

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)

Р е ц е н з е н т и :

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

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

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

Є. 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 розповсюдженю 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

Зверніть увагу!

Дана цифрова копія призначена для викладачів та студентів освітніх закладів.

Усі права захищені. Контент даної копії не можна друкувати, розповсюджувати або змінювати без дозволу правовласника.

Зміст

ВСТУП	10
ПРО DISTRIBUTED LAB.....	13
1. ДЕЦЕНТРАЛІЗАЦІЯ В ІНФОРМАЦІЙНИХ СИСТЕМАХ	15
1.1 Що таке децентралізація?	15
Поняття децентралізації для інформаційних систем	16
Відмінність децентралізованих систем від систем з резервуванням.....	16
1.2 Історія децентралізованих систем.....	17
Децентралізовані файлообмінні системи	18
Децентралізовані системи передачі даних	20
Децентралізовані обчислювальні системи	20
Децентралізовані системи зберігання даних	21
Децентралізовані системи прийняття рішень	23
Децентралізовані платіжні системи.....	24
1.3 Застосування принципів децентралізації.....	25
Обмеження та проблеми централізованих систем	26
Застосування децентралізованого підходу.....	28
Принципи побудови децентралізованих систем	28
Типова архітектура децентралізованих систем	31
Обмеження децентралізованих систем	34
Фактори, що впovільнюють впровадження децентралізованих систем.....	35
Висновки	39
2. ІСТОРІЯ ТА ПРИНЦИПИ ФУНКЦІОNUВАННЯ BITCOIN.....	40
2.1 Що таке Bitcoin?.....	40
Історія виникнення Bitcoin.....	42
Проблеми, які здатний вирішити Bitcoin	45
Головні принципи функціонування Bitcoin	47
Емісія в Bitcoin	48
Формування ціни на монети.....	51
Поняття довіри в Bitcoin	54
Обмеження технології Bitcoin	55
Значення децентралізації для Bitcoin.....	56
2.2 Як застосовувати Bitcoin?	58
Ключі у Bitcoin	59
Транзакції в Bitcoin.....	59
Програмні гаманці	60
Апаратні гаманці	61
Централізовані сховища.....	64
Резервне копіювання гаманців	64

Зміст

2.3 Поняття транзакції у Bitcoin	68
Що таке Bitcoin-транзакція?.....	68
Перевірка транзакцій	71
Поняття комісії у Bitcoin.....	74
Поняття конфліктуючих транзакцій	75
2.4 Високорівнева архітектура Bitcoin.....	77
Архітектура системи з технологією blockchain.....	77
Процеси в обліковій системі Bitcoin.....	79
Ролі учасників в обліковій системі Bitcoin	80
Умови, за яких досягається консенсус у Bitcoin	80
Як досягається консенсус в Bitcoin?.....	82
Порівняння Bitcoin з традиційними платіжними системами	83
2.5 Підтвердження транзакцій у Bitcoin	86
Формування блоків транзакцій.....	86
Вимоги до нових блоків	88
Принципи змагання між користувачами.....	90
Розповсюдження блоку	91
Вирішення розбіжностей	92
Поняття повного підтвердження транзакції.....	94
Винагороди за створення блоків	95
Вплив розривів мережі на облікову систему Bitcoin	97
3. ВСТУП ДО КРИПТОГРАФІЇ ТА УПРАВЛІННЯ КЛЮЧАМИ.....	105
3.1 Вступ до криптографії	105
Принципи криптографічного захисту інформації	105
Поняття ключів.....	107
Модель загроз та порушника.....	108
Генерація та обробка секретних ключів	113
Поняття односторонньої функції та NP-повної задачі.....	115
Геш-функція	116
Застосування геш-функцій	121
Дерева Меркла.....	121
Симетричне шифрування	123
Асиметрична криптографія	126
3.2 Криптографія у Bitcoin	128
Особливості роботи еліптичних кривих	128
Створення біткоін-адрес	130
Конфіденційність в Bitcoin.....	131
3.3 Зберігання та обробка ключів	135
Головна задача цифрового гаманця.....	135
Основні підходи до синхронізації гаманця	136
Обробка та зберігання ключів на сервері.....	137

Ключі на сервері, але доступ до них тільки у клієнта	139
Ключі на пристрій користувача.....	140
Зберігання монет із застосуванням мультипідпису	142
Холодні, теплі та гарячі гаманці.....	143
4. ТЕХНОЛОГІЧНІ ДЕТАЛІ ФУНКЦІОNUВАННЯ BITCOIN	147
4.1 Як працюють транзакції в Bitcoin?.....	147
Структура транзакції	147
Unspent Transaction Outputs (UTXOs)	152
Отримання решти та встановлення комісії	153
Схема передачі монет на прикладі	154
Формування транзакцій у bitcoin-гаманцях	156
Механізм LockTime	160
Off-chain протоколи	161
Signature hash types	164
Запис довільних даних до ланцюга блоків.....	165
Висновки	169
4.2 Майнінг у Bitcoin	173
Поняття і цілі майнінгу в Bitcoin.....	173
Класифікація вузлів мережі.....	174
Поняття ресурсомісткого завдання.....	175
Обмеження частоти формування блоків	178
Orphan blocks	178
Атака подвійної витрати	180
Поява спеціального обладнання	184
Майнінгові пули та їх завдання	187
Статистика майнінгу і оцінка енергоспоживання	190
4.3 Як реалізований blockchain у Bitcoin	195
Структура блоку	197
Приклади блоків у Bitcoin.....	199
Поняття Mempool у Bitcoin	202
Життєвий цикл блоку.....	203
Початкова синхронізація вузла	206
Checkpoints	208
Властивості спільноти бази даних Bitcoin.....	209
4.4 Підходи до синхронізації з мережею та SPV-вузол	213
Складнощі роботи у розподіленій мережі	215
Підходи до синхронізації гаманця з платіжною мережею.....	216
Робота з повним вузлом мережі	216
Робота з довіреним вузлом мережі	217
Робота з SPV-вузлами	220
Функціонування SPV-вузла	221
Висновки	224

Зміст

4.5 Механізм мультипідпису та Bitcoin Script.....	227
Bitcoin-транзакція, яка використовує мультипідпис	228
Варіант мультипідпису 2-3-2	230
Варіант мультипідпису 2-3-3	233
Переваги Wallet-сервісів із мультипідписом 2-3-3	237
Знайомство з Bitcoin Script.....	237
Концепція P2SH-адрес і переваги їх використання.....	238
Приклад використання P2SH для MultiSig-адреси	241
4.6 Особливості оновлення Segregated Witness.....	243
Збільшення пропускної здатності та зворотна сумісність	246
Нововведення Segregated Witness.....	248
Приклад SegWit-транзакції	251
Нові поняття ваги і розміру.....	253
Статистика адаптації оновлення.....	255
4.7 Механізм комісій у Bitcoin.....	258
Волатильність ціни запису даних	260
Рішення проблеми з волатильністю комісій	261
Підвищення комісії після відправки транзакції	262
Як Segregated Witness допомагає знизити комісії	264
Варіант із другом-майнером.....	265
Варіант із продажем місць у черзі на підтвердження.....	266
4.8 Платіжні канали та Lightning Network.....	268
Що таке платіжний канал?	268
Чому потрібні платіжні канали?	269
Платіжний канал: приклад крок за кроком	270
Особливості платіжного каналу	272
Методи реалізації платіжних каналів	273
Spillman-style payment channels	273
Застосування платіжних каналів	277
Особливості роботи мережі Bitcoin та Lightning Network	278
Як працює Lightning Network	279
5. ТЕХНОЛОГІЯ BLOCKCHAIN	288
5.1 Технологія blockchain та її можливості	288
Ступені децентралізації	290
Архітектура blockchain	293
Властивості блокчейна.....	294
Застосування технології блокчейн	296
Висновки	302
5.2 Відмінності підходів до досягнення консенсусу	306
Механізм досягнення консенсусу як ключовий елемент децентралізованої системи обліку.....	306
Proof-of-work	307

Proof-of-stake	308
Delegated proof-of-stake	309
Proof-of-importance	310
BFT	310
FBA	312
Протоколи досягнення консенсусу, що базуються на DAG	313
Основні критерії класифікації механізмів досягнення консенсусу	314
Висновки	316
5.3 Обмеження технології blockchain і складнощі її застосування	318
Упровадження digital identity	319
Дигіталізація всіх процесів	320
Прийняття єдиних правил обробки даних	320
Перенесення всіх цифрових активів до однієї облікової системи	321
Організація децентралізованого прийняття рішень	321
Обмеження пропускної здатності	322
Обмеження часу підтвердження транзакції	323
Проблема управління (governance)	325
Розподілена відповідальність	326
Проблема оновлення протоколу	327
Висновки	328
6. РОЗВИТОК ДЕЦЕНТРАЛІЗОВАНИХ ТЕХНОЛОГІЙ	329
6.1 Відгалуження та клони Bitcoin	329
Сплановані форки	330
Методи оновлення програмного забезпечення: softfork i hardfork	333
Незапланований softfork у Bitcoin	335
Поняття спланованих форків	336
Приклади спланованих форків Bitcoin	337
6.2 Альтернативні цифрові валюти та токени	341
Що таке криптовалюта?	342
Litecoin	343
Dash	343
Відмінність алгоритмів майнінгу Litecoin, Dash і Bitcoin	345
NXT	346
BitShares	346
Monero	347
Ethereum	349
Cardano	350
Ripple і Stellar	350
ZCash	351
Інші цифрові валюти	352
Токени	354
Висновки	356

