

П. КРАВЧЕНКО, Б. СКРЯБІН, О. ДУБІНІНА



БЛОКЧЕЙН І ДЕЦЕНТРАЛІЗОВАНІ СИСТЕМИ

ЧАСТИНА 1

Distributed Lab

УДК 004.9:512.624.95:336.76
К78

Рекомендовано Вченою радою Харківського національного
університету радіоелектроніки
(протокол засідання №1 від 22 лютого 2019 року)

Рецензенти:

Р. В. Олійников – доктор технічних наук, професор кафедри безпеки інформаційних систем і технологій ХНУ ім. В. Н. Каразіна, провідний дослідник в ІОНК;

І. Д. Горбенко – доктор технічних наук, професор кафедри безпеки інформаційних систем і технологій ХНУ ім. В. Н. Каразіна, академік Академії наук прикладної радіоелектроніки.

О. Г. Оксіюк – доктор технічних наук, професор, завідувач кафедри кібербезпеки та захисту інформації факультету інформаційних технологій КНУ ім. Т. Г. Шевченка.

С. В. Васілю – доктор технічних наук, професор, директор навчально-наукового інституту Радіо, телебачення та інформаційної безпеки ОНАЗ ім. О. С. Попова.

Автори:

П. Кравченко, Б. Скрябін, О. Дубініна

Кравченко П.

К78 Блокчейн і децентралізовані системи : навч. посібник для студ. закладів вищ. освіти : в 3 частинах. Ч. 1 / П. Кравченко, Б. Скрябін, О. Дубініна. – Харків : ПРОМАРТ, 2019. – 452 с. : іл. 191; табл. 13; бібліогр.: 124 назв.

ISBN 978-617-7634-39-2

ISBN 978-617-7634-40-8 (ч. 1)

Запропонований навчальний посібник присвячено децентралізованим технологіям, які стали широко популярні завдяки розповсюдженню криптовалют. На початку автори акцентують увагу на технічних і фундаментальних аспектах криптовалют, технології блокчейн і рівні додатків, надаючи читачу можливість глибоко розібратися в основах. Особливість книги полягає в тому, що матеріал викладений на стику принципів роботи, переваг і ризиків інноваційних інформаційних технологій.

Видання розраховано на наукових працівників, викладачів, аспірантів, студентів спеціальностей «Кібербезпека», «Комп'ютерні науки», «Системний аналіз», «Інформаційні системи та технології», «Комп'ютерна інженерія», «Інженерія програмного забезпечення».

УДК 004.9:512.624.95:336.76

ISBN 978-617-7634-40-8 (ч. 1)
ISBN 978-617-7634-39-2

© Кравченко П., Скрябін Б.,
Дубініна О., 2018

7 847 14

Зміст

ВСТУП	9
ПРО DISTRIBUTED LAB.....	12
1. ДЕЦЕНТРАЛІЗАЦІЯ В ІНФОРМАЦІЙНИХ СИСТЕМАХ	14
1.1 Що таке децентралізація?	14
Поняття децентралізації для інформаційних систем	15
Відмінність децентралізованих систем від систем з резервуванням.....	15
1.2 Історія децентралізованих систем	16
Децентралізовані файлообмінні системи	17
Децентралізовані системи передачі даних	19
Децентралізовані обчислювальні системи	19
Децентралізовані системи зберігання даних	20
Децентралізовані системи прийняття рішень	21
Децентралізовані платіжні системи.....	23
1.3 Застосування принципів децентралізації.....	24
Обмеження та проблеми централізованих систем	24
Застосування децентралізованого підходу.....	26
Принципи побудови децентралізованих систем	27
Типова архітектура децентралізованих систем	30
Обмеження децентралізованих систем	32
Фактори, що вповільнюють впровадження децентралізованих систем.....	33
Висновки	37
2. ІСТОРІЯ ТА ПРИНЦИПИ ФУНКЦІОНУВАННЯ BITCOIN.....	39
2.1 Що таке Bitcoin?.....	39
Історія виникнення Bitcoin.....	41
Проблеми, які здатний вирішити Bitcoin	43
Головні принципи функціонування Bitcoin	45
Емісія в Bitcoin	46
Формування ціни на монети.....	49
Поняття довіри в Bitcoin	52
Обмеження технології Bitcoin	53
Значення децентралізації для Bitcoin.....	54
2.2 Як застосовувати Bitcoin?	56
Ключі у Bitcoin	57
Транзакції в Bitcoin.....	57
Програмні гаманці	58
Апаратні гаманці	59
Централізовані сховища.....	61
Резервне копіювання гаманців	62
2.3 Поняття транзакції у Bitcoin	65

