



# БЛОКЧЕЙН

## І ДЕЦЕНТРАЛІЗОВАНІ СИСТЕМИ

ЧАСТИНА 2

Distributed Lab

УДК 004.738.5:336]:007-057.21](07)  
К78

Рекомендовано Вченою радою  
Харківського національного університету радіоелектроніки  
(протокол засідання №9 від 24 жовтня 2019 року)

*Рецензенти:*

*Р. В. Олійников* – доктор технічних наук, професор кафедри безпеки інформаційних технологій ХНУРЕ, ведучий дослідник у ІОНК.

*О. О. Кузнецов* – доктор технічних наук, професор кафедри безпеки інформаційних систем і технологій ХНУ ім. В. Н. Каразіна.

*Л. В. Ковальчук* – доктор технічних наук, професор кафедри математичних методів захисту інформації НТУУ КПІ.

*М. О. Полуяненко* – кандидат технічних наук, доцент кафедри безпеки інформаційних систем і технологій ХНУ ім. В. Н. Каразіна.

*Автори:*

П. Кравченко, Б. Скрябін, О. Курбатов, О. Дубініна

**Кравченко П.**

К78 Блокчейн і децентралізовані системи: навч. посібник для студ. закладів вищ. освіти: в 3 частинах. Ч. 2 / П. Кравченко, Б. Скрябін, О. Курбатов, О. Дубініна. - Харків: ПРОМАРТ, 2018. – 412 с. : рис. 256; табл. 17; бібліогр.: 78 назв.

ISBN 978-617-7634-40-8

ISBN 978-617-7634-63-7 (ч. 2)

Запропонований навчальний посібник присвячений децентралізованим технологіям, які стали популярні завдяки поширенню криптовалют. Спочатку автори акцентують увагу на технічних і фундаментальних аспектах криптовалют, технології блокчейн і рівні додатків, надаючи читачеві можливість глибоко розібратися в основах. Особливість книги полягає в тому, що матеріал викладено на стику принципів роботи, переваг і ризиків інноваційних інформаційних технологій.

Видання розраховане на широку аудиторію: наукових працівників, викладачів, аспірантів, студентів, які мають базові знання в області криптографії та інформаційних технологій, – всіх, кого цікавлять питання децентралізованих технологій.

УДК 004.738.5:336]:007-057.21](07)

ISBN 978-617-7634-63-7 (ч. 2)  
ISBN 978-617-7634-40-8

© Кравченко П., Скрябін Б.,  
Курбатов О., Дубініна О., 2019

# ЗМІСТ

ВСТУП.....	14
ПРО DISTRIBUTED LAB.....	16
1 ДЕЦЕНТРАЛІЗАЦІЯ ЯК ПІДХІД У ІНФОРМАЦІЙНИХ СИСТЕМАХ .....	18
1.1 Пірінгові мережі та протокол BitTorrent.....	18
Традиційна клієнт-серверна архітектура .....	18
Принципи побудови однорангової файлообмінної мережі.....	20
Історія розвитку BitTorrent .....	21
Як працює BitTorrent.....	22
Розбиття даних на фрагменти .....	25
Обмеження протоколу .....	26
1.2 Принцип роботи та застосування DHT .....	29
Завдання, які вирішує Distributed Hash Table .....	29
Як працює DHT?.....	30
Проблема блокування контенту зловмисником .....	34
1.3 Концепція web-of-trust .....	36
Поняття сертифікату відкритого ключа .....	36
Як працює ієрархічна ІВК .....	37
Принципи функціонування web-of-trust.....	42
Приклад з італійською мафією.....	44
Переваги та обмеження технології web-of-trust .....	46
1.4 Протокол BitMessage.....	50
Принципи функціонування протоколу.....	50

---

Адреси в BitMessage .....	52
Структура повідомлень в BitMessage .....	54
Типи повідомлень в BitMessage .....	55
Поняття stream в BitMessage.....	56
1.5 Архітектура й особливості протоколу IPFS .....	58
Основні принципи протоколу.....	59
Як працює IPFS .....	60
Використання IPFS .....	64
Filecoin .....	65
Алгоритм досягнення консенсусу в Filecoin.....	66
Переваги протоколу Filecoin.....	67
2 КРИПТОГРАФІЯ В ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ.....	69
2.1 Генерація та обробка ключових даних .....	69
Основні функції ключів .....	69
Життєвий цикл ключа .....	71
Принципи генерації ключів .....	72
Генератори випадкових послідовностей .....	72
Генератори псевдовипадкових послідовностей.....	73
Тестування генераторів випадкових та псевдовипадкових послідовностей .....	75
Функції породження ключів (KDF) .....	78
2.2 Протоколи обміну ключами .....	80
Протокол Діффі-Хеллмана .....	83
Протокол Діффі-Хеллмана на еліптичних кривих .....	85

---

Протокол ЕКЕ.....	86
2.3 Концепція та застосування Merkle tree.....	89
Структура дерев Меркла.....	89
Побудова дерева Меркла.....	91
Автентифікація в дереві Меркла.....	93
Галузі застосування Merkle Tree.....	95
2.4 Різновиди цифрових підписів.....	98
Схеми одноразового підпису.....	99
Lamport one time signature.....	99
Чому одноразовий підпис "одноразовий"?.....	101
Winternitz one time signature.....	103
Мультипідпис.....	105
Пороговий підпис.....	107
Груповий підпис.....	108
Кільцевий підпис.....	110
Сліпий підпис.....	113
3 ТЕХНОЛОГІЧНІ ДЕТАЛІ ФУНКЦІОНУВАННЯ BITCOIN.....	117
3.1 Будова й особливості Bitcoin Script.....	117
Як виконується Bitcoin Script?.....	119
Операції в Bitcoin Script.....	121
Приклад виконання Bitcoin Script для P2PKH.....	122
Приклад з multisignature.....	125
Використання механізму locktime.....	128
Нестандартні транзакції за допомогою Bitcoin Script.....	129

---

Статистика транзакцій в мережі Bitcoin.....	130
3.2 Формати ключів у Bitcoin .....	133
Поняття стиснутого відкритого ключа .....	134
Формати особистих ключів.....	135
Формати відкритих ключів .....	138
3.3 Формати серіалізації транзакцій і блоків у Bitcoin.....	140
Серіалізація bitcoin-транзакції.....	140
Серіалізація блоку в Bitcoin .....	145
3.4 Як вузли мережі Bitcoin обмінюються повідомленнями .....	147
Ролі вузлів в мережі Bitcoin .....	148
Поточний стан мережі Bitcoin .....	154
Структура повідомлень в Bitcoin .....	158
Протокол поширення інформації.....	159
Початок роботи вузла в мережі Bitcoin .....	160
Протокол поширення інформації Flooding.....	161
Diffusion – розширення Flooding.....	163
Приклади проблем в протоколах і їх рішення .....	163
3.5 Testnet і складнощі оновлення протоколу .....	170
Testnet в Bitcoin і його призначення .....	170
Оновлення протоколу.....	171
Найбільш значні оновлення протоколу Bitcoin .....	173
Адаптація нових версій Bitcoin серед вузлів .....	174
3.6 Основні класи атак на Bitcoin .....	176
Flood-атака і механізм захисту .....	177

---

Spam-атака та її наслідки .....	177
Призупинення підтвердження нових транзакцій (DoS) .....	178
Long-range атака .....	179
Routing attacks .....	180
Інші технічні і соціальні атаки .....	184
Bitcoin alert system і відмова від неї.....	185
Деякі з виявлених і вирішених проблем протоколу.....	187
<b>4 BITCOIN ЯК ПЛАТФОРМА .....</b>	<b>191</b>
<b>4.1 Як працюють sidechains .....</b>	<b>191</b>
One-way peg and two-way peg sidechains .....	193
Federated sidechains.....	194
Merged-mined sidechains.....	195
Недоліки sidechains.....	197
Висновки .....	198
<b>4.2 Будова Lightning Network .....</b>	<b>199</b>
Будова двостороннього платіжного каналу .....	199
Відкриття платіжного каналу .....	201
Передача монет в рамках каналу .....	205
Механізм штрафування за шахрайство в каналі .....	207
Закриття платіжного каналу .....	210
Як Lightning Network використовує платіжні канали .....	212
Переваги та недоліки Lightning Network.....	223
<b>4.3 Принципи роботи і застосування atomic swap.....</b>	<b>225</b>
Як працюють централізовані біржі?.....	226

---

Ідея atomic swaps і вимоги до облікової системи .....	228
Принципи роботи atomic swaps .....	229
Обмеження atomic swaps .....	236
Застосування atomic swaps децентралізованими біржами.....	237
Проблема Panic Sells.....	239
5 МЕТОДИ ДОСЯГНЕННЯ КОНСЕНСУСУ .....	241
5.1 Proof-of-stake алгоритми досягнення консенсусу.....	241
Принцип роботи та переваги proof-of-stake .....	241
Peercoin .....	243
Nxt .....	244
NEM.....	245
Ouroboros .....	246
Ouroboros Praos .....	248
Ouroboros Genesis.....	248
Основні недоліки та ризики при використанні proof-of-stake .....	249
Атака nothing-at-stake .....	250
Атака попереднього обчислення.....	253
Атака fake stake .....	253
Атака накопиченням віку монет.....	254
Short-range атаки .....	254
Long-range атаки .....	254
5.2 Delegated proof-of-stake як алгоритм досягнення консенсусу .....	255
Алгоритм DPoS .....	256
Як запускається облікова система, яка використовує DPoS .....	259



---

Як працює DPoS .....	259
5.3 Алгоритми, що належать до BFT-класу .....	263
Practical BFT algorithm .....	263
Процес досягнення консенсусу .....	268
HotStuff як алгоритм досягнення консенсусу .....	273
5.4 FBA як підхід до досягнення консенсусу .....	278
Поняття quorum, quorum slice і quorum intersection .....	278
Blocking set .....	280
Disjoint quorums і divergent state .....	280
Federated Voting .....	281
Застосування FBA в Stellar .....	283
Проблема централізації .....	286
Рівень децентралізації мережі Stellar .....	287
FBA в порівнянні з іншими алгоритмами досягнення консенсусу ..	289
5.5 Hashgraph .....	289
Принцип роботи hashgraph .....	291
Створення події .....	291
Поширення події .....	292
Підтвердження події .....	295
<b>6 МЕТОДИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ В СУЧАСНИХ ОБЛІКОВИХ СИСТЕМАХ .....</b>	<b>309</b>
6.1 Стандарти CryptoNote .....	309
Підписи в стандарті CryptoNote .....	309
Зв'язок ключів і адрес .....	311

---

Stealth addresses .....	312
Механізм захисту від подвійної витрати .....	314
Структура блоків в CryptoNote .....	316
Структура транзакцій в CryptoNote .....	319
6.2 MimbleWimble .....	322
Модель транзакцій MimbleWimble .....	324
Докази діапазону .....	328
Всі етапи проходження транзакції .....	329
Перевірка і поширення транзакції .....	331
Відсутність адрес .....	332
Метод cut-through .....	332
Структура транзакції і блоку .....	334
6.3 Вступ до zk-SNARKs .....	335
Принципи гомоморфного шифрування .....	335
Трохи про поліноми і їх blind evaluation .....	337
Algebraic circuit .....	338
Rank-1 constraint system (R1CS) .....	339
Quadratic arithmetic programs .....	343
Спрощений протокол перевірки знання .....	347
7 РОЗВИТОК ДЕЦЕНТРАЛІЗОВАНИХ ТЕХНОЛОГІЙ .....	349
7.1 Будова протоколу Bitshares .....	349
Призначення платформи Bitshares .....	349
Модель акаунтів .....	350
Модель транзакцій .....	350

---

Децентралізований обмін активами .....	352
Гнучкість управління акаунтами .....	352
Емісія UIA .....	354
Механізм голосувань.....	355
Механізм комісій.....	355
SmartCoins .....	356
Формат заголовка блоку .....	357
Множина операцій і особливості їх виконання.....	357
Організація бази даних .....	359
Оптимізація виконання бізнес-логіки .....	360
Опції підвищення конфіденційності користувачів .....	361
7.2 Платформа Ethereum і смарт-контракти.....	362
Особливості роботи платформи Ethereum .....	363
Створення акаунтів в Ethereum .....	363
Повідомлення виклику в Ethereum. ....	365
Комісійні збори і gas .....	365
Структура транзакції в Ethereum .....	366
Обробка транзакцій .....	368
Структура блоку Ethereum.....	369
Ethereum virtual machine.....	370
Приклад вихідного коду смарт-контракту.....	370
Виконання контракту на платформі Ethereum.....	372
Обмеження платформи Ethereum.....	374
Недоліки платформи Ethereum.....	375

---

ВИСНОВОК .....	379
ТЕСТОВІ ЗАПИТАННЯ З ВАРІАНТАМИ ВІДПОВІДЕЙ.....	381
СЛОВНИК ТЕРМІНІВ .....	393
ПОДЯКИ.....	403
ПРО АВТОРІВ .....	404
ВИКОРИСТАНІ ДЖЕРЕЛА ТА ПОСИЛАННЯ .....	406