Зміст

6.3 Вступ до смарт-контрактів.....	359
Що таке смарт-контракт?	362
Роль оракулів для смарт-контрактів	365
Приклад із купівлею в онлайн-магазині	366
Приклад контракту для спільної купівлі.....	369
Класифікація платформ смарт-контрактів	371
Відмінність платформ за середовищем виконання	371
Відмінність платформ за способом виконання контрактів	373
Відмінність платформ за способом ініціювання контрактів.....	374
Висновки	375
6.4 Вступ до токенізації активів	377
Проблеми існуючих облікових систем	380
Що таке платформа токенізації?.....	381
Принципи функціонування платформи токенізації.....	383
Можливості, які надає токенізація	384
Прозорість процесів облікової системи	385
Як токенізація приводить до збільшення вартості активів?	385
Умови ефективного застосування платформ токенізації	386
Ризики	387
Відмінність токенізації від оцифровки	387
Чому саме blockchain технологія?	388
Висновки	389
7. КОНФІДЕНЦІЙНІСТЬ КОРИСТУВАЧІВ У ВІДКРИТИХ СИСТЕМАХ	392
7.1 Поняття приватності у цифровому світі	392
Важливість збереження приватності	392
Складові приватності	394
7.2 Конфіденційність у цифрових валютах	396
Blind Signatures	397
Конфіденційність в Bitcoin за замовчуванням	398
CoinJoin	400
Chaumian CoinJoin	402
CoinShuffle	404
Недоліки методу CoinJoin	407
Концепція zero-knowledge proof	408
Confidential Transactions	412
Ring Confidential Transactions	413
MimbleWimble	414
Stealth Addresses	415
Концепція гомоморфного шифрування	417
ЗАКЛЮЧЕННЯ	419

ТЕСТОВІ ПИТАННЯ З ВАРИАНТАМИ ВІДПОВІДЕЙ	421
СЛОВНИК ТЕРМІНІВ.....	447
ПОДЯКИ	459
ПРО АВТОРІВ.....	460
ВИКОРИСТАНІ ДЖЕРЕЛА ТА ПОСИЛАННЯ.....	461

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, зображені їх розуміння та стане дорожевказом 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 DISTRIBUTED LAB

Місія Distributed Lab – зробити Фінансовий Інтернет реальністю. Суспільство насолоджується перевагами, що доступні завдяки сучасному Інтернету, починаючи з сімейних розваг і соціальних мереж та закінчуючи інтернет-банкінгом і глобальними ланцюгами постачань. Однак процеси, пов’язані з платежами, торгівлею й управлінням правами власності, як і раніше засновані переважно на операціях з паперовими документами і, внаслідок цього, є повільними, громіздкими, неефективними і, більш того, небезпечними. Ми уявляємо світ, в якому всі активи управляються за допомогою доступного та відкритого програмного забезпечення з єдиним протоколом.

Компанія Distributed Lab (<https://distributedlab.com/>) була заснована в 2014 році как R&D (науково-дослідницька) компанія. Ми працювали над найрізноманітнішими проектами: від гаманців до цифрових банків, – все так чи інакше пов’язано з галуззю обліку й управління активами.

Ми побачили потенціал, який технологія blockchain може принести бізнесу, чим вкрай зацікавилися. В якийсь момент ми зрозуміли, що повинні розповсюджувати новини про блискавичне майбутнє з однієї простої причини – неможливо створювати передові системи без належної освіти, яка орієнтована на глибоке розуміння принципів blockchain і децентралізованих технологій. Саме так ми прийшли до ідеї, яка опинилася наріжним каменем побудови Фінансового Інтернету, – шляхом проведення досліджень і обміну знаннями.

Наша місія може здаватися занадто амбіційною, але ми вважаємо, що її можливо досягти крок за кроком. Найближча мета – токенізація (оцифровка) систем управління активами. Для цього ми створили фреймворк TokenD (<https://tokend.io/>). Він з’явився у результаті багаторічної роботи над різноманітними проектами, які, як ми

пізніше зрозуміли, потребували одного й того ж – захищеної системи обліку з гаманцями для користувачів, реєстром (ledger) для активів, внутрішньою платіжною системою, біржею, модулями, керуючими identities, ролями, життєвим циклом активів і шлюзами для зовнішніх інтеграцій. Поєднуючи в собі все згадане, TokenD дозволяє запустити екосистему цифрових активів протягом декількох днів при невеликій частці витрат на внутрішню розробку.

Під час божевільного хайпу 2017 року ми зберігали спокій і не брали участі ні в яких ICO, зосередившись на пошуку реальної цінності для бізнесу, яку може забезпечити технологія блокчейн. Ми присвячуємо себе до тривалої подорожі по перетворенню світу за допомогою саме таких технологій.

1. ДЕЦЕНТРАЛІЗАЦІЯ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

1.1 Що таке децентралізація?

Децентралізація є протилежним до централізації процесом і передбачає розподілення функцій системи (зберігання даних, обчислення тощо) між її учасниками, причому без єдиного керуючого органу. Важливо розуміти, що це поняття можна застосувати далеко поза межами інформаційних технологій, і воно вже давно використовується в таких галузях суспільного життя як політика, менеджмент, юриспруденція, економіка тощо. Саме слово децентралізація увійшло у вжиток в 1820-і рр.

У теорії передачі даних децентралізація передбачає створення умов, за яких зникає потреба в існуванні центрального сервера, а учасники мережі мають одинаковий ранг. Децентралізація також має місце і у глобальній мережі Інтернет, маршрутизатори якої працюють незалежно один від одного. У більшості випадків існує більше одного маршруту доставки пакета даних, а вихід з ладу одного з маршрутизаторів не є критичним для користувачів.

Централізовані системи та ієрархічні моделі управління, що застосовуються в них, мають низку недоліків. Наприклад, будь-яка централізована соціальна мережа, подібна до Facebook, має можливість здійснювати цензуру та блокувати акаунти користувачів. Непрозорість процесів, які відбуваються у централізованих інформаційних системах, не залишає клієнтам можливості доведення факту порушення конфіденційності їх приватних даних. Такий стан речей дозволяє власникам системи навіть модифікувати історію змін на свій розсуд, у тому числі заднім числом. Очевидно, що в таких системах процес прийняття рішень носить суб'єктивний характер.

Децентралізована система передбачає наявність великої кількості незалежних учасників, які спільно здійснюють управління процесами. Подібний підхід вимагає від учасників узгоджених дій, що потрібні для досить ефективної взаємодії за відсутності

1. Децентралізація в інформаційних системах

центральної сторони. У цьому випадку децентралізація має безліч переваг. Для їх розуміння корисно буде звернутися до історії її розвитку.

Поняття децентралізації для інформаційних систем

Спочатку необхідно розібратися, що являє собою інформаційна система. Згідно стандарту ISO/IEC 2382:2015 [1], інформаційна система – це система, призначена для збору, структурування, зберігання та обробки інформації, і відповідні організаційні ресурси, які до неї належать. Для функціонування інформаційної системи необхідна низка наступних компонентів: база даних, користувачі та технічні засоби з відповідним програмним забезпеченням.

Можна виділити дві головні ознаки, що відрізняють децентралізовану інформаційну систему від централізованої. Перша з них полягає в тому, що всі її компоненти обов'язково повинні бути децентралізованими. «Ну і що ж?» – скажете ви. – «Припустимо, централізований сервіс передбачає, що копії бази даних зберігаються паралельно у всіх користувачів. Але ж подібний підхід не робить систему децентралізованою?» Правильно, але існує ще друга ознака. Вона передбачає, що децентралізація *розщеплює ядро* системи. Усі процеси, що раніше вважалися нероздільними, а саме – керування системою, управління особистими даними та активами, комунікація, процес прийняття рішень, зберігання й обробки інформації, аудит, – відтепер можуть виконуватися багатьма учасниками паралельно і незалежно.

Відмінність децентралізованих систем від систем з резервуванням

Для забезпечення стабільності характеристик певної системи часто використовується принцип резервування. Резервування передбачає введення надмірності до системи шляхом додавання запасних (резервних) компонентів. Такий підхід передбачає, що за відмови одного з компонентів системи, її функціонування не

припиниться, а просто відбудеться заміна цього компонента на резервний. Прикладом резервування може вважатись дублювання деяких органів у організмі людини або ж наявність заступників у керівних посадовців.

Згідно з вищезазначеним, надамо визначення системи з резервуванням. *Система з резервуванням – це система з резервними складовими, надлишковими відносно до мінімально необхідної їх кількості і виконуючими такі ж функції, що й основні елементи системи.*

Важливо розуміти, що децентралізація обов'язково передбачає наявність резервування, але резервування не завжди передбачає децентралізацію. Справа в тому, що процес резервування може здійснюватися і для централізованих систем. Цей процес передбачає додавання резервних копій для ключових компонентів системи. У децентралізованому середовищі резервування є обов'язковим наслідком наявності незалежного набору компонентів у кожного з учасників системи.

Виходячи з визначення системи з резервуванням і децентралізованої системи, можна відзначити дві основні відмінності між ними. Перша полягає в тому, що управління компонентами децентралізованої системи, на відміну від системи з резервуванням, не може здійснюватися з єдиного центру (згідно з визначенням). Друга відмінність полягає в тому, що наявність надлишковості є необхідною складовою для децентралізованої системи. Для системи з резервуванням надлишковість застосовується з метою покращення характеристик системи, але вона не є обов'язковою.

1.2 Історія децентралізованих систем

Ще в 1970-х рр. у пошуках надійнішого способу зберігання цифрових даних суспільство звернуло увагу на децентралізацію, і одним з перших був реалізований проект під назвою Usenet [2]. Принцип його роботи полягав у тому, що сервери обмінювалися даними згідно зі спеціальним алгоритмом, який забезпечував їх

1. Децентралізація в інформаційних системах

синхронізацію між собою. Таким чином, кожен сервер являв собою оновлювану локальну копію будь-якого іншого зі своєї мережі. У разі відмови в обслуговуванні одного з серверів система продовжувала своє функціонування, адже самі дані зберігалися на будь-якому іншому сервері. В порівнянні з наявними на той момент централізованими альтернативами підхід Usenet дозволив підвищити надійність зберігання даних.

Ідея Usenet надала уявлення про новий підхід до зберігання та синхронізації даних, тому цілком закономірно, що пізніше вона була покладена в основу подальших спроб реалізації надійного способу передачі даних.

У цей час був запропонований протокол передачі файлів – FTP (*File Transfer Protocol*) [3]. Він дозволив користувачам незалежно передавати файли один до одного і дав поштовх виникненню децентралізованих файлообмінних мереж і протоколів обміну повідомленнями, які почали активно розвиватися пізніше, в 1990-х рр. Серед них можна відзначити Topsites, IRC, Napster тощо.

На початку 1980-х світ побачив стек протоколів передачі даних TCP/IP [4], з яким з'явився звичний для нас сьогодні Інтернет. Це стало революцією в інформаційному світі, оскільки комп'ютери отримали можливість підключатися до глобального цифрового простору. Бізнес також отримав великий зиск від переходу процесів до цифрової форми, і більшість держав підтримали цю інновацію.

Інтернет став вільною мережею для поширення інформації та прикладом для інших сфер, які стали застосовувати принципи децентралізації для пошуку та обробки даних – зараз ми називаємо їх *open API* і *sharing economy* [5]. Їх основна ідея полягає у прямій взаємодії користувачів один з одним, а також у спільному використанні ресурсів, послуг, контенту, пристрійв тощо.

Децентралізовані файлообмінні системи

Стрімкий розвиток децентралізації у Мережі почався з появию сервісів і протоколів для кооперативного обміну файлами (рис. 1.1).

Один із перших сервісів, Napster, надавав можливість обміну MP3-файлами. У той час музичні композиції були доступні людям переважно у вигляді касет і дисків, які до того ж коштували грошей. Тому Napster став дуже популярним серед користувачів Інтернету. І хоча користувачі взаємодіяли за принципом *peer-to-peer* (P2P), база даних з файлами останньої версії все одно зберігалася на централізованому сервері. Пізніше це і виявилось слабким місцем, тиск на яке згодом завершився закриттям сервісу.

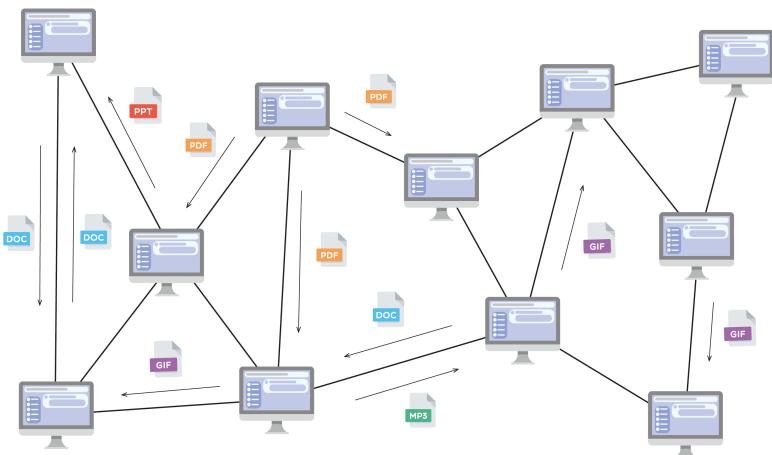


Рис 1.1 – Схема обміну файлами в децентралізованих файлообмінних мережах

Далі з'являлися інші файлообмінні мережі, такі як Gnutella, eDonkey2000, DC++ і I2HUB. Але пізніше багато з них також опинилися під загрозою, оскільки у регулюючих органів була можливість вплинути на компанію, що стояла за тим чи іншим сервісом. У 2005 році компанія MetaMachine, що розробляла та підтримувала eDonkey2000, отримала спеціальний лист від Американської асоціації індустрії звукозапису (RIAA) з вимогою припинити діяльність своєї файлообмінної мережі. Діяльність, яка велася за допомогою eDonkey2000, не могла вважатися легальною, а компанія могла понести серйозну відповідальність в тому випадку, якщо не припинить діяльність сервісу. Проект eDonkey2000 довелося

закрити. Проте світ вже отримав приклади, які показали, як можна змінити бізнес та економічні взаємовідносини. Реакцією на заборону та закриття p2p-проектів стала поява нових проектів, які розвивали децентралізовані моделі та створювали нові можливості для роботи з даними (доступність, надійність зберігання, відмовостійкість при роботі тощо).

Децентралізовані системи передачі даних

Що більше люди використовували глобальну мережу, тим гостріше відчуvalася необхідність у забезпеченні конфіденційності. На початку 2002 року був запущений проект під назвою Tor (The onion router) [6], який є системою проксі-серверів, що дозволяють встановлювати анонімне мережеве з'єднання, захищене від стеження за передачею даних. Реалізація Tor дозволила користувачам з усього світу обходити блокування трафіку місцевих провайдерів й отримувати доступ до даних, зберігаючи при цьому конфіденційність [7].

В окремих сферах технології засновані на принципах децентралізації, отримали дуже сильний поштовх до розвитку. Наприклад, в 2004 році були запущені перші проекти з використання бездротових mesh-мереж в Південній Африці. Принцип їх роботи полягає в тому, що користувачі безпосередньо підтримують канали передачі даних і виконують маршрутизацію пакетів даних по мережі. У такій мережі вузли «слухають» один одного, і якщо один з них виходить з ладу, то ті вузли, що були підключенні до нього, шукають альтернативні вузли для підключення. Такий спосіб організації мережової взаємодії [8] зробив Інтернет доступнішим в тій місцевості, де централізовані провайдери не стали розміщувати своє обладнання з різних причин.

Децентралізовані обчислювальні системи

Децентралізовані обчислювальні системи (*grid systems*) – це системи, що використовують розподілені комп'ютерні ресурси для

досягнення спільної мети (рис. 1.2). Кількість вузлів в таких системах може коливатися від декількох машин до сотень і тисяч робочих станцій.

Такий підхід вперше був запропонований в 1999 р. у публікації «The Grid: Blueprint for a new computing infrastructure». У тому ж році був запущений перший проект, в якому реалізований даний підхід, під назвою SETI@home [10]. На сьогодні існує безліч реалізацій подібних проектів, таких як BOINC, Folding@home, Einstein@Home тощо. Відзначимо, що вищезгаданий проект SETI@home, що з'явився раніше за всіх, і дотепер є одним з найпотужніших розподілених суперкомп'ютерів.

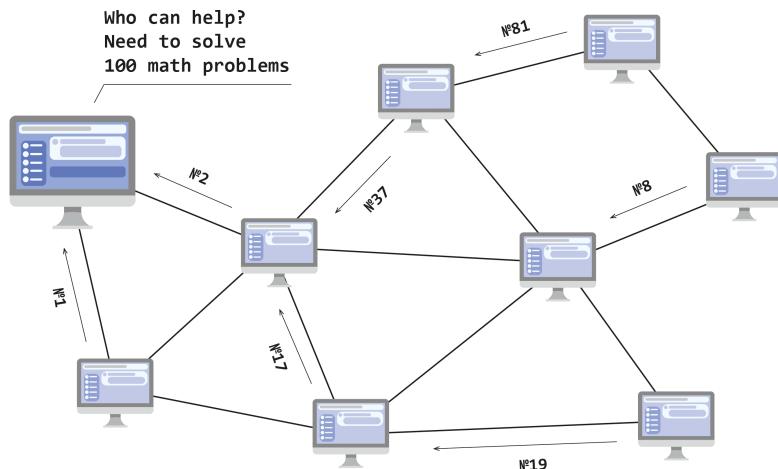


Рис. 1.2 – Схема передачі результатів обчислень в децентралізованих обчислювальних системах

Децентралізовані системи зберігання даних

Перераховані вище проекти дозволили зрозуміти, в якому напрямку можна змінити існуючі системи зберігання даних. Децентралізований підхід до побудови таких систем передбачає, що різні фрагменти файлів зберігаються різними вузлами мережі (рис. 1.3).

У 2001 році з'явився BitTorrent – протокол, що дозволив працювати швидко, ефективно і був не тільки відмовостійким, але і незалежним. Звичайно, спочатку для роботи був потрібен централізований клієнт, але пізніше з'явилися torrent-клієнти, яких важко відстежити, а використання VPN (Virtual Private Network) дозволило підвищити рівень анонімності користувачів. І саме BitTorrent на сьогоднішній день є все ще функціонуючим продуктом та символом децентралізованого підходу – підходу, який успішно працює і донині.

