П. КРАВЧЕНКО, Б. СКРЯБІН, О. ДУБІНІНА

# БЛОКЧЕЙН І ДЕЦЕНТРАЛІЗОВАНІ СИСТЕМИ

ЧАСТИНА 1

Distributed Lab

DISTRIBUTED LAB

П. Кравченко, Б. Скрябін, О. Дубініна

# БЛОКЧЕЙН І ДЕЦЕНТРАЛІЗОВАНІ СИСТЕМИ

**Навчальний посібник для студентів закладів вищої освіти**

*Видання в авторській редакції*

У трьох частинах

**Частина 1**

Харків
2019

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.

*Є. В. Васіліу* – 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



# Зміст

# ВСТУП

З появою Інтернету світ почав стрімко змінюватися, до того ж темп змін постійно зростає. Децентралізація в інформаційних системах стала не просто черговою віхою технологічної еволюції, як це було у випадку з появою рідинно-кристалічних моніторів і відмовою людей від звичних моніторів з електронно-променевою трубкою; вона пропонує кардинально новий підхід, який здатен змінити принципи людської взаємодії. Це особливо помітно, коли йдеться про політичний устрій чи забезпечення довіри до систем обліку фінансів.

Устрій традиційних облікових систем не дозволяє користувачам бути впевненими у цілісності та достовірності отриманих даних – усе, що залишається, це довіряти. У сучасному світі користувачі все частіше хочуть *не просто довіряти, а мати можливість перевірити.*

Зацікавленість в прозорих облікових системах стала особливо високою після появи цифрових платіжних систем, які висували суворі вимоги до часу підтвердження і безпеки транзакцій. Побічним ефектом підвищення продуктивності стала сильна централізація та повна непрозорість таких систем, що позначилося на житті цілих груп людей і навіть країн. Можливість відключення від платіжних систем використовується як важіль політичного тиску, непрозорість систем знижує довіру і обмежує вільну конкуренцію, а доступ до історії транзакцій тільки для обмеженого кола організацій дозволяє контролювати життя людей.

До появи Bitcoin всі фінансові системи були закритими і захищалися «традиційними» методами: за допомогою фаєрволів, систем контролю доступу тощо. Поява Bitcoin показала, що фінансова система може не тільки існувати без єдиного центру прийняття рішень, але також бути прозорою для *всіх* та дозволяти проводити її аудит, при цьому забезпечуючи приватність платежів користувачів та гарантуючи за допомогою математики надійну роботу за заданими правилами.

Принципи та архітектура Bitcoin можуть бути застосовані для вирішення широкого класу задач, починаючи від голосування та

взаєморозрахунків до управління ланцюгами поставок товарів. Блокчейн як спосіб спільної обробки інформації стає інструментом, що дозволяє проектувати надійні та прозорі облікові системи.

Багато технологій, які розглядаються в цьому навчальному посібнику, або винайдені, або вперше широко застосовані в Bitcoin. Тому було прийнято рішення приділити особливу увагу саме йому. При цьому Bitcoin буде розглянутий не стільки в контексті фінансового або інвестиційного інструменту, скільки в якості прикладу реалізації *децентралізованої облікової системи*.

Основною метою, яку ставлять перед собою автори, є донесення принципів роботи децентралізованих систем в аспекті прийняття рішень, зберігання даних, управління безпекою, довіреного аудиту та забезпечення приватності. Розуміння цих принципів, на наш погляд, дозволить читачеві детальніше розібратися в децентралізованих технологіях, зогранізує їх розуміння та стане дороговказом в океані різних протоколів і систем. Для досягнення мети були здійснені наступні кроки:

- кожен розділ містить визначення та контекст, в межах якого оперують розглянуті системи;
- фокус уваги зосереджений у першу чергу на питанні, *чому* так працює та чи інша технологія (з прикладами застосування);
- принципи роботи пояснюються на реальних прикладах з мінімально необхідною кількістю технічних деталей;
- матеріал викладений за допомогою ілюстрацій, схем та діаграм;
- технічні концепції пояснюються на прикладах з життя;
- наводяться поширені міфи та їх спростування;
- наводяться відповіді на найбільш поширені питання;
- для контролю засвоєння знань розроблені тести.

