

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені В. Н. КАРАЗІНА

О. О. Кузнецов
М. О. Полуяненко
О. О. Полуяненко

ПИТАННЯ БЕЗПЕКИ ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМ

КОНСПЕКТ ЛЕКЦІЙ

з дисципліни
«Технології блокчейн»

для студентів
спеціальності 125 «Кібербезпека»

Харків – 2021

УДК 004.031.43

К 89

Рецензенти:

О. В. Лемешко – доктор технічних наук, професор, завідувач кафедри інфокомунікаційної інженерії імені В. В. Поповського Харківського національного університету радіоелектроніки;

О. Г. Толстолузька – доктор технічних наук, старший науковий співробітник, професор кафедри теоретичної та прикладної системотехніки факультету комп'ютерних наук Харківського національного університету імені В. Н. Каразіна.

*Затверджено до друку рішенням Науково-методичної ради
Харківського національного університету імені В. Н. Каразіна
(протокол № 5 від 10 червня 2021 року)*

К 89 **Кузнецов О. О.** Питання безпеки децентралізованих систем : конспект лекцій з дисципліни «Технології блокчейн» для студентів спеціальності 125 «Кібербезпека» / О. О. Кузнецов, М. О. Полуяненко, О. О. Полуяненко. – Харків : ХНУ імені В. Н. Каразіна, 2021. – 36 с.

Реалізація блокчейну пов'язана з низкою проблем, включно із масштабованістю, ефективністю і безпекою. Пошук оптимальних рішень побудови ефективних децентралізованих систем без довіри між учасниками системи, що могли би масштабуватися необмеженим лінійним способом та були б надійними, триває і досі. Третя частина «питання безпеки децентралізованих систем» конспектів лекцій для студентів факультету комп'ютерних наук за спеціальністю «Кібербезпека» присвячена огляду безпеки механізмів та технологій, а також їх обмежень щодо застосувань у блокчейн рішеннях.

УДК 004.031.43

© Харківський національний університет імені В. Н. Каразіна, 2021

© Кузнецов О. О., Полуяненко М. О.,
Полуяненко О. О., 2021

© Дончик І. М., макет обкладинки, 2021

ЗМІСТ

Вступ.....	4
1 Властивості розподіленої системи	5
1.1 Паралельність.....	5
1.2 Нестача глобальних годинників.....	5
1.3 Передача повідомлень.....	6
1.4 Незалежний збій компонентів.....	6
2 Відмовостійкість системи.....	8
3 Технічні обмеження	9
3.1 Брак «технічної» безпеки в асинхронних середовищах.....	9
3.2 Обмежена масштабованість	10
3.3 Обмежена конфіденційність	15
3.4 Обмеження зберігання.....	17
4 Реалізації на мобільних пристроях.....	19
4.1 Сфера застосування.....	20
4.2 Обмеження мобільних платформ	21
4.3 Напрямки рішення обмежень мобільних платформ.....	22
5 Проблема досягнення консенсусу розподіленої системи	24
6 Вимоги до застосування алгоритмів консенсусу	25
7 Рекомендації щодо стандартизації	27
7.1 Серверна частина.....	27
7.2 Клієнтська частина.....	28
7.3 Використання сервера для запуску інших застосунків	28
7.4 Інтерфейс API / протоколи, використовувані для надсилання запиту ..	28
7.5 Сумісність	29
7.6 Структура даних, що зберігаються.....	29
7.7 Методи консенсусу	29
7.8 Аудит	29
7.9 Автентифікація вузла.....	30
7.10 Життєвий цикл вузла	30
7.11 Довгострокове управління даними блокчейну	31
7.12 виправлення помилок у транзакціях	31
7.13 Допоміжні / бічні ланцюжки	32
7.14 Ведення журналу подій	32
7.15 Кібер і мережеві атаки	33
Перелік джерел посилання	34