БАКАЛАВРСЬКА РОБОТА

БР. ІП - 64.00.00.000 ПЗ

Група ІП-21-3

Ватащук Олександр

2025

Івано-Франківський національний технічний університет нафти і газу
Інститут інформаційних технологій
Кафедра інженерії програмного забезпечення

Ватащук Олександр Васильович

(прізвище, ім'я, по батькові)

УДК 004.942
(індекс)

БАКАЛАВРСЬКА РОБОТА

Інтеграція програмування з блокчейном

(назва роботи)

Інженерія програмного забезпечення

(назва освітньої програми)

121– Інженерія програмного забезпечення

(шифр і назва спеціальності)

Робота містить результати власних досліджень, використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело:

Здобувач освітнього ступеня _____Ватащук О.В._____
(підпис, ініціали та прізвище здобувача)

Науковий керівник _____Зікратий Сергій Вікторович, к.т.н., доцент_____
(підпис, прізвище, ім'я, по батькові, науковий ступінь, вчене звання керівника)

Допущено до захисту
Завідувач кафедри

_доц._____Бандура В.В.__
(посада) (підпис) (дата) (ініціали та прізвище)

Івано-Франківськ – 2025

Івано-Франківський національний технічний університет нафти і газу

Інститут, факультет інформаційних технологій

Кафедра інженерії програмного забезпечення

Ступінь вищої освіти бакалавр

Спеціальність 121 – Інженерія програмного забезпечення

ЗАТВЕРДЖУЮ:
Зав. кафедрою **ІПЗ**
доцент. В.В. Бандура
“ ____ ” _____2025 р.

ЗАВДАННЯ
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТОВІ

Ватащук Олександру Васильовичу

(прізвище, ім’я, по-батькові)

1. Тема проекту (роботи) "Інтеграція програмування з блокчейном”.

керівник проекту, роботи Зікратий Сергій Вікторович, к.т.н., доцент

затверджені наказом вищого навчального закладу від “ 28 ” квітня 2025 р. № 264/7

2. Строк подання студентом проекту (роботи) 10 червня 2025 р.

3. Вихідні дані до проекту (роботи) Результати і матеріали отримані під час проходження переддипломної практики

4. Зміст розрахунково - пояснювальної записки(перелік питань, які потрібно розробити)

1 Вступ до проблеми
2 Огляд існуючих концепцій , рішень та сервісів в даній області
3 Побудова моделі або алгоритму власного рішення
4 Документування реалізації власного оригінального рішення вибраними засобами

5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)

1. Еволюція блокчейну за допомогою Google Trends (рис.1.1, ст 15)
2. Інтерес до технологій блокчейн за країнами (рис.1.2, ст 16)
3. Технологія розподіленого реєстру та блокчейн (рис.1.3, ст 21)
4. Розподіл часток ринку серед основних майнерів у біткойн-блокчейні(рис.1.4, ст 24)

6. Консультанти розділів проекту (роботи)

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

2. Дата видачі завдання _____

Керівник _____
(підпис)

Завдання прийняв до виконання_____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту	Примітка
1	Визначення та обгрунтування теми роботи	15.02.2025	виконано
2	Огляд існуючих концепцій, рішень та сервісів в даній області	25.02.2025	виконано
3	Побудова моделі або алгоритму власного рішення	15.03.2025	виконано
4	Документування реалізації власного оригінального рішення вибраними засобами	25.04.2025	виконано
5	Оформлення пояснювальної записки бакалаврської роботи	10.06.2025	виконано

Студент _____
(підпис)

Керівник роботи _____
(підпис)

АНОТАЦІЯ

Бакалаврська робота містить 65 сторінки, 4 рисунки, 1 таблиця, список використаних джерел із 26 найменування,

Метою роботи є проаналізувати технологію блокчейн у контексті її програмної реалізації, виявити її ключові риси, потенціал та обмеження, а також дослідити вплив блокчейн-додатків на суспільні та приватні сфери та розвиток людського потенціалу.

Об'єкт дослідження: технологія блокчейн як інноваційна основа для розробки програмних рішень у різних галузях.

Предмет дослідження: особливості інтеграції програмування з блокчейном, архітектура блокчейн-додатків та вплив цієї інтеграції на соціальні, економічні та управлінські процеси.

Результати дослідження: виокремлення програмних моделей реалізації блокчейну.

У першому розділі розкрито технічну сутність блокчейну, його ключові риси, потенціал для цифрової трансформації та існуючі обмеження технології.