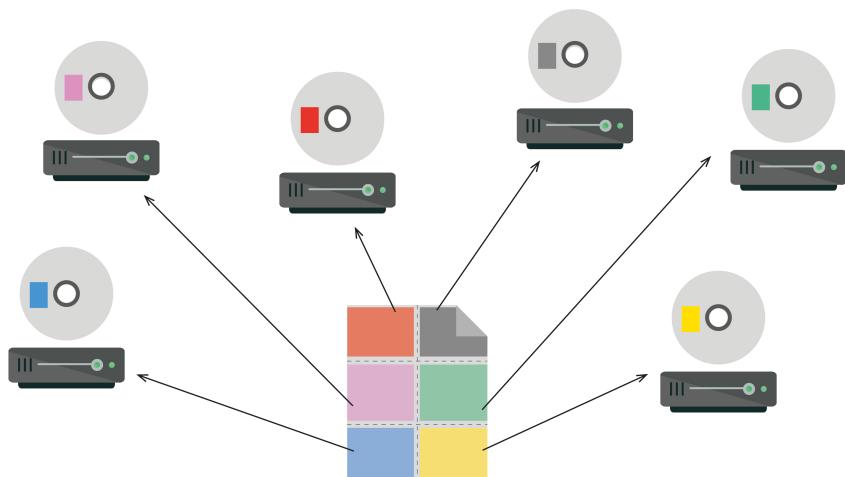


Рис. 1.3 – Схема розподілення фрагментів файла між учасниками децентралізованої системи зберігання даних

Крім BitTorrent існують інші цікаві рішення, що підтримують децентралізоване зберігання даних. Одним з таких є розподілене сховище IPFS [11]. Суть функціонування цієї системи полягає в тому, що користувачі не завантажують файли з централізованих серверів, а безпосередньо обмінюються ними між собою. Ідея IPFS доволі схожа з концепцією World Wide Web. Кожному файлу в системі присвоюється унікальний ідентифікатор, який є його геш-значенням. Для відстеження історії цього файлу використовується Git (система управління версіями). Подібний підхід дозволяє забезпечити доступ

до найбільш актуальної версії контенту, і при цьому гарантувати його автентичність. Пошук певного файлу можливий як за його ідентифікатором, так і за зрозумілим для людини іменем. Для цього використовується децентралізована система імен IPNS.

Децентралізовані системи прийняття рішень

Іншим цікавим способом застосування децентралізованого підходу є системи децентралізованого прийняття рішень. Наведемо приклад, коли 5 людей поклали до сейфу торт і домовилися, що з'їдять його тільки у тому випадку, якщо цього захоче більшість з них. Тому вони розділили секрет від кодового замку і розподілили його між собою. Після цього торт можна буде з'їсти, тільки якщо більшість з учасників відкриють свої секретні частини та знімуть замок з сейфу (рис. 1.4)



Рис. 1.4 – Прийняття рішень незалежними учасниками

На сьогодні дуже великі фірми не можуть керуватися однією людиною, а якщо такі й існують, то їх ефективність знаходитьться під великим сумнівом. Тому практично у будь-якій достатньо великий

1. Децентралізація в інформаційних системах

організації існує рада директорів, безліч радників, а іноді право голосу в прийнятті рішень надається навіть співробітникам компанії. Практика показує, що такий підхід дійсно підвищує ефективність компанії завдяки співпраці людей, які мають різні погляди, різні способи оцінки конкретної проблеми та різні підходи до її рішення. Таким чином, кінцеве рішення, прийняте незалежними сторонами, можна вважати більш об'єктивним.

З розширенням зв'язку керівництва вищого рівня з керівництвом, яке знаходиться на середньому і низовому рівнях, продуктивність організації зазвичай збільшується. На сьогодні все більше і більше організацій переходят від ієрархічного способу управління до більш децентралізованого, що вже принесло і продовжує приносити свої плоди.

Децентралізовані платіжні системи

Наступним кроком стала децентралізація платіжних систем. Їх було набагато складніше децентралізувати зі зрозумілої причини – чутливості людей до всього, що безпосередньо пов'язане з безпекою їх грошей.

Винахід *грошей* піднес поняття приватної власності до того рівня, де її значення стало набагато легше оцінити (можливість об'єктивної оцінки – одна з основоположних властивостей грошей). Гроші були історично прив'язані до товарів, таких, як золото, корови, хутро, мушлі, сигарети тощо. Рівень добробуту людини базувався на тому, яка кількість товару їй належить.

На сьогодні гроші стали цифровими: просто число у базі даних, яке відображає відносини між людьми; засіб оцінки можливостей, влади та статусів людей відносно один одного. Проблема з грошима такого роду полягає у непрозорому випуску, який базується на рішеннях окремих людей, а не на загальній згоді, що доволі логічно, адже сама по собі задача досягнення загальної згоди відносно монетарної політики є дуже складною.

У 2009 році поява Bitcoin як першого дефіцитного цифрового товару надихнула людей на ідею відокремлення грошей від держави

чи банків (в незалежності від того, наскільки вони життєздатні). Наприклад, те ж саме трапилося в деяких розвинених країнах століття назад, коли релігія та преса стали існувати незалежно (майже...) від держави. Тим не менш, на сьогодні поняття *єдиної національної валюти* досі передбачено у конституціях більшості країн.

Головне питання полягає у тому, чи можливо створення ефективної платіжної системи з необмеженою від самого початку емісією? Системи, яка здатна наслідувати моделі паперових грошей, але при цьому позбавленої впливу окремих осіб? Можливо. Час покаже. Що можна сказати напевно – це те, що можливість створення цифрового дефіциту (обмеженої математичної емісії) та запрограмованих правил роботи (конституції, що гарантується криптографією) є революційною для багатьох аспектів життя та поза сумнівом буде продовжувати розвиватися. З цієї причини, розуміння принципів роботи Bitcoin є невід'ємною складовою підготовки до нового цифрового світу.

Саме на прикладі Bitcoin в першій частині книги ми розглянемо особливості роботи децентралізованої облікової системи, оскільки багато принципів, згідно до яких він був спроектований і реалізований, є фундаментальними для будь-якої децентралізованої системи.

1.3 Застосування принципів децентралізації

У цій темі конкретизуються та формалізуються *принципи децентралізації* та особливості їх застосування в інформаційних системах. Наприклад, вони вже успішно застосовуються в системах зберігання даних (IPFS), обчислювальних системах для розподілу навантаження (BOINC project), mesh-мережах (Open Garden), телекомунікації (Tor, I2P), месенджерах (Tox, BitMessage), мережах розповсюдження контенту (BitTorrent), а також знаходять застосування у цифрових валютах.

Обмеження та проблеми централізованих систем

В основі централізованих систем закладено централізоване управління процесами. У деяких випадках подібний підхід може забезпечити більшу ефективність функціонування системи. Яскравим прикладом можна навести можливість простого та швидкого оновлення правил протоколу. Уявімо, що у централізованій обліковій системі виявляється вразливість. Розробники швидко з'ясовують причину проблеми та випускають відповідне оновлення. В результаті всі користувачі, що хочуть надалі взаємодіяти з обліковою системою, змушені оновити своє програмне забезпечення. Процес оновлення у цьому випадку відбувається швидко та максимально безболісно.

Як працюють традиційні платіжні системи

- ❖ База даних зберігається на головному сервері (хмарі чи кластері)
- ❖ Система керується централізовано
- ❖ Користувачі відправляють запити до системи для проведення транзакцій

Однак мають місце певні ризики, які необхідно враховувати при роботі в такій системі. Одним з них є можливість повної відмови системи. При виникненні певного роду ситуацій, ключові компоненти системи можуть відмовити і тим самим привести до повної втрати її функціональності. Наявність систем резервування в деякій мірі пом'якшує ситуацію, однак і такий підхід не завжди може гарантувати безперебійну роботу сервісу.

Традиційні фінансові інструменти працюють по принципу, згідно з яким внутрішню облікову систему необхідно захищати з допомогою грубої сили [12]. Мається на увазі, що центральний сервер, на якому знаходиться база даних, захищений тільки вздовж периметру. Якщо подолати зовнішній захист, то сама база даних залишиться незахищеною. В цьому і криються деякі недоліки. З однієї сторони, якщо атакуючий подолає цей захист, то він може отримати повний доступ до даних та можливість їх модифікації. З іншого боку, такий підхід не дозволяє користувачам особисто перевіряти дані.

Користувач може тільки відправити запит до серверу, який в свою чергу обробить цей запит і згодом надішле відповідь (рис. 1.5).

Для звичайного користувача внутрішня структура такої системи обліку не прозора та відсутні будь-які гарантії правильності її роботи, однак у випадку збою чи відмови в обслуговуванні є людина, яка несе за це відповідальність. Крім того, централізована облікова система має єдину точку відмови.

Якщо необхідно провести перевірку облікової системи, прийдеться робити це вручну чи використовувати деякі інструменти автоматизації, причому велика ймовірність, що її буде здійснювати аудитор. До 2009 року так працювали всі облікові системи.

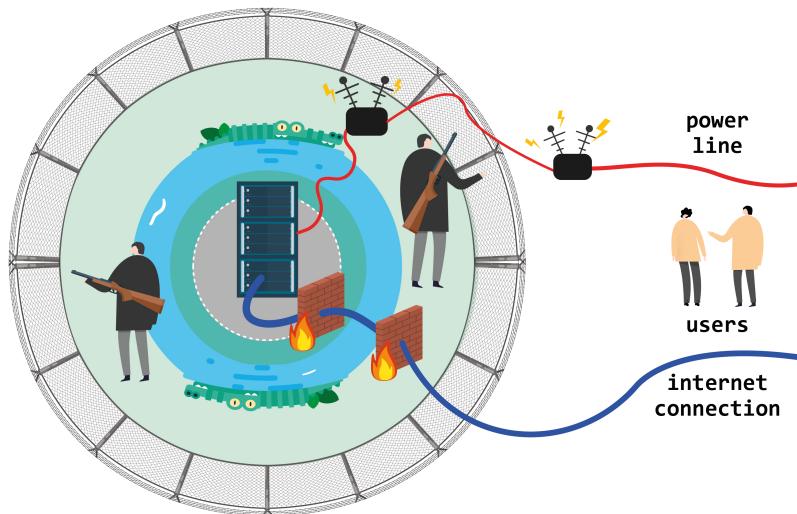


Рис. 1.5 – Принципи захисту традиційних систем

Потенційна можливість цензурування дій користувача у системі також є одним з недоліків. Централізована система передбачає повну і беззастережну довіру користувача до власника і керівництва організації. Такий підхід містить у собі загрозу, що правила протоколу взаємодії в системі можуть бути порушені, якщо власнику системи це буде вигідно.

Застосування децентралізованого підходу

Історично люди будували системи, що копіюють звичну модель соціальних відносин, тому більшість систем, які ми бачимо навколо, побудовані за принципом ієрархії. Існує чимало сфер, де ієрархічна модель добре працює, але такий підхід потенційно пов'язаний з низкою проблем.

Проблеми, вирішення яких пропонує децентралізація

- ❖ *Можливість цензури*
- ❖ *Наявність єдиної точки відмови*
- ❖ *Необхідність довіряти власнику системи*

Зауваження: цензура у контексті облікової системи означає, що конкретна сторона (наприклад організація, що обслуговує систему) може виконувати дії, такі як блокування облікових записів користувачів та зміна даних транзакцій на власний розсуд.

Децентралізація можлива, коли йдеться про взаємодію рівноправних сторін. Протягом останніх двадцяти років були розроблені технології, які дозволяють реалізувати системи з рівноправними взаємовідносинами (*peer-to-peer*) між учасниками. З'явилася можливість здійснювати ряд процесів децентралізовано, при цьому зберігаючи достатній рівень автоматизації. Тим не менш завдання децентралізації майже завжди дуже складне та не має тривіального рішення, не кажучи вже про готові технології та вдалі практики застосування.

Принципи побудови децентралізованих систем

Далі будуть перераховані основні аспекти децентралізації, які пов'язані з новими технологічними та організаційними ризиками. Цей матеріал допоможе набагато краще відчути особливості та складності на шляху проектування, розробки і використання децентралізованих систем.

Базові принципи децентралізації

- ❖ Максимальне збільшення рівня незалежності кожного компонента системи
- ❖ Збереження балансу між ефективністю роботи та засобами, що застосовуються
- ❖ Децентралізація можлива лише за умови збереження цілісності всієї системи [13]

Перш ніж продовжити, слід згадати про способи взаємодії користувачів з системою. На рис. 1.6 зображені три підходи [14], що принципово відрізняються один від одного за своїм устроєм.

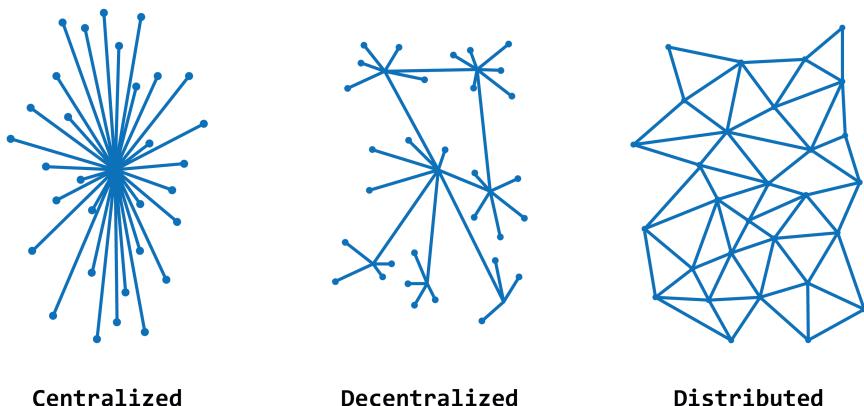


Рис. 1.6 – Види систем в залежності від способу взаємодії користувачів між собою

Зauważення: тут і далі (на малюнках і протягом тексту) ми будемо часто вживати стійкі вирази та терміни в оригіналі (англійською), щоб було менше розбіжностей у подальшому.

До централізованих систем можна віднести популярні соціальні мережі. Порушення роботи бази даних в таких системах торкнеться всіх користувачів.

До децентралізованих систем – банківську систему в цілому, бо її утворюють безліч локальних центрів, і несправності, наприклад, в

1. Децентралізація в інформаційних системах

банку Аргентини, не приведуть до затримок платежів у банках Німеччини.

До розподілених систем можна віднести mesh-мережі та систему зв'язку на основі кишенькових рацій, де система підтримується тільки пристроями користувачів, а відключення одного з пристрій не вплине на взаємодію інших користувачів.

Зauważення: для позначення систем другого та третього типів ми будемо вживати загальний термін – децентралізована система, бо обидва випадки мають на увазі відсутність центрального вузла.

Облікова система – це окремий випадок автоматизованої системи обробки даних, яка передбачає наявність деякої бази даних і необхідності прийняття рішень стосовно її оновлення (рис. 1.7).

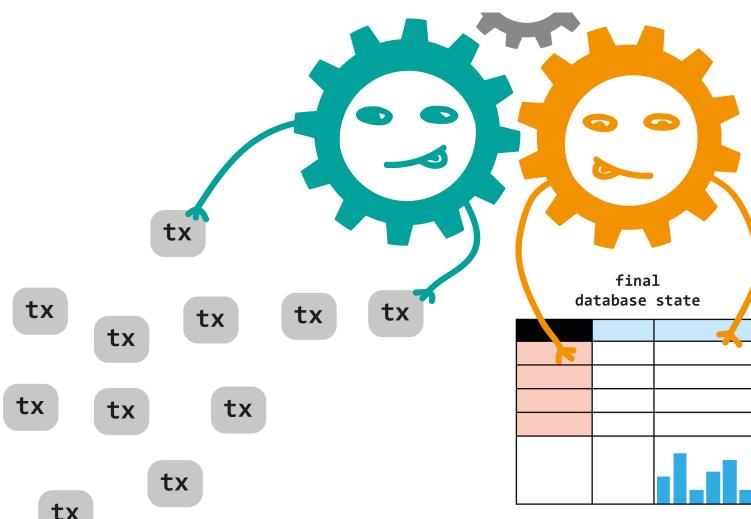


Рис. 1.7 – Архітектура облікової системи

Зauważення: під абревіатурою tx в цьому місці та в подальшому ми будемо мати на увазі транзакції.

Централізована облікова система включає до себе базу даних, механізми її оновлення та керуючий центр, відповідальний за підтримку її роботи. Керуючий центр не завжди може забезпечити достатній рівень безпеки обробки даних і надійності прийняття рішень. У пошуках кращих рішень світ прийшов до ідеї децентралізації облікових систем.

Зауваження: ми будемо використовувати термін «дані», коли мова йде про послідовність байт, що піддається передачі, зберіганню та обробці автоматизованими системами, а термін «інформація» – коли маються на увазі деякі знання або відомості, якими обмінюються або які запам'ятовують люди.

Типова архітектура децентралізованих систем

Децентралізована облікова система – це окремий випадок облікової системи, принциповою відмінністю якої є використання механізму досягнення консенсусу (згоди) між декількома незалежними сторонами (рис. 1.8). Отже, кожна сторона будує власну базу даних, а алгоритм досягнення консенсусу гарантує, що кожна побудована база даних ідентична іншим копіям. В узгодженні кінцевого стану всіх копій беруть участь безліч незалежних сторін (валідаторів), а не одна уповноважена сторона (центр).

1. Децентралізація в інформаційних системах

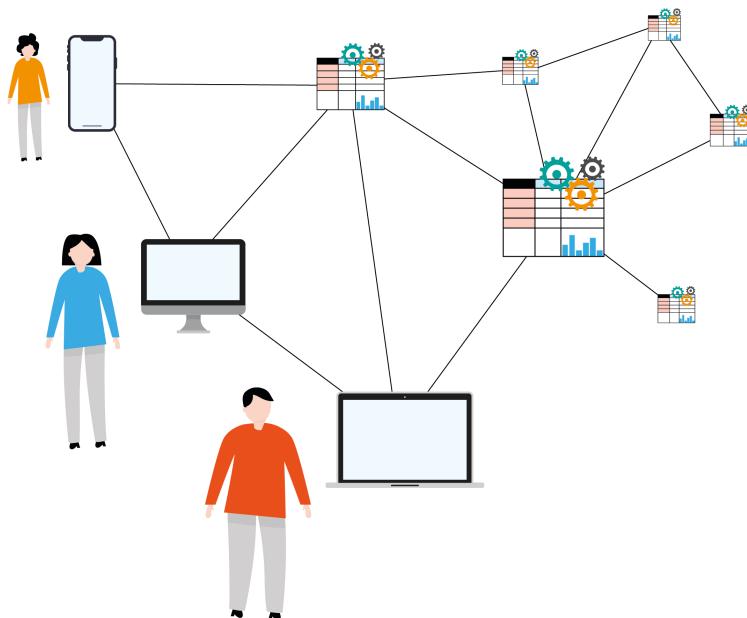


Рис. 1.8 – Архітектура децентралізованої облікової системи

Переваги децентралізованих систем

У загальному випадку децентралізована система передбачає, що учасники обмінюються інформацією безпосередньо, використовуючи p2p-протоколи та самостійно зберігають дані, що потрібні для них самих. Для цього вони запускають спеціальне програмне забезпечення, яке підтримує необхідний p2p-протокол конкретної децентралізованої системи. У децентралізованих системах обліку фінансів, таких як криптовалюти, передбачається, що всі учасники зберігають копії однієї і тієї ж бази даних й оновлюють їх, використовуючи алгоритми досягнення консенсусу.