Що таке Bitcoin-транзакція?.....	66
Перевірка транзакцій	68
Поняття комісії у Bitcoin.....	71
Поняття конфліктуючих транзакцій	72
2.4 Високорівнева архітектура Bitcoin.....	74
Архітектура системи з технологією blockchain.....	74
Процеси в обліковій системі Bitcoin.....	76
Ролі учасників в обліковій системі Bitcoin	77
Умови, за яких досягається консенсус у Bitcoin	77
Як досягається консенсус в Bitcoin?.....	79
Порівняння Bitcoin з традиційними платіжними системами	80
2.5 Підтвердження транзакцій у Bitcoin	83
Формування блоків транзакцій.....	83
Вимоги до нових блоків	85
Принципи змагання між користувачами.....	86
Розповсюдження блоку	87
Вирішення розбіжностей	88
Поняття повного підтвердження транзакції.....	90
Винагороди за створення блоків	91
Вплив розривів мережі на облікову систему Bitcoin	93
3. ВСТУП ДО КРИПТОГРАФІЇ ТА УПРАВЛІННЯ КЛЮЧАМИ.....	100
3.1 Вступ до криптографії.....	100
Принципи криптографічного захисту інформації	100
Поняття ключів.....	102
Модель загроз та порушника.....	103
Генерація та обробка секретних ключів	107
Поняття однонаправленої функції та NP-повної задачі.....	109
Геш-функція	111
Застосування геш-функцій	115
Дерева Меркла.....	115
Симетричне шифрування	117
Асиметрична криптографія	120
3.2 Криптографія у Bitcoin	122
Особливості роботи еліптичних кривих	122
Створення біткоїн-адрес	124
Конфіденційність в Bitcoin.....	125
3.3 Зберігання й обробка ключів	129
Головна задача цифрового гаманця.....	129
Основні підходи до синхронізації гаманця	130
Обробка та зберігання ключів на сервері.....	131
Ключі на сервері, але доступ до них тільки у клієнта	133
Ключі на пристрої користувача.....	134
Зберігання монет із застосуванням мультипідпису.....	136

Холодні, теплі та гарячі гаманці.....	137
4. ТЕХНОЛОГІЧНІ ДЕТАЛІ ФУНКЦІОНУВАННЯ BITCOIN.....	141
4.1 Як працюють транзакції в Bitcoin?.....	141
Структура транзакції	141
Unspent Transaction Outputs (UTXOs)	146
Отримання решти та встановлення комісії	147
Схема передачі монет на прикладі	148
Формування транзакцій у bitcoin-гаманцях	150
Механізм LockTime	154
Off-chain протоколи	155
Signature hash types	157
Запис довільних даних до ланцюга блоків.....	158
Висновки	161
4.2 Майнінг у Bitcoin	166
Поняття і цілі майнінгу в Bitcoin.....	166
Класифікація вузлів мережі.....	167
Поняття ресурсомісткого завдання.....	168
Обмеження частоти формування блоків	171
Orphan blocks	171
Атака подвійної витрати	173
Поява спеціального обладнання	177
Майнінгові пули та їх завдання	179
Статистика майнінгу і оцінка енергоспоживання	182
4.3 Як реалізований blockchain у Bitcoin	187
Структура блоку	189
Приклади блоків у Bitcoin.....	191
Поняття Mempool у Bitcoin	193
Життєвий цикл блоку.....	194
Початкова синхронізація вузла	197
Checkpoints	199
Властивості спільної бази даних Bitcoin.....	200
4.4 Підходи до синхронізації з мережею та SPV-вузол	204
Складнощі роботи у розподіленій мережі	206
Підходи до синхронізації гаманця з платіжною мережею	207
Робота з повним вузлом мережі	207
Робота з довіреним вузлом мережі	208
Робота з SPV-вузлами	210
Функціонування SPV-вузла	212
Висновки	214
4.5 Механізм мультипідпису та Bitcoin Script.....	218
Bitcoin-транзакція, яка використовує мультипідпис	219
Варіант мультипідпису 2-3-2.....	220
Варіант мультипідпису 2-3-3	223

Переваги Wallet-сервісів із мультипідписом 2-3-3	226
Знайомство з Bitcoin Script	227
Концепція P2SH-адрес і переваги їх використання	228
Приклад використання P2SH для MultiSig-адреси	231
4.6 Особливості оновлення Segregated Witness	233
Збільшення пропускнуої здатності та зворотна сумісність	235
Нововведення Segregated Witness	237
Приклад SegWit-транзакції	240
Нові поняття ваги і розміру	242
Статистика адаптації оновлення	244
4.7 Механізм комісій у Bitcoin	246
Волатильність ціни запису даних	249
Рішення проблеми з волатильністю комісій	249
Підвищення комісії після відправки транзакції	250
Як Segregated Witness допомагає знизити комісії	252
Варіант із другом-майнером	253
Варіант із продажем місць у черзі на підтвердження	254
4.8 Платіжні канали та Lightning Network	256
Що таке платіжний канал?	256
Чому потрібні платіжні канали?	257
Платіжний канал: приклад крок за кроком	258
Особливості платіжного каналу	260
Методи реалізації платіжних каналів	260
Spillman-style payment channels	261
Застосування платіжних каналів	265
Особливості роботи мережі Bitcoin та Lightning Network	265
Як працює Lightning Network	267
5. ТЕХНОЛОГІЯ BLOCKCHAIN	275
5.1 Технологія blockchain та її можливості	275
Ступені децентралізації	277
Архітектура blockchain	280
Властивості блокчейна	281
Застосування технології блокчейн	283
Висновки	288
5.2 Відмінності підходів до досягнення консенсусу	292
Механізм досягнення консенсусу як ключовий елемент децентралізованої системи обліку	292
Proof-of-work	294
Proof-of-stake	294
Delegated proof-of-stake	295
Proof-of-importance	296
BFT	296
FBA	298

Протоколи досягнення консенсусу, що базуються на DAG	299
Основні критерії класифікації механізмів досягнення консенсусу	300
Висновки	302
5.3 Обмеження технології blockchain і складнощі її застосування	304
Упровадження digital identity	305
Дигіталізація всіх процесів	306
Прийняття єдиних правил обробки даних	306
Перенесення всіх цифрових активів до однієї облікової системи	307
Організація децентралізованого прийняття рішень	307
Обмеження пропускної здатності	308
Обмеження часу підтвердження транзакції	309
Проблема управління (governance)	310
Розподілена відповідальність	311
Проблема оновлення протоколу	312
Висновки	313
6. РОЗВИТОК ДЕЦЕНТРАЛІЗОВАНИХ ТЕХНОЛОГІЙ	314
6.1 Відгалуження та клони Bitcoin	314
Сплановані форки	315
Методи оновлення програмного забезпечення: softfork і hardfork	318
Незапланований softfork у Bitcoin	320
Поняття спланованих форків	321
Приклади спланованих форків Bitcoin	322
6.2 Альтернативні цифрові валюти та токени	326
Що таке криптовалюта?	326
Litecoin	327
Dash	328
Відмінність алгоритмів майнінгу Litecoin, Dash і Bitcoin	329
NXT	330
BitShares	331
Monero	331
Ethereum	333
Cardano	334
Ripple і Stellar	334
ZCash	335
Інші цифрові валюти	336
Токени	338
Висновки	339
6.3 Вступ до смарт-контрактів	343
Що таке смарт-контракт?	346
Роль оракулів для смарт-контрактів	348
Приклад із купівлею в онлайн-магазині	350
Приклад контракту для спільної купівлі	352
Класифікація платформ смарт-контрактів	354

Відмінність платформ за середовищем виконання	354
Відмінність платформ за способом виконання контрактів	356
Відмінність платформ за способом ініціювання контрактів	357
Висновки	358
6.4 Вступ до токенизації активів	360
Проблеми існуючих облікових систем	363
Що таке платформа токенизації?	364
Принципи функціонування платформи токенизації	366
Можливості, які надає токенизація	367
Прозорість процесів облікової системи	368
Як токенизація приводить до збільшення вартості активів?	368
Умови ефективного застосування платформ токенизації	369
Ризики	370
Відмінність токенизації від оцифровки	370
Чому саме blockchain технологія?	371
Висновки	371
7. КОНФІДЕНЦІЙНІСТЬ КОРИСТУВАЧІВ У ВІДКРИТИХ СИСТЕМАХ	374
7.1 Поняття приватності у цифровому світі	374
Важливість збереження приватності	374
Складові приватності	376
7.2 Конфіденційність у цифрових валютах	378
Blind Signatures	379
Конфіденційність в Bitcoin за замовчуванням	380
CoinJoin	381
Chaumian CoinJoin	383
CoinShuffle	385
Недоліки методу CoinJoin	388
Концепція zero-knowledge proof	389
Confidential Transactions	392
Ring Confidential Transactions	393
MimbleWimble	394
Stealth Addresses	396
Концепція гомоморфного шифрування	397
ЗАКЛЮЧЕННЯ	399
ТЕСТОВІ ПИТАННЯ З ВАРІАНТАМИ ВІДПОВІДЕЙ	401
СЛОВНИК ТЕРМІНІВ	426
ПОДЯКИ	437
ПРО АВТОРІВ	438
ВИКОРИСТАНІ ДЖЕРЕЛА ТА ПОСИЛАННЯ	439