

Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна

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

**ПРОТОКОЛИ КОНСЕНСУСУ
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. Толстолюзка – 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)*

Кузнецов О. О.

К 89

Протоколи консенсусу 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. – 60 с.

Ключовим аспектом технології блокчейн є визначення того, який вузол публікує наступний блок. Це вирішується шляхом реалізації однієї з багатьох можливих моделей консенсусу. Друга частина – «протоколи консенсусу децентралізованих систем» конспектів лекцій для студентів факультету комп'ютерних наук за спеціальністю «Кібербезпека» присвячена огляду найбільш популярних та перспективних алгоритмів консенсусу. Розглядаються їх переваги та недоліки, сфера застосування, та проводиться їх порівняння.

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

1 Основні поняття та визначення в моделюванні консенсусу децентралізованих систем.....	5
2 Протокол консенсусу відповідно до моделі «Доказ виконаної роботи» (PoW).....	9
2.1 Історія появи	10
2.2 Опис моделі консенсусу PoW	12
2.3 Протокол GHOST	15
2.4 Протоколи SPECTRE і PHANTOM.....	17
2.5 Переваги PoW	18
2.6 Недоліки PoW	18
2.7 Атаки на алгоритм консенсусу PoW	20
3 Протокол консенсусу відповідно до моделі «Доказ частки володіння» (PoS)	20
3.1 Опис моделі консенсусу PoS	21
3.2 Візантійський відмовостійкий доказ частки (BFTPoS).....	22
3.3 Доказ віку монет (CAPoS)	22
3.4 Орендований доказ частки володіння (LPoS).....	23
3.5 Делегований доказ частки володіння (DPoS).....	23
3.6 Ієрархічний делегований PoS (HDPoS)	24
3.7 Протокол досягнення консенсусу Ouroboros	25
3.8 Перевага PoS	27
3.9 Недоліки PoS.....	27
4 BFT-протоколи	28
4.1 Опис моделі консенсусу BFT	28
4.2 Practical BFT.....	30
4.3 HoneyBadger BFT.....	31
4.4 Algorand.....	31
4.5 HashGraph.....	32
4.6 Делегований BFT-протокол (DBFT)	33
4.7 Федеративна візантійська угода (FBA)	33
4.8 Переваги BFT.....	34
4.9 Недоліки BFT.....	34

5	Протоколи консенсусу відповідно до кругової моделі (Round Robin)	35
6	Протоколи консенсусу з альтернативними моделями доказу	37
6.1	Доказ володінням простору (PoSpace)	37
6.2	Доказ ресурсів (PoCapacity)	37
6.3	Доказ розташування (PoL)	37
6.4	Доказ важливості (PoI)	38
6.5	Доказ витраченого часу (PoET)	39
6.6	Доказ активу (PoAsset)	40
6.7	Доказ авторитету (PoAuthority) або Доказ ідентичності (PoIdentity)	41
6.8	Доказ мозкової діяльності (PoBrain)	42
6.9	Доказ внеску (PoCo)	43
6.10	Доказ спалювання (PoBurn)	43
7	Гібридні моделі консенсусу	44
7.1	Доказ активності (PoActivity)	44
7.2	Алгоритм «Обмеження довіри» (LC)	45
7.3	Доказ активності з обмеженою довірою (LCPoA)	46
8	Порівняння протоколів консенсусу децентралізованих систем	47
	Перелік джерел посилання	54