- ❖ *Відмовостійкість*
- ❖ *Незалежність від одноосібного контролю*
- ❖ *Trustless (відсутнія необхідність у довірі третій стороні)*
- ❖ *Permissionless (вільне використання)*

- ❖ *Persistence* (незмінність кінцевого стану бази даних)
- ❖ *Liveness* (гарантується додавання записів)
- ❖ *Формальність* протоколів

Почнемо з *відмовостійкості*. Відмовостійкість є властивістю системи, за якої система зберігає свою працездатність навіть після відмови одного або декількох її компонентів. У традиційній клієнт-серверній архітектурі основні зусилля спрямовуються на захист центрального серверу. Якщо атакуюча сторона заволодіє сервером та отримає доступ до бази даних, то вона може переписати історію на власний розсуд. Атакуючий децентралізованої системи оперуючи одним сервером отримує доступ до бази даних, але він не зможе завдати критичної шкоди системі. Принципи децентралізації багато років успішно застосовуються при проектуванні та побудові авіаційної та космічної техніки, а також при роботі високоточних обчислювальних систем. Наприклад, при роботі в нестабільних умовах дуже важливо, щоб основні системи (навігації, зв'язку, управління тощо) працювали надійно. У таких випадках проектувальники систем вдаються до використання *надмірності* (див. 1.1).

Незалежність від одноосібного контролю є ще однією відмінною рисовою децентралізованої системи. За наявності великої кількості незалежних учасників ніхто, навіть дуже зацікавлена сторона, не може вплинути на прийняття рішення на свою користь.

Властивість *trustless* полягає у відсутності необхідності довіряти системі щодо зберігання й обробки деяких даних або виконання деяких процесів. Зазвичай вона досягається завдяки великій кількості незалежних учасників, що досягають згоди у прийнятті спільногого рішення. Вочевидь, що зростом кількості незалежних (незнайомих) учасників сильно знижується ймовірність їхньої змови.

Властивість *permissionless* значить, що система доступна для роботи без будь-яких додаткових дозволів (відсутні ѹерархія зумовлених ролей). Будь-який бажаючий може читувати та записувати дані, здійснювати їх аудит, а також брати участь у

прийнятті спільного рішення, тобто у процесі управління. Однак в низці випадків, коли мова йде про рішення, що повинні прийматися експертами, загальнодоступна участь і навіть відкритість бази даних облікової системи вже не є перевагами. Також властивість *permissionless* буде недоліком у тому випадку, коли валідатори будуть обробляти конфіденційні дані.

Властивість *persistence* має на увазі, що система зберігає незмінність кінцевого стану своєї базі даних навіть якщо вона повністю припинила свою роботу на деякий час.

Властивість *liveness* гарантує, що якщо всі чесні учасники бажають додати запис до спільної базі даних, то у результаті він буде до неї доданий.

Під *формальністю протоколів* мається на увазі, що всі учасники прийдуть до єдиного рішення якщо кожен з них жорстко дотримується завчасно встановленому алгоритму.

Обмеження децентралізованих систем

Поряд з беззаперечними перевагами (які, у свою чергу, залежать від рівня децентралізації системи), у децентралізованих системах наявні деякі обмеження.

Перше з них полягає у відсутності служби підтримки (за визначенням), яка здатна вплинути на акаунти користувачів або транзакції. Це означає, що якщо ви випадково відправили транзакцію, і вона була додана до загальної бази даних, то вам буде нікуди звернутися за відшкодуванням, виправдовуючи це тим, що транзакція була випадковою.

Другим обмеженням є підвищена вартість підтримки системи. З плином часу база даних тільки зростає у розмірі. Це означає, що кожен її учасник повинен відводити все більше і більше ресурсів для зберігання та обробки даних.

Третім обмеженням є складність реалізації на децентралізованих платформах деяких функцій, що доступні централізованим системам. В якості прикладу можна навести підрахунок статистики чи оцінку стану системи у конкретний момент часу.

Фактори, що впovільнюють впровадження децентралізованих систем

Зі збільшенням рівня децентралізації зростає надійність і стійкість системи, проте збільшувати цей рівень не завжди просто. У процесі децентралізації можуть зустрічатися деякі складнощі та обмеження.

- ❖ Складнощі оновлення протоколу
- ❖ Проблема відповідальності
- ❖ Складний процес монетизації розробки
- ❖ Надлишковість і високі вимоги до обладнання
- ❖ Проблема масштабованості

Складнощі оновлення протоколу. Складність впровадження будь-якого оновлення протоколу взаємодії у децентралізованому середовищі полягає в тому, що запропоноване оновлення повинно бути підтримано більшістю активних вузлів мережі (рис. 1.9). Для цього стороні, що пропонує оновлення, необхідно довести необхідність його впровадження решті вузлів системи, що само собою є дуже складним завданням.

В якості одного із прикладів можна привести перехід з IPv4 на IPv6, який вимагає більше часу, ніж планували розробники. Пов'язано це з необхідністю оновлення протоколу на всіх пристроях всіх виробників. При цьому вигода для користувачів помітна далеко не відразу.

1. Децентралізація в інформаційних системах



Рис. 1.9 – Проблема оновлення протоколу

Проблема відповідальності. Будь-яке рішення в децентралізованій системі є результатом згоди більшості учасників (обраних певним чином). Тому не існує єдиної сторони, яка могла б скасувати рішення, прийняте спільно, або нав'язати своє. Але якщо користувач з власної неуважності все-таки стане жертвою шахрайів, то йому нікуди буде скаржитися, бо в загальному випадку немає відповідальної сторони та будь-яких гарантій (рис. 1.10). Тут йде мова саме про прийняття ризиків самими користувачами. А розрахунок цих ризиків є досить складним процесом.



Рис. 1.10 – Проблема відповідальності

Складний процес монетизації розробки. Монетизувати централізовану систему зазвичай легше, ніж децентралізовану. Так відбувається, тому що централізована система більш керована та може мати юридичну підтримку, оскільки адміністрація системи відповідальна за ведення діяльності в межах правового поля. При таких умовах простіше побудувати бізнес-модель і монетизувати проект. У децентралізованій системі, навпаки, досить складно ввести ефективну цензуру, забезпечити захист авторського права та контролювати використання сервісу. Створюються умови, в яких стає набагато складніше підтримувати діяльність системи у рамках правового поля. Тому розробникам протоколів децентралізованих систем складно навіть мати прибуток зі своїх проектів.

Проблема масштабованості. У разі використання механізму розподіленого прийняття рішень, потрібно, щоб всі учасники обмінялися новими даними та погодилися, які з них вважати правильними. Пропускна здатність облікової системи знижується зростом кількості валідаторів (рис. 1.11).

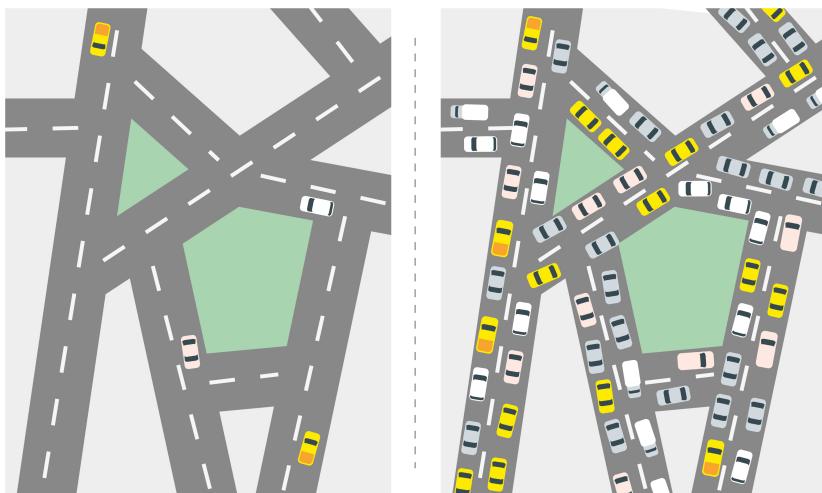


Рис. 1.11 – Приклад зниження пропускної здатності системи у зв'язку зі збільшенням кількості її користувачів

1. Децентралізація в інформаційних системах

Децентралізовані системи також стикаються з необхідністю зберігання надлишкового обсягу даних і високими вимогами до обладнання. Детальніше ці обмеження розглядатимуться далі (детальніше у 5.3).

Існують й інші фактори, що можуть стояти на шляху розповсюдження програмного забезпечення, яке призначено для роботи у децентралізованому середовищі. Наприклад, мережевий трафік легко підається фільтрації з боку інтернет-провайдеру, а значна частина програмного забезпечення поширюється через такі централізовані сервіси, як GitHub, Apple Store, Google Play тощо. Як відомо, такі сервіси здатні на суб'єктивну цензуру (рис. 1.12). Додатки можуть її не пройти або ж бути видалені навіть після успішного існування на протязі тривалого часу.

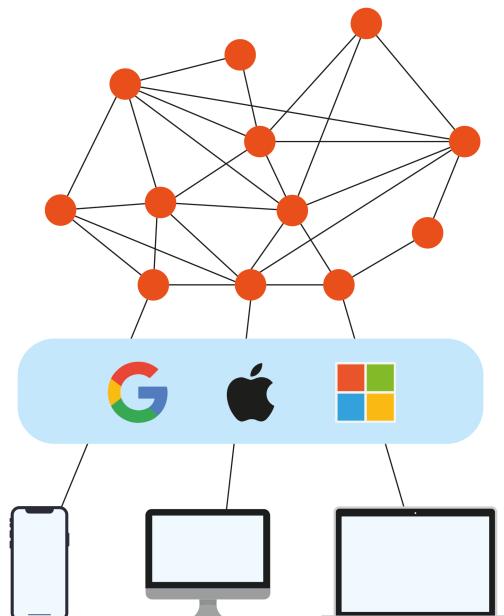


Рис. 1.12 – Постачальники програмного забезпечення для роботи в децентралізованих системах

Висновки

Порівняння децентралізації з централізацією не завжди є гарною ідеєю, так як усе залежить від вимог та умов експлуатації.

Централізована система має низку корисних властивостей. Керувати такою системою куди легше та зазвичай відомо, хто несе відповідальність за її роботу. Рішення в таких системах зачасту приймаються доволі швидко. Можна побудувати цілком конкретну бізнес-модель і дотримуватися її, що є перевагою, коли мова йде про монетизацію.

Принципи децентралізації використовують інженери, які проектують системи з високими вимогами до надійності роботи, наприклад, системи управління авіаційним обладнанням. Ці принципи продовжують знаходити своє застосування і в багатьох інших сферах (енергетика, економіка, транспорт, управління різними процесами тощо).

Основна мета децентралізації – забезпечити систему властивостями, що дозволяють ефективно та надійно взаємодіяти користувачам один з одним в ситуації, коли вони не довіряють якомусь центральному органу чи посереднику. Криптографічні алгоритми, протоколи спільного прийняття рішень і технологія blockchain стали фундаментом, на якому можна побудувати дійсно прозору, захищена та досить ефективну *децентралізовану облікову систему*.

2. ІСТОРІЯ ТА ПРИНЦИПИ ФУНКЦІОNUВАННЯ BITCOIN

2.1 Що таке Bitcoin?

Можна сказати, що Bitcoin – це протокол, що реалізує незалежну валюту та платіжну систему. Тобто, якщо розглядати інші електронні гроші чи платіжні системи, наприклад, WebMoney, PayPal, – це платіжні системи, які оперують вже існуючими валютами: долар, євро, фунт тощо. Bitcoin є як окремої валютою, так і платіжною системою, яка керує цією валютою. Важливо розуміти, що це незалежна платіжна система, тобто немає організації, яка б контролювала її роботу.

Зауваження: далі ми будемо використовувати слова «Bitcoin» і «Біткоін», коли мова йде про платіжну мережу чи протокол, а слова «bitcoin» і «біткоін», якщо мається на увазі валюта або відповідні монети.

У спробах зрозуміти, що таке Bitcoin, люди нерідко звертаються до Wikipedia, де написано, що це пірнгова платіжна система, яка використовує власні монети, як одиниці обліку цінності, а для забезпечення функціонування та захисту системи використовуються криптографічні методи. Для людини, не досвідченої в питаннях платіжних систем, таке визначення може виявитися складним і незрозумілим у повному обсязі, особливо якщо вона чує про Bitcoin вперше. Доведеться підібрати більш зрозумілі слова. Кращою з аналогій, що зустрічаються у публікаціях на цю тему, є аналогія з цифровим золотом (рис. 2.1).

Можна припустити, що творець Bitcoin дійсно спробував відтворити всі властивості золота, такі як: обмежена кількість, складність видобутку, незалежність від єдиної організації, неможливість його штучного відтворення. Той факт, що Bitcoin чітко

відтворює перераховані властивості у цифровому вигляді, можна вважати великим проривом у комп'ютерних науках.



Рис. 2.1 – Bitcoin як цифрове золото

Використовуючи Bitcoin, можна відправити платіж кому завгодно і куди завгодно. Для цього потрібен доступ до Мережі, цифровий гаманець та адреса отримувача. Обмеження, характерні для звичайного міжнародного переказу, просто відсутні. Ніяких додаткових дозволів для здійснення платежу не потребується.

Тому Bitcoin зацікавив людей, які підтримували анархізм, ліберальні ідеї, повну приватність тощо. Саме у них Bitcoin і здобув популярність спочатку. Пізніше до них приєдналися комп'ютерні ентузіасти (шифропанки, хакери), а також вчені, для яких Bitcoin став об'єктом для досліджень і проведення цікавих експериментів. Як тільки ціна біткоіну стала хоч якось помітною, він почав привертати увагу підприємців і спекулянтів, що намагалися заробити на коливанні курсу. Для звичайної людини інтерес представляють відсутність необхідності реєструватися і можливість здійснювати платежі без залучення третіх сторін.

Якщо розглядати такі платіжні системи, як PayPal або WebMoney, то вони керуються конкретними компаніями, куди можна прийти з обшуками, забрати сервери та заблокувати рахунки. У разі Bitcoin не існує компанії Bitcoin, яка здійснює облік монет або підтверджує транзакції. Це означає, що транзакції не схильні до цензури. Дана

2. Історія та принципи функціонування Bitcoin

властивість є дуже важливою і пізніше ми обговоримо, яким чином вона досягається.

Історія виникнення Bitcoin

Ми не знаємо хто вперше запропонував дану технологію і назвав її Bitcoin. Офіційно відомо, що це був хтось під псевдонімом Сатоші Накамото. Можливо, цей хтось – одна людина, але є припущення, що за псевдонімом може стояти і група людей. Сатоші зареєстрував домен bitcoin.org в 2008 році, випустив першу статтю, опублікував початкову версію вихідного коду протоколу. До 2011 року від псевдоніма Satoshi Nakamoto на відповідних форумах і в email-розсилках з'являлися повідомлення. Пізніше він написав, що вирішив займатися іншими справами та припинив публічні комунікації.

Проте варто визнати, що ідея створення Bitcoin виникла у Сатоші Накамото зовсім не на рівному місці. У своїй статті «Bitcoin: A Peer-to-Peer Electronic Cash System» [15] (рис. 2.2) він згадав два інших ключових проекта.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
 satoshin@gmx.com
 www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Рис. 2.2 – Перша публікація про Bitcoin

Це були попередні спроби створити незалежну цифрову валюту: HashCash доктора Адама Бека (Adam Back) [16] і B-Money інженера Вей Даю (Wei Dai) [17]. У першому з'явився підхід proof-of-work, спочатку створений для боротьби зі спамом в електронних листах, а в іншому – модель мережі для розподіленого зберігання даних про транзакції та використання криптографічних підписів для відправки грошей.

Таким чином, Сатоші задіяв вже існуючі концепції для реалізації Bitcoin, зумівши вирішити проблеми, що залишилися на ранніх етапах, чого не вдалося зробити їх творцям. Вважаємо, що знайдеться небагато людей, які здатні були б розгледіти у вищезазначених провальних проектах свого роду ембріон незалежної цифрової валюти.

Передумови до створення Bitcoin

2. Історія та принципи функціонування Bitcoin

- ❖ *David Chaum – DigiCash [18] (1989)*
- ❖ *Adam Back – HashCash (1997)*
- ❖ *Nick Szabo – BitGold [19] (1998)*
- ❖ *Wei Dai – B-Money (1998)*
- ❖ *Hal Finney – RPoW as e-money [20] (2004)*

Однак потрібно розуміти, що Bitcoin – це перша успішна реалізація децентралізованої системи обліку. До нього були й інші спроби, наприклад, компанія DigiCash, яку заснував David Chaum в 1989 році, однією з найперших запропонувала цифрові платежі зі спеціальною валютою, яка називалася Ecash. Користувачі платіжної системи були анонімними, так що банки не могли відстежити їх рахунки. Проект підтримали тільки декілька інноваційних банків в США та один у Фінляндії, але оскільки було дуже складно переконати інші банки та продавців приймати анонімну валюту, проект згорнули.

Одним з перших кроків в розвитку Bitcoin була, власне, публікація Bitcoin White Paper – 31 жовтня 2008 року. Перший вихідний код був опублікований в 2009 році, 3 січня. Тоді ж був сформований і перший блок – в Bitcoin з'явилися перші 50 монет. Тому можна вважати цю дату запуском валюти. У лютому 2010 року відбувся перший обмін біткоіну на гроші.

Ключові дати

- ❖ *Bitcoin White Paper – 31 October 2008*
- ❖ *Genesis Block – 3 January 2009*
- ❖ *First Bitcoin Exchange – February 2010*
- ❖ *P2SH accepting – 5 January 2012*
- ❖ *BCash fork – 1 August 2017*
- ❖ *Segregated Witness accepted – 24 August 2017*
- ❖ *Lightning Network – 15 March 2018*

Важливою в історії Bitcoin подією став форк Bcash (відгалуження від основної цифрової валюти), який відбувся 1 серпня 2017 року. Ще одне важливе оновлення, що реалізує низку певних покращень протоколу, які в свою чергу відкрили для Bitcoin раніше не досяжні можливості, – це оновлення Segregated Witness, що було активовано 24 серпня 2017 року. А 15 березня 2018 року світ побачив надбудову над Bitcoin для здійснення миттєвих платежів – Lighting Network.

Статистика по мережі Bitcoin на 2018 рік

- ❖ Близько 10 мільйонів унікальних користувачів
- ❖ У середньому 300 тисяч платежів на добу
- ❖ Добовий обсяг торгів – 15 мільярдів доларів

На момент 2018 року по всьому світу Bitcoin користуються мільйони людей, сотні тисяч компаній приймають його в якості оплати. На базі Bitcoin розробляється безліч проектів. Деякі країни, зокрема Японія, визнали його законним засобом платежу.

Проблеми, які здатний вирішити Bitcoin

Перш за все, Bitcoin отримав свою популярність через те, що він реалізує децентралізовану облікову систему, тобто працює незалежно від режимів, що діють в різних країнах, не схильний до інфляції, не дозволяє скасовувати транзакції та спирається тільки на математику, а не на забаганки окремих людей. Крім того, платежі у Bitcoin можуть допомогти підвищити рівень конфіденційності користувачів у порівнянні з цифровими валютами, що існували до нього.

- ❖ Фінансовий інструмент, який працює без обмежень
- ❖ Відсутня обов'язкова реєстрація користувачів
- ❖ Bitcoin можна використовувати анонімно
- ❖ Стійкий до цензури

Звичайно, ці властивості приваблюють споживача. Наприклад, для бізнесу вони виступають гарантам того, що якщо покупець

2. Історія та принципи функціонування Bitcoin

відмовився від товару, то він не може автоматично вимагати повернення грошей. Подібна проблема дуже гостро посталася для PayPal, коли відбувалося блокування рахунків бізнесів з повідомленням «на вас подана скарга», а десятки тисяч доларів могли бути заблоковані на півроку – в таких випадках бізнес повністю зупинявся. У випадку з Bitcoin це неможливо. Саме тому він став привабливим для бізнесу.

Непрозорість існуючої фінансової системи виявилася ще одним аргументом на користь Bitcoin. З історії відомі приклади, коли уряд здійснював емісію без вагомих підстав для цього, що згодом приводило до гіперінфляції та падіння рівня життя населення. Так сталося в 1990-х роках на території пострадянського простору: особисті фінанси громадян знецінилися з причин, що не були їм підвладні. Такі події цілком пояснюють, чому люди хочуть незалежно керувати своїми фінансами.

Власне, перший блок транзакцій, що з'явився, включав у себе посилання на новини про друк великої кількості готівки як спробі залагодити кризу 2008 року [21]. Платіжні системи, а саме проблеми їхнього функціонування, викликали невдоволення користувачів. Так з'явилася «Теорія всесвітньої змови», прихильники якої стверджують, що банки можуть робити з грошима клієнтів усе що завгодно (в деяких країнах так і відбувається). На практиці це відбувається пристойніше: банк приймає у клієнта фіатні гроші, натомість видає зобов'язання повернути їх на вимогу клієнта, а трохи пізніше банк відмовляється від своїх зобов'язань. Суть проблеми в тому, що для клієнта дуже складно довести таку відмову і повернути гроші.

Liquidez und Dokumentation machen das System transparenter und adipiscing elit.

- ❖ Користувач не контролює свій баланс
- ❖ Кошти можуть бути заражовані на рахунок одержувача через кілька діб, а іноді кілька десятків діб після їх відправки
- ❖ Платежі можуть бути скасовані у процесі виконання
- ❖ Кошти можуть бути заблоковані

Виникла потреба реалізувати систему, в якій люди зможуть незалежно та повністю самостійно управляти своїми грошима. Незважаючи на те, що дана задача виявилася дуже складною, з плином часу це бажання тільки посилювалося, і пошуки тривали. Рішенням став Bitcoin. Він був представлений у 2009 році. Звичайно, увага з боку суспільства не змусила довго чекати на себе.

Головні принципи функціонування Bitcoin

Якщо спробувати коротко сформулювати основний принцип функціонування Bitcoin, то він буде звучати так: *кожен користувач запускає своє програмне забезпечення, що реалізує загальний для всіх набір правил, і в результаті чого всі користувачі підтримують децентралізовану облікову систему.*

- ❖ *Копія бази даних зберігається у всіх*
- ❖ *Користувачі самостійно обробляють транзакції*
- ❖ *Користувачі дотримуються одних і тих же правил*
- ❖ *Користувачі довіряють тільки тому, що можуть перевірити самі*

Підключення та відключення учасників відбувається незалежно і не впливає на роботу інших учасників мережі. Усі зберігають й оновлюють базу даних і відповідне програмне забезпечення незалежно, усі правила роботи містяться у кожного, і всі користувачі перевіряють один одного. Мережу користувачів Bitcoin можна уявити, як на рис. 2.3.

2. Історія та принципи функціонування Bitcoin

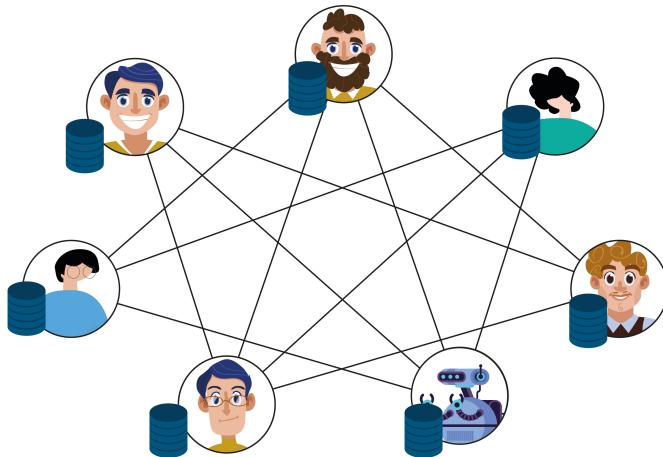


Рис. 2.3 – Схема мережі користувачів Bitcoin

Більш того, користувачі самостійно обробляють транзакції. Якщо окремий користувач згоден з певною транзакцією, то він підтверджує її. У результаті кожен з користувачів має набір транзакцій, які він верифікував і вважає правильними. На підставі цього кожен вузол мережі формує базу даних, що складається з транзакцій, з якими погодилася більшість користувачів. Як тільки чергова транзакція потрапляє в цю базу даних, вона вважається підтвердженою.

Емісія в Bitcoin

Емісія у додатку до грошей – це випуск до обігу готівки чи безготівкових грошей. У Bitcoin це не зовсім та емісія, що присутня у традиційних фінансових системах. У даному випадку емісія являє собою випуск монет за певним алгоритмом. Основний принцип полягає у тому, що весь процес повністю децентралізований та підкріплюється математичними алгоритмами. Таким чином досягається абсолютна прозорість у розподілі монет.

- ❖ Процес емісії децентралізований
- ❖ Правила емісії контролюються математично
- ❖ Емісію виконують самі користувачі

❖ *Нові монети розподіляються серед активних учасників*

За правилами протоколу, емісію може виконувати будь-який з користувачів, а всі учасники мережі перевіряють дотримання цих правил. Якщо коротко, то нові біткоіни розподіляються між користувачами, які беруть активну участь у підтримці облікової системи. Їх називають валідаторами. Тобто у системі може бути безліч учасників і кожен з них може отримати нові монети.

Правила емісії біткоїнів

- ❖ У середньому кожні 10 хвилин з'являються нові монети
- ❖ Кожні 4 роки кількість нових монет знижується вдвічі
- ❖ Усього буде емітовано 20 999 999.9769 BTC

Емісія монет визначена правилами, що закладені у самому програмному забезпеченні вузлів мережі. Сатоші встановив, що у середньому кожні 10 хвилин з'являються нові біткоіни. Спочатку це було 50 монет. Кількість нових монет скорочується вдвічі приблизно кожні 4 роки. На момент написання книги пройшло більше 8 років від початку існування Bitcoin і зараз об'єм емісії монет значно знизився.

У Bitcoin запрограмовано максимальну кількість монет – це число близько 21 мільйона. Чому 21 мільйон? Цього ніхто не знає, так вирішив Сатоші, але це насправді не важливо. Більш того, кожен bitcoin ділиться на 100 000 000 частин, а найменша одиниця називається сатоші (в честь псевдоніма творця протоколу). Вам не обов'язково мати цілу монету – ви можете володіти її частиною.

$$1 \text{ BTC} = 100 \text{ 000 000 satoshi}$$

Згідно з розрахунками кількість у 21 000 000 монет буде досягнута приблизно в 2140 році, тобто близче до середини наступного століття. Якщо точніше, то навіть менше 21 млн BTC, а саме 2 099 999 997 690 000 satoshi.

Тепер подивимося, як кількість випущених монет змінюється з часом. На рис. 2.4 представлений графік зміни кількості монет в обігу протягом певного часу. Ми бачимо, що він нагадує логарифмічну

2. Історія та принципи функціонування Bitcoin

кризу. На момент 2018 року кількість здобутих монет перевищила 17 млн BTC.

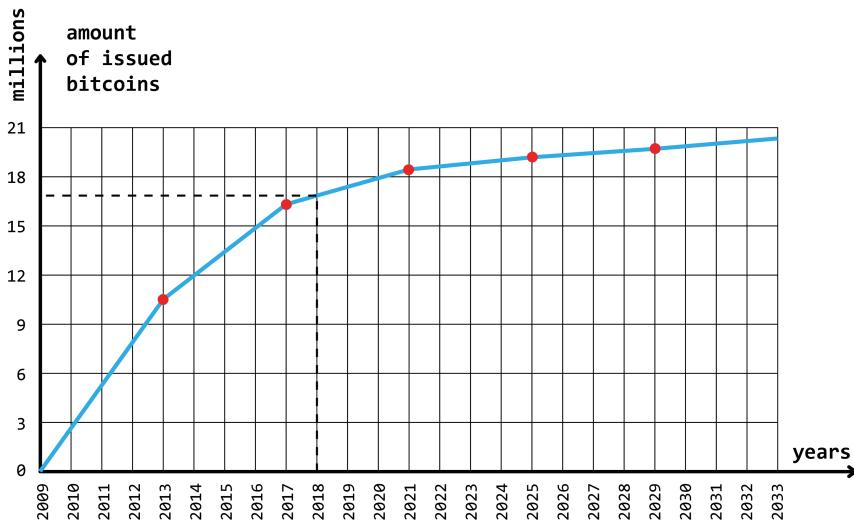


Рис. 2.4 – Графік зміни кількості bitcoin-монет в обороті з плином часу

Важливо розуміти, що Bitcoin є *scarcity* цифровим активом, так як 10 мільйонів біткоїн-монет було здобуто менш, ніж за 10 років, а для здобуття 4 мільйонів, що залишилися, знадобиться більш ніж 120 років.

Властивості bitcoin-монет

- ❖ *Обмежена кількість*
- ❖ *Необхідність добування*
- ❖ *Дискретність (подільність монет)*
- ❖ *Незалежність*
- ❖ *Неможливість скопіювати*

Bitcoin дозволяє платити кому завгодно, скільки завгодно, за що завгодно та у будь-яку точку світу. Крім того, bitcoin як валюта має низку властивостей, які роблять його придатним для зберігання