до системи моделювання і верифікації таких алгоритмів.

Розглянуто кілька існуючих підходів до дослідження алгоритмів консенсусу та зроблений їх короткий і порівняльний аналіз. Визначено причини, що ускладнюють використання цих підходів.

Результатом зробленого, таким чином, аналізу став програмний проект, який містить бібліотеку основних класів для моделювання тимчасової децентралізованої бізнес-функції та розповсюдження в ній повідомлень по протоколу Gossip. Реалізовано 2 додатки, які демонструють результати такого моделювання. Консольний додаток показав, що змодельована мережа коректно розповсюджує одне або одночасно кілька повідомлень з урахуванням стохастичних затримок.

У віконному додатку реалізовано паралельне виконання моделі і управління нею через візуальний інтерфейс.

Незважаючи на невеликий обсяг написаного програмного коду, дана система є перспективним прототипом для моделювання реальних за масштабом мереж і запропонованих дослідниками протоколів консенсусу. Для цього потрібно розширити логіку вузла комп'ютерної мережі для аналізу свого стану і отриманого повідомлення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- 1) Dunbar, R.: Grooming, Gossip, and the Evolution of Language. Harvard University Press, 1998.
- 2) Nakamoto, Satoshi Bitcoin: A Peer-to-Peer Electronic Cash System, 2009.
- 3) Gavin Wood, Andreas M. Antonopoulos Mastering Ethereum O'Reilly Media, Inc., 2018.
- 4) Brewer's CAP Theorem. [Електронний ресурс] – Режим доступу: <https://habr.com/ru/post/258145/>.
- 5) Byzantine Fault Tolerance Explained. [Електронний ресурс] – Режим доступу: <https://www.binance.vision/blockchain/byzantine-fault-tolerance-explained>.
- 6) Leslie Lamport Specifying Systems The TLA+ Language and Tools for Hardware and Software Engineers. Pearson Education, Inc, 2003.
- 7) Dilsun K. Kaynar and Nancy Lynch The Theory of Timed I/O Automata. Radboud University Nijmegen, 2005.
- 8) Боев В.Д. Компьютерное моделирование: Пособие для практических занятий, курсового и дипломного проектирования в AnyLogic7. СПб.: ВАС, 2014.
- 9) Калачев О.Н., Синяева А.Н. Имитационное моделирование в Tescomatix Plant Simulation 11 в учебном процессе // CAD/CAM/CAE Observer, 2015.
- 10) Беляева К.С. Розробка засобів верифікації протоколу консенсусу в децентралізованих системах / Беляева К.С., Пенко В.Г. // Інформатика, інформаційні системи та технології: тези доповідей шістнадцятої всеукраїнської конференції студентів і молодих науковців Одеса, 19 квітня 2019р. – Одеса, 2019. – с.61-62.