Аудиторією для даного посібника є читачі зі знаннями в області побудови комп'ютерних систем і мереж, починаючи з базового рівня. За допомогою цієї книги ми маємо наміри підготувати читача до





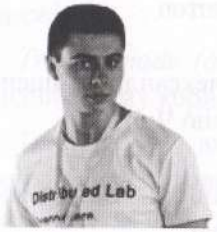
розуміння суті наступаючої ери цифрової економіки. Теми, що розглядаються, ретельно підібрані і дозволяють людині, яка бажає створювати інновації, отримати вичерпну оцінку найбільш важливих технологій. У деяких місцях книги представлений текст вельми технічного характеру, та ми розуміємо, що деякі моменти у змісті таких ділянок можуть виявитися не достатньо зрозумілими для читачів без технічної освіти. Однак ми спробували збалансувати рівень складності викладеного матеріалу за допомогою ілюстрацій та узагальнюючих висновків.

Основою для написання навчального посібника став курс лекцій, спочатку створений Павлом Кравченком у 2014 році для студентів у галузі інформаційної безпеки. Пізніше матеріал курсу допрацював Богдан Скрябін до онлайн-версії. Дидактичний аспект розроблений Оксаною Дубініною. На момент завершення роботи над даною книгою курс був прочитаний 15 разів в університетах Харкова, Одеси та Хайфи.

# ПРО АВТОРІВ

**Павло Кравченко**

Засновник компанії Distributed Lab. Галузь наукових досліджень: блокчейн і децентралізовані технології. Галузь експертизи: криптографія, інфраструктура відкритих ключів, токенізація активів, моделі безпеки, архітектура децентралізованих систем. Кандидат технічних наук у галузі інформаційної безпеки, автор 15 наукових робіт, з яких 5 присвячено технології блокчейн і децентралізованим системам. З 2014 року почав свою діяльність у галузі створення децентралізованих облікових систем як криптограф у проекті Stellar.



**Богдан Скрябін**

Провідний спеціаліст із криптографії та децентралізованих систем у Distributed Lab. Галузь наукових досліджень: протоколи децентралізованих облікових систем, архітектура програмних гаманців, криптографічні схеми, конфіденційність у цифрових валютах. З 2014 року залучений до індустрії децентралізованих технологій і блокчейн. Захистив магістерську роботу з теми «Аналіз вразливостей децентралізованих платіжних систем». Провів 9 академічних курсів і факультативів у вищих навчальних закладах технічного профіля.

**Оксана Дубініна**

Професор кафедри комп'ютерної математики та аналізу даних факультета комп'ютерних наук і програмної інженерії Національного технічного університету «Харківський політехнічний інститут». Галузь наукових досліджень: математичний апарат у Software Engineering, дидактичний простір комп'ютингу, математичне моделювання. Кандидат технічних наук, доктор педагогічних наук у галузі професійної освіти (IT-галузь). Автор 75 наукових і навчально-методичних праць.



# ВИКОРИСТАНІ ДЖЕРЕЛА ТА ПОСИЛАННЯ


1. Online Browsing Platform [Електронний ресурс]. – Режим доступу: https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en.
2. Usenet: A Bulletin Board for Unix Users // BYTE. – 8(10) January 1983. – P. 219–236.
3. Bhushan A. A File Transfer Protocol [Електронний ресурс] / A. Bhushan. – April 1971. – Режим доступу: https://www.rfc-editor.org/rfc/pdfrfc/rfc114.txt.pdf.
4. Hauben R. From the ARPANET to the Internet : A Study of the ARPANET TCP/IP Digest and of the Role of Online Communication in the Transition from the ARPANET to the Internet [Електронний ресурс] / Ronda Hauben. – Режим доступу: http://www.columbia.edu/~rh120/other/ tcpdigest_paper.txt.
5. Huckle S. Internet of Things, Blockchain and Shared Economy Applications / S. Huckle, R. Bhattacharya, M. White, N. Beloff // Procedia Comput. Science. – 2016. – Вид. 98. – с. 461–466.
6. Dingledine R. Tor: The second-generation onion router [Електронний ресурс] / Roger Dingledine, Nick Mathewson, Paul Syverson. – Режим доступу: https://www.freehaven.net/anonbib/cache/draft-tor-design-2004.pdf.
7. Cjdns [Електронний ресурс]. – Режим доступу: https://github.com/cjdelisle/cjdns/blob/master/doc/Whitepaper.md.
8. Chris O'Brien. Open Garden uses FireChat in Tahiti to create cell phone network that eliminates need for carriers. (October 20, 2015). [Електронний ресурс]. – Режим доступу: https://venturebeat.com/2015/10/20/open-garden-uses-firechat-in-tahiti-to-create-a-cell-phone-network-that-eliminates-need-for-carriers.
9. Foster I. The Grid: Blueprint for a new computing infrastructure / Foster Ian, Kesselman Carl. – San Francisco, CA, USA : Morgan Kaufmann Publishers Inc., 1999. – 677 p.
10. SETI@home [Електронний ресурс]. – Режим доступу: https://

setiathome.berkeley.edu/.

11. IPFS is the Distributed Web [Електронний ресурс]. – Режим доступу: https://ipfs.io.
12. PCI DSS Quick Reference Guide [Електронний ресурс]. – October 2010. – Режим доступу: https://www.pcisecuritystandards.org/documents/ PCI%20SSC%20Quick%20Reference%20Guide.pdf.
13. Ланкин В. Е. Децентрализация управления социально-экономическими системами (системный аспект) : монография / В. Е. Ланкин. – Таганрог : Изд-во ТРТУ, 2005. – 228 с.
14. Baran P. On distributed communications: I. Introduction to distributed communications networks [Електронний ресурс] / Paul Baran. – Aug. 1964. – Режим доступу: https://www.rand.org/content/dam/rand/pubs/ research_memoranda/2006/RM3420.pdf.
15. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [Електронний ресурс] / S. Nakamoto. – 2008. – Режим доступу: https://bitcoin.org/bitcoin.pdf.
16. Back A. Hashcash – A Denial of Service Counter-Measure [Електронний ресурс] / Adam Back. – Aug. 2002. – Режим доступу: http://www.hashcash.org/papers/hashcash.pdf.
17. Bmoney. [Електронний ресурс]. – Режим доступу: http://www.weidai.com/bmoney.txt.
18. Chaum D. Untraceable Electronic Cash / David Chaum, Amos Fiat, Moni Naor // Advances in Cryptology – CRYPTO '88 Proceedings.
19. Szabo N. Bit Gold [Електронний ресурс] / Nick Szabo // Unenumerated: An unending variety of topics. – December 2008. – Режим доступу: https://unenumerated.blogspot.com/2005/12/bit-gold.html.
20. Finney H. Reusable Proofs of Work [Електронний ресурс] / Hal Finney. – Режим доступу: https://nakamotoinstitute.org/finney/rpow/ index.html.
21. Amadeo K. 2007 Financial Crisis Explanation, Causes, and Timeline: Here's How They Missed the Early Clues of the Financial Crisis [Електронний ресурс] / Kimberly Amadeo. – Режим





доступу: https://www.thebalance.com/ 2007-financial-crisis-overview-3306138.

22. BTC to USD: Bitcoin to US Dollar Market Price–Blockchain [Електронний ресурс]. – Режим доступу: https://www.blockchain.com/charts/market-price.
23. Wong J. Bitcoin Pizza Day 2018: Eight years ago today, someone bought two pizzas with bitcoins now worth $82 million [Електронний ресурс] / Joon Ian Wong. – 2018. – Режим доступу: https://qz.com/1285209/bitcoin-pizza-day-2018-eight-years-ago-someone-bought-two-pizzas-with-bitcoins-now-worth-82-million.
24. How Many Bitcoins Are Lost Forever? [Електронний ресурс] / calaber24p (74). – Режим доступу: https://steemit.com/bitcoin/@calaber24p/how-many-bitcoins-are-lost-forever.
25. Bitxfy [Електронний ресурс]. – Режим доступу: https://bitxfy.com.
26. Sedgwick K. Man's Life Savings Stolen from Hardware Supplied by a Reseller [Електронний ресурс] / Kai Sedgwick. – 2018. – Режим доступу: https://news.bitcoin.com/mans-life-savings-stolen-from-hardware-wallet-supplied-by-a-reseller/.
27. Man Who 'Threw Away' Bitcoin Haul Now Worth over $80m Wants to Dig Up Landfill Site [Електронний ресурс] // Independent. – Режим доступу: https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-value-james-howells-newport-landfill-hard-drive-campbell-simpson-laszlo-hanyecz-a8091371.html.
28. CAP theorem [Електронний ресурс] // Wikipedia. — Режим доступу: https://en.wikipedia.org/wiki/CAP_theorem.
29. Coinbase maturity of 100 transactions [duplicate] [Електронний ресурс]. – Режим доступу: https://bitcoin.stackexchange.com/questions/ 22548/coinbase-maturity-of-100-transactions.
30. Entropy (computing) [Електронний ресурс] // Wikipedia. – Режим доступу: https://en.wikipedia.org/wiki/Entropy_(computing).

31. Specifications for the Secure Hash Standard [Електронний ресурс] // Federal Information Processing Standards Publication 180-4. – 2012. – Режим доступу: http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf.
32. Merkle R. C. A Digital Signature Based on a Conventional Encryption Function [Електронний ресурс] / Ralph C. Merkle // Advances in Cryptology – CRYPTO '87, Lecture Notes in Computer Science. – Вид. 293. – с. 369–378. – Режим доступу: https://people.eecs.berkeley.edu/~raluca/cs261-f15/readings/merkle.pdf.
33. Specification for the Advanced Encryption Standard (AES). [Електронний ресурс] // Federal Information Processing Standards Publication 197. – 2001. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf.
34. Bos J. W. Elliptic curve cryptography in practice / J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, E. Wustrow // 18th International Conference, FC 2014. – Springer Berlin Heidelberg, 2014. – P. 157–175.
35. Federal Information Processing Standard (FIPS) 186-4, Digital Signature Standard; Request for Comments on the NIST-Recommended Elliptic Curves [Електронний ресурс]. – October 20, 2015 // Computer Security Resource Center. – Режим доступу: https://csrc.nist.gov/news/2015/fips-186-4-rfc-nist-recommended-elliptic-curves.
36. Secp256k1 [Електронний ресурс] // Bitcoin Wiki. – Режим доступу: https://en.bitcoin.it/wiki/Secp256k1.
37. Miller V. S. Use of elliptic curves in cryptography / V. S. Miller // Williams H. C. (eds.) Advances in Cryptology – CRYPTO '85 Proceedings. CRYPTO 1985. Lecture Notes in Computer Science. – Springer, Berlin, Heidelberg, 1986. – Вид. 218. – с. 417–426.
38. Eskandari S. A First Look at the Usability of Bitcoin Key Management / S. Eskandari, D. Barrera, E. Stobert, J. Clark, Proceedings of the NDSS // Workshop on Usable Security (USEC), February 2015.





39. Tyagi A. Confirmed: "Malicious Code Deployed on Versions 5.0.2 through 5.1.0 of Copay & BitPay apps" / Anjali Tyagi. – 2018. – Режим доступу: https://coingape.com/malicious-code-deployed-copay-bitpay-apps.
40. Exploring Bitcoin: Signature Hash Types [Електронний ресурс]. – Режим доступу: https://medium.com/@support_62391/exploring-bitcoin-signature-hash-types-15427766f0a9.
41. Bitcoin Transaction 8bae12b5f4c088d940733dcd1455efc6a3a69cf9340e17a981286d3778615684 [Електронний ресурс]. – Режим доступу: https://www.blockchain.com/en/btc/tx/8bae12b5f4c088d940733dcd1455efc6a3a69cf9340e17a981286d3778615684.
42. Standard Transactions [Електронний ресурс] // Bitcoin Developer Guide. – Режим доступу: https://bitcoin.org/en/developer-guide#standard-transactions.
43. Back A. Enabling Blockchain Innovations with Pegged Sidechains [Електронний ресурс] / Adam Back, Matt Corallo, Luke Dashjr et al. – Oct. 2014. – Режим доступу: https://blockstream.com/sidechains.pdf.
44. Difficulty [Електронний ресурс]. – Режим доступу: https://en.bitcoin.it/wiki/Difficulty.
45. Zhang R. Broadcasting intermediate blocks as a defense mechanism against selfish-mine in bitcoin / Ren Zhang, Bart Preneel // IACR Cryptology ePrint Archive, 2015.
46. Bitcoin Difficulty [Електронний ресурс]. – Режим доступу: https://bitcoinwisdom.com/bitcoin/difficulty.
47. Global Bitcoin Nodes Distribution [Електронний ресурс]. – December 2018. – Режим доступу: https://bitnodes.earn.com/.
48. Number Of Orphaned Blocks [Електронний ресурс]. – Режим доступу: https://www.blockchain.com/charts/n-orphaned-blocks?timespan=4years.
49. Краузова Е. Валерий Вавилов, BitFury Group: «Блокчейн – индустрия на триллионы долларов» [Електронний ресурс] /

Елена Краузова. – Режим доступу: http://www.forbes.ru/tehnologii/344801-valeriy-vavilov-bitfury-group-blokcheyn-industriya-na-trilliony-dollarov.

50. Blockchain Explorer–Search the Blockchain | BTC | ETH [Електронний ресурс]. – Режим доступу: https://www.blockchain.com/explorer.
51. Blockchain Hashrate Distribution–Blockchain.info [Електронний ресурс] // Blockchain. – Режим доступу: https://www.blockchain.com/pools.
52. Bitcoin Energy Consumption Index [Електронний ресурс]. – Режим доступу: https://digiconomist.net/bitcoin-energy-consumption#assumptions.
53. U.S. Electric System Operating Data [Електронний ресурс]. – Режим доступу: https://www.eia.gov/realtime_grid/?src=data#/status?end=20180906T10.
54. Bitcoin Energy Consumption Index [Електронний ресурс]. Режим доступу: https://digiconomist.net/bitcoin-energy-consumption.
55. Rosenfeld M. Analysis of hashrate-based double-spending [Електронний ресурс] / M. Rosenfeld. – Dec. 2012. – Режим доступу: https://arxiv.org/pdf/1402.2009.pdf.
56. Bitcoin Block #0 [Електронний ресурс] // Blockchain. – Режим доступу: https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.
57. Lopp J. Bitcoin's Security Model: A Deep Dive [Електронний ресурс] /Jameson Lopp. – Nov 13, 2016. – Режим доступу: https://www.coindesk.com/bitcoins-security-model-deep-dive.
58. BIP9 [Електронний ресурс]. – Режим доступу: https://github.com/bitcoin/bips/blob/master/bip-0009.mediawiki.
59. Caffyn G. Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network [Електронний ресурс] / Grace Caffyn. – 2015. – Режим доступу: https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network.





60. We're researching a DNS issue and looking into it. We apologize for the inconvenience. Stay tuned [Електронний ресурс] / @blockchain. // Twitter. – Режим доступу: https://twitter.com/blockchain/status/786151063955136512.
61. Simplified Payment Verification (SPV) [Електронний ресурс] // Bitcoin Developer Guide. – Режим доступу: https://bitcoin.org/en/developer-guide#simplified-payment-verification-spv.
62. Szabo N. The Idea of Smart Contracts [Електронний ресурс] / N. Szabo. – Режим доступу: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html.
63. Shamir A. How to Share a Secret [Електронний ресурс]/ Adi Shamir // Communications of the ACM. – Nov. 1979. – Вид. 22, № 11. – с. 612–613. – Режим доступу: https://cs.jhu.edu/~sdoshi/crypto/papers/shamirturing.pdf.
64. Script opcodes [Електронний ресурс]. – Режим доступу: https://github.com/bitcoin/bitcoin/blob/v0.14.0/src/script/script.h#L46L187.
65. Andresen G. BIP 0016: Pay to Script Hash [Електронний ресурс] / Gavin Andresen. – Jan. 2012. – Режим доступу: https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki.
66. BIP13 [Електронний ресурс]. – Режим доступу: https://github.com/bitcoin/bips/blob/master/bip-0013.mediawiki.
67. Bradbury D. What the 'Bitcoin Bug' Means: A Guide to Transaction Malleability [Електронний ресурс] / Danny Bradbury. – Feb 12, 2014. – Режим доступу: https://www.coindesk.com/bitcoin-bug-guide-transaction-malleability.
68. BitMEX Research. The SegWit Transaction Capacity Increase – Part 2 – The First Month After Activation [Електронний ресурс] / BitMEX Research. – Sep. 2017. – Режим доступу: https://blog.bitmex.com/the-segwit-transaction-capacity-increase.

69. BIP125 [Електронний ресурс]. – Режим доступу: https://github.com/bitcoin/bips/blob/master/bip-0125.mediawiki.
70. Miller B. Improving Bitcoin Reliability through Child Pays for Parent [Електронний ресурс] / Brock Miller, Eli Haims. – Режим доступу: https://blog.coinbase.com/improving-bitcoin-reliability-through-child-pays-for-parent-77e771bb04d6.
71. Bitcoin Core :: Bitcoin Core 0.13.0 Released! [Електронний ресурс]. – Aug. 23, 2016. – Режим доступу: https://bitcoincore.org/ en/2016/08/23/release-0.13.0/#more-intelligent-transaction-selection-for-mining.
72. Poon J. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments [Електронний ресурс] / Joseph Poon, Thaddeus Dryja. – January 2016. – Режим доступу: https://lightning.network/lightning-network-paper.pdf.
73. Payment channels [Електронний ресурс]. – Режим доступу: https://en.bitcoin.it/wiki/Payment_channels.
74. Working with micropayment channels [Електронний ресурс]. – Режим доступу: https://bitcoinj.github.io/working-with-micropayments.
75. Poon J. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments [Електронний ресурс] / Joseph Poon, Thaddeus Dryja. – January 2016. – Режим доступу: https://lightning.network/lightning-network-paper.pdf.
76. Alpha Release of the Lightning Network Daemon [Електронний ресурс]. – Jan 10, 2017. – Режим доступу: https://lightning.community/release/software/lnd/lightning/2017/01/10/lightning-network-daemon-alpha-release/.
77. Lightning-rfc [Електронний ресурс]. – Режим доступу: https://github.com/lightningnetwork/lightning-rfc.
78. Lightning Network Explorer (TESTNET). Supported by ACINQ. [Електронний ресурс]. – Режим доступу: https://explorer.acinq.co.





79. EOS.IO Technical White Paper v2 [Електронний ресурс]. – 2018. – Режим доступу: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md.
80. Delegated Proof-of-Stake Consensus–Bitshares [Електронний ресурс]. – Режим доступу: https://bitshares.org/technology/delegated-proof-of-stake-consensus.
81. Proof-of-Importance. NEM: Technical Reference [Електронний ресурс]. – Режим доступу: https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf#section.7.
82. Lamport L. The byzantine generals problem / L. Lamport, R. Shostak, M. Pease // ACM Transactions Programming Languages and Systems. – Jul. 1982. – Вид. 4, № 3. – с. 382–401.
83. Mazières D. The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus [Електронний ресурс] / David Mazières. – Режим доступу: https://www.stellar.org/papers/stellar-consensus-protocol.pdf.
84. Sompolinsky Y. SPECTRE: Serialization of Proof-of-work Events: Confirming Transactions via Recursive Elections [Електронний ресурс] / Yonatan Sompolinsky, Yoad Lewenberg, Aviv Zohar. – Режим доступу: https://eprint.iacr.org/2016/1159.pdf.
85. Sompolinsky Y. PHANTOM, GHOSTDAG: Two Scalable BlockDAG protocols [Електронний ресурс] / Yonatan Sompolinsky, Aviv Zohar. – Режим доступу: https://eprint.iacr.org/2018/104.pdf.
86. Siegel D. Understanding The DAO Attack [Електронний ресурс] / David Siegel. – Jun 25, 2016. – Режим доступу: https://www.coindesk.com/understanding-dao-hack-journalists.
87. BIPs [Електронний ресурс]. – Режим доступу: https://github.com/bitcoin/bips.
88. Strange block 74638 [Електронний ресурс]. – August 15, 2010. – Режим доступу: https://bitcointalk.org/index.php?topic=822.0.
89. Woo W. Bitcoin Cash: BitPico 'Stress Test' Claims To Show Node Centralization [Електронний ресурс] / Wilma Woo. – 2018. –

Режим доступу: https://bitcoinist.com/bitcoin-cash-test-node-centralization.

90. Duffield E. Dash: A Payments-Focused Cryptocurrency [Електронний ресурс] / Evan Duffield, Daniel Diaz. – Режим доступу: https://github.com/dashpay/dash/wiki/Whitepaper.
91. Whitepaper:Nxt [Електронний ресурс]. – Режим доступу: https://nxtwiki.org/wiki/Whitepaper:Nxt.
92. Bytecoin and its forks (Monero, Fantomcoin, Quazarcoin) [Електронний ресурс]. – May 28, 2014. – Режим доступу: https://bitcointalk.org/index.php?topic=629122.0.
93. CryptoNote Standards [Електронний ресурс]. – Режим доступу: https://cryptonote.org/standards/.
94. Maxwell G. Confidential Transactions [Електронний ресурс] / Greg Maxwell. – Режим доступу: https://people.xiph.org/~greg/confidential_values.txt.
95. The Invisible Internet Project (I2P) [Електронний ресурс]. – Режим доступу: https://geti2p.net/en/about/intro.
96. Parameter Generation–Zcash [Електронний ресурс]. – Режим доступу: https://z.cash/technology/paramgen.
97. Kravchenko P. Tokenization in a nutshell [Електронний ресурс] / Pavel Kravchenko. – Режим доступу: https://medium.com/@pavelkravchenko/tokenization-in-a-nutshell-349968702e33.
98. Кравченко П. Теория токенизации / П. Кравченко, Б. Скрябин. – Харьков : Промарт, 2018. – 46 с.
99. David Crosbie [Електронний ресурс] // Penn Engineering Profile. – Режим доступу: In. https://www.seas.upenn.edu/directory/profile.php?ID=221.
100. Confidential Assets [Електронний ресурс] / Andrew Poelstra, Adam Back, Mark Friedenbach, Gregory Maxwell, and Pieter Wuille. – Режим доступу: https://blockstream.com/bitcoin17-final41.pdf.
101. Reid F. An Analysis of Anonymity in the Bitcoin System [Електронний ресурс] / F. Reid and M. Harrigan // Security and





Privacy in Social Networks. – Springer New York, 2013. – P. 197–223. – Режим доступу: https://users.encs.concordia.ca/~clark/biblio/bitcoin/Reid%202011.pdf.

102. Herrera-Joancomartí J. Privacy in bitcoin transactions: New challenges from blockchain scalability solutions / J. Herrera-Joancomartí and C. Perez-Solá // Modeling Decisions for Artificial Intelligence: 13th International Conference, MDAI 2016. – Springer International Publishing, 2016.
103. Meiklejohn S. A fistful of bitcoins: characterizing payments among men with no names [Електронний ресурс] / Sarah Meiklejohn, Marjori Pomarole, Grant Jordan et al. // Proceedings of the 2013 conference on Internet measurement conference, 2013. – Режим доступу: https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf.
104. Ruffing T. P2P Mixing and Unlinkable Bitcoin Transactions. Anonymity of the people, by the people, and for the people / T. Ruffing, P. Moreno-Sanchez, A. Kate // IACR Cryptology ePrint Archive, 2017.
105. Chaum D. Blind Signatures for Untraceable Payments [Електронний ресурс] / David Chaum. – Режим доступу: http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF.
106. Maxwell G. Coinjoin: Bitcoin privacy for the real world [Електронний ресурс] / G. Maxwell. – Mar. 2013. – Режим доступу: https://bitcointalk.org/index.php?topic=279249.0.
107. Ruffing T. CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin [Електронний ресурс] / Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate. – Режим доступу: https://petsymposium.org/2014/papers/ Ruffing.pdf.
108. Van Saberhagen N. CryptoNote v 2.0 [Електронний ресурс] / Nicolas van Saberhagen. – Oct. 2013. – Режим доступу: https://cryptonote.org/whitepaper.pdf.

109. Introduction to MimbleWimble and Grin [Електронний ресурс]. – Режим доступу: https://github.com/mimblewimble/grin/blob/master/doc/intro.md.

110. Courtois N. T. Stealth Addresses and Key Management Techniques in Blockchain Systems / Nicolas T. Courtois, Rebekah Mercer // Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017). – с. 559–566. – Режим доступу: http://www.scitepress.org/Papers/2017/62700/62700.pdf.

111. Malkhi D. Byzantine quorum systems / Dahlia Malkhi, Michael Reiter // Distributed Computing. – Oct. 1998. – Вид. 11, Вип. 4. – с. 203–213.

112. Van Wirdum A. The History of Lightning: From Brainstorm to Beta [Електронний ресурс] / Aaron van Wirdum. – Apr. 2018. – Режим доступу: https://bitcoinmagazine.com/articles/history-lightning-brainstorm-beta.

113. Three Gorges Dam [Електронний ресурс] // Wikipedia. – Режим доступу: https://en.wikipedia.org/wiki/Three_Gorges_Dam#cite_note-Xinhua20081007-11.

114. Van Wirdum A. Lightning's First Implementation Is Now in Beta; Developers Raise $2.5M [Електронний ресурс] / Aaron van Wirdum. – Mar 15, 2018. – Режим доступу: https://bitcoinmagazine.com/articles/lightnings-first-implementation-now-beta-developers-raise-25m/.

115. Solidity [Електронний ресурс]. – Режим доступу: http://solidity.readthedocs.io.

116. Bonneau J. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies [Електронний ресурс] / Joseph Bonneau, Andrew Miller, Jeremy Clark et al. – Режим доступу: https://wws.princeton.edu/system/files/research/documents/Felten_SoK.pdf.





117. Möser M. An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem [Електронний ресурс] / Malte Möser, Rainer Böhme, Dominic Breuker // 2013 eCrime Researchers Summit. – Режим доступу: https://maltemoeser.de/paper/money-laundering.pdf.

118. The Next CryptoKitties? The Blockchain Might Not Be Ready [Електронний ресурс]. – Режим доступу: https://www.coindesk.com/token-summit-scaling-cryptokitties.

119. Varshney N. Here's how much it costs to launch a 51% attack on PoW cryptocurrencies [Електронний ресурс] / Neer Varshney. – 2018. – Режим доступу: https://thenextweb.com/hardfork/2018/05/30/heres-how-much-it-costs-to-launch-a-51-attack-on-pow-cryptocurrencies.

120. BIP38 [Електронний ресурс]. – Режим доступу: https://github.com/bitcoin/bips/blob/master/bip-0038.mediawiki.

121. Conti M. A Survey on Security and Privacy Issues of Bitcoin [Електронний ресурс] / Mauro Conti. – Режим доступу: https://arxiv.org/pdf/1706.00916.pdf.

122. Maltese Marco E. G. Satoshi Nakamoto Writes To Cointelegraph About The Nobel Prize [Електронний ресурс] / Marco E. G. Maltese. – Dec. 17, 2015. – Режим доступу: https://cointelegraph.com/news/satoshi-nakamoto-writes-to-cointelegraph-about-the-nobel-prize.

123. BIP39 [Електронний ресурс]. – Режим доступу: https://github.com/bitcoin/bips/tree/master/bip-0039.

124. Wuille P. [Bitcoin-development] Scaling Bitcoin with Subchains [Електронний ресурс] / Pieter Wuille. – Режим доступу: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-June/008617.html.

*Навчальне видання*

**КРАВЧЕНКО** Павло Олександрович
**СКРЯБІН** Богдан Борисович
**ДУБІНІНА** Оксана Миколаївна

# БЛОКЧЕЙН І ДЕЦЕНТРАЛІЗОВАНІ СИСТЕМИ

Навчальний посібник
для студентів закладів вищої освіти
У трьох частинах

**Частина 1**

*В авторській редакції*

*Роботу до видання рекомендував проф. Кузнєцов О. О.*
*Редактор Курбатов О. С.*

Підписано до друку 22.02.2019
Формат 60×90 11/16. Папір офсетний. Гарнітура Times.
Умовн. друк. лист. 27,5. Облік.-вид. лист. 18,69. Вид. № 2102.
Тираж 100 экз.

Надруковано у типографії ТОВ «ПРОМАРТ»
Тел. (057) 717-28-80