Другий розділ - описує приклади практичного застосування блокчейн-технологій у сфері громадських благ та приватних товарів.

Третій розділ аналізує вплив блокчейну на розвиток цифрової інфраструктури, політико-правові аспекти та управління в умовах децентралізації

Висновок: блокчейн виступає не лише технічною інновацією, а й рушієм змін у цифровому суспільстві. Його інтеграція з програмуванням відкриває нові підходи до безпеки, децентралізації та довіри в IT-системах.

КЛЮЧОВІ СЛОВА: БЛОКЧЕЙН, ПРОГРАМУВАННЯ, ДЕЦЕНТРАЛІЗОВАНІ ДОДАТКИ, СМАРТ-КОНТРАКТИ, ETHEREUM, SOLIDITY, СОЦІАЛЬНО-ЕКОНОМІЧНИЙ РОЗВИТОК, ЦІЛІ СТАЛОГО РОЗВИТКУ, ПОРІВНЯЛЬНИЙ АНАЛІЗ.

ANNOTATION

The bachelor's thesis contains 65 pages, 4 figures, 1 table, a list of used sources with 26 names,

The purpose of the work is to analyze blockchain technology in the context of its software implementation, identify its key features, potential and limitations, as well as to investigate the impact of blockchain applications on the public and private spheres and the development of human potential.

Object of research: blockchain technology as an innovative basis for developing software solutions in various industries.

Subject of research: features of programming integration with blockchain, architecture of blockchain applications and the impact of this integration on social, economic and management processes.

Research results: identification of software models for implementing blockchain.

The first section reveals the technical essence of blockchain, its key features, potential for digital transformation and existing limitations of the technology.

The second section describes examples of practical application of blockchain technologies in the field of public goods and private goods.

The third section analyzes the impact of blockchain on the development of digital infrastructure, political and legal aspects and governance in a decentralized environment.

Conclusion: Blockchain is not only a technical innovation, but also a driver of change in the digital society. Its integration with programming opens up new approaches to security, decentralization and trust in IT systems.

KEYWORDS: BLOCKCHAIN, PROGRAMMING, DECENTRALIZED APPLICATIONS, SMART CONTRACTS, ETHEREUM, SOLIDITY, SOCIO-ECONOMIC DEVELOPMENT, SUSTAINABLE DEVELOPMENT GOALS, COMPARATIVE ANALYSIS.

ЗМІСТ

ВСТУП

Робототехніка та штучний інтелект стрімко зростають у використанні, масово впроваджуючи їх у виробничі процеси приватним сектором. Новіші технології також є частиною хвилі інновацій. На передньому плані тут стоїть блокчейн, нова технологія, розроблена як один з основних стовпів Bitcoin, криптовалюти, винайденої у 2008 році досі анонімним автором.Хоча штучний інтелект та робототехніка, здається, мають темну сторону, багато хто сприймає технологію блокчейн як платформу для позитивних змін – таку, що може порушити світову економіку та вирішити багато соціально-економічних та політичних проблем, з якими країни стикаються сьогодні. Хоча такі твердження, безумовно, не є новими, технологія блокчейн привертає увагу широкого кола учасників, від урядів та міжнародних донорів до приватного сектору та венчурних капіталістів.

Ці технології мають спільну рису: високий рівень складності не лише з точки зору вимог до програмного та апаратного забезпечення, але й щодо потреб у капіталі, людських ресурсах та інституційному середовищі. На відміну від мобільної «революції», нинішня хвиля інновацій може виявитися складнішою для країн, що розвиваються, якщо вони мають намір бути активними учасниками, а не лише кінцевими користувачами чи споживачами цих технологій. Вивчення актуальності нових технологій для подолання існуючих соціально-економічних розривів та підтримки міжнародно узгоджених цілей розвитку, таких як Цілі сталого розвитку, має вирішальне значення для країн глобального Півдня.

Спочатку пов'язана з фінансовими програмами, технологія блокчейн зараз впроваджується в багатьох інших сферах і секторах, включаючи розвиток і гуманітарну допомогу. Питання для країн глобального Півдня полягає не лише в тому, як це може бути реалізовано, але й у тому, хто може бути залучений до використання технологій блокчейн для подолання розривів у розвитку, сприяння соціальній інтеграції та просування демократичного управління. Мета цього

білого документа — дослідити потенціал технології блокчейн для сприяння розвитку людського потенціалу в країнах, що розвиваються. Спочатку в документі наведено нетехнічний огляд технологій блокчейн. Потім він переходить до ілюстрації спектру застосувань технології блокчейн у сферах та секторах розвитку з точки зору державних/приватних благ. У наступному розділі представлено дослідження фактичної актуальності блокчейнів у країнах, що розвиваються, з використанням структури ІКТ для розвитку (ІКТД).

Дипломна робота присвячена дослідженню інтеграції програмування з технологією блокчейн як інструменту для створення інноваційних рішень у різних секторах, зокрема в країнах, що розвиваються. Метою роботи є аналіз потенціалу блокчейн-технологій для сприяння соціально-економічному розвитку, демократичному управлінню та подоланню розривів у розвитку через створення децентралізованих програм (dApps). Дослідження зосереджується на нетехнічному огляді блокчейн-технологій, їх застосуванні в нефінансових сферах і програмних техніках для реалізації таких рішень.

У роботі розглянуто теоретичні основи блокчейну, включаючи принципи роботи децентралізованих мереж, смарт-контрактів і консенсусних алгоритмів (PoW, PoS). Проаналізовано основні платформи для розробки, такі як Ethereum, Hyperledger, Polkadot і Solana, з точки зору їх програмних інтерфейсів (API), мов програмування (Solidity, Rust, JavaScript) і можливостей масштабування.

Практична частина дослідження включає розробку прототипу децентралізованої програми на одній із блокчейн-платформ для вирішення конкретної задачі, наприклад, забезпечення прозорості в гуманітарній допомозі. Оцінюються такі аспекти, як складність розробки, безпека смарт-контрактів, продуктивність і витрати на транзакції. Додатково проведено аналіз інструментів розробки (Truffle, Hardhat, Remix) і документації платформ.

Актуальність теми. У цифрову епоху зростає потреба у децентралізованих, безпечних та прозрачних рішеннях. Блокчейн, як технологія, здатний змінити не лише технічні аспекти програмування, а й фундаментально

трансформувати соціальні інститути, моделі управління, взаємодію з даними та цифрову інфраструктуру в цілому.

Метою цього дослідження проаналізувати технологію блокчейн у контексті її програмної реалізації, виявити її ключові риси, потенціал та обмеження, а також дослідити вплив блокчейн-додатків на суспільні та приватні сфери та розвиток людського потенціалу.

Завданнями дослідження: дослідити трансформаційний потенціал блокчейндля, проаналізувати архітектуру та принципи функціонування блокчейнів, оцінити обмеження блокчів, визначити можливості інтеграції блокчейну в прикладні програми, розглянути роль блокчейну у розвитку цифрової інфраструктури, сформулювати рекомендації щодо розробки програмного забезпеченнядля сталого розвитку та цифрової безпеки.

Об'єкт дослідження: технологія блокчейн як інноваційна основа для розробки програмних рішень у різних галузях.

Предмет дослідження: особливості інтеграції програмування з блокчейном, архітектура блокчейн-додатків та вплив цієї інтеграції на соціальні, економічні та управлінські процеси.

Методи дослідження: аналіз наукових джерел, порівняльний аналіз, моделювання, систематизація.

Наукова новизна: Дослідження пропонує системний підхід до розгляду блокчейну не лише як базової технології, а як інструменту інтеграції з програмуванням. У роботі висвітлюється взаємозв'язок технічних можливостей блокчейну з прикладним програмуванням, соціальними функціями та людським розвитком.

Бакалаврська робота містить 65 сторінок, 4 рисунки, 1 таблиця, три розділи, список використаних джерел із 27 найменуванням.

РОЗДІЛ 1 ТЕХНОЛОГІЯ БЛОКЧЕЙН: ПРИНЦИПИ, МОЖЛИВОСТІ ТА ОБМЕЖЕННЯ

1.1 Трансформаційний потенціал блокчейну

Блокчейн є однією з основних технологій, що підтримують Bitcoin перша успішна децентралізована, peer-to-peer криптовалюта 12 в історії. 13 Біткойн був створений у 2008 році Сатоші Накамото, справжня особистість якого залишається загадкою. 14 Як фінансова платформа, Bitcoin потребував цифрового реєстру15 для запису всіх транзакцій , що відбуваються між користувачами криптовалюти. Блокчейн – це технологія, яка забезпечує такий реєстр. Спосіб розробки цього реєстру призвів до появи технологій блокчейн16. Програмне забезпечення Bitcoin, створене Накамото, було опубліковано в Інтернеті як програмне забезпечення з відкритим кодом (OSS), що сприяло його поширенню в глобальному масштабі з моменту його створення. У свої перші роки біткойн діяв на периферії економіки, оскільки мало хто з продавців був готовий приймати криптовалюту як законну форму 18 оплати. Однак даркнет 17 побачив речі в іншому світлі. Біткойн >1 надав анонімну форму оплати, яку неможливо було використовувати для відстеження м покупців і продавців. Нині сумнозвісний веб-сайт Silk Road 18 , онлайн-платформа для чорних ринкова платформа, широко використовувала біткойн, а біткойн-біржі сприяли конвертація криптовалюти в долари США.

Таким чином, біткойн був пов'язаний з низкою незаконної діяльності, від торгівлі наркотиками до відмивання грошей. Правоохоронні органи та регулятори звернули на це увагу та негайно почали переслідувати тих, хто брав участь у такій діяльності. Спільноті біткойнів довелося відновлювати репутацію криптовалюти, і ці зусилля окупилися через пару років.19 Це питання досі залишається актуальним для біткойна та всіх інших криптовалют, 20 але не настільки важливим для 0) технологій блокчейн, оскільки останні можуть бути повноцінно функціональними без біткойна. (Л Спочатку біткойн затьмарив

блокчейни, тому його ігнорували експерти та технологи. Але все змінилося приблизно у 2014 році, коли його потенціал як самостійної технології, що працює в секторах, відмінних від фінансів, був визнаний новаторами, а невдовзі після цього – венчурними капіталістами. На рисунку 1 зображено цю еволюцію за допомогою Google Trends. Зверніть увагу на експоненціальне зростання, що почалося у 2016 році.

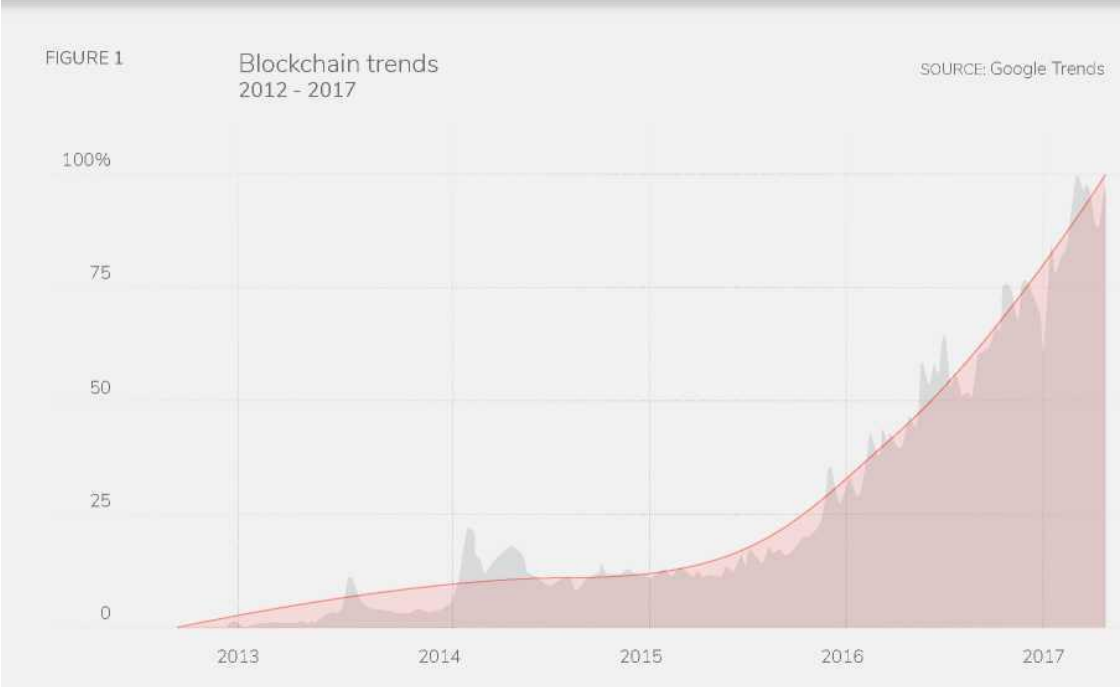

Рисунок 1.1 - зображено еволюцію блокчейну за допомогою Google Trends

коли його потенціал як самостійної технології для секторів, відмінних від фінансів, був визнаний новаторами та венчурними капіталістами. Зверніть увагу, що вісь Y відображає частку щомісячних пошуків відносно місяця з найвищою кількістю пошуків за весь період, і вона ніколи не може перевищувати 100%.

Блокчейн не лише стрімко розвивається, але й впроваджується в кількох країнах для найрізноманітніших цілей, як описано нижче. Навіть великі та традиційні фінансові установи зараз знаходяться на межі впровадження технологій блокчейн, хоча й не без попередньої спроби змінити їх для підтримки сучасних бізнес-процесів та практик.

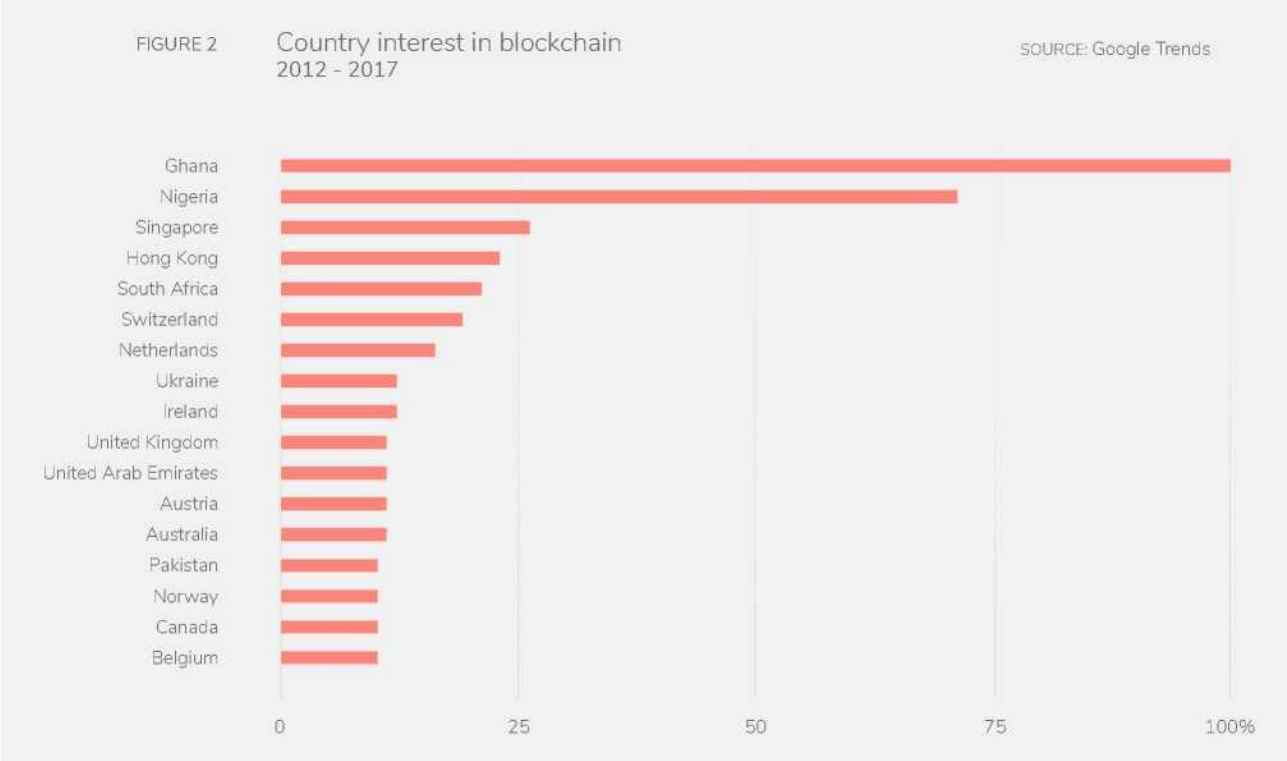

Рисунок 1.2 - Показано інтерес до технологій блокчейн за країнами.

1.2 Погляд середину блокчейнів

З точки зору неспеціаліста, блокчейн можна розглядати як електронну таблицю, яка послідовно записує транзакції між користувачами, що працюють в мережі peer-to-peer. мережа [22]. За замовчуванням електронна таблиця є публічною: усі користувачі або вузли мережі мають повний доступ до даних, записаних у базі даних, у режимі реального часу. Попередня авторизація чи дозвіл, наданий третіми сторонами або вже існуючим центральним органом влади, не потрібен. Електронна таблиця також є розподіленою [23]. Кожен вузол мережі зберігає актуальну копію даних. Аналогічно, оновлення даних автоматично поширюються мережею щоразу, коли додається новий рядок. Таким чином, не потрібен центральний комп'ютер чи сервер, який би обробляв або спрямовував трафік.

Одним з ключових нововведень блокчейну є спосіб взаємозв'язку записів або рядків. Кожен запис у публічній базі даних складається з *блоку* транзакцій [26] та має унікальний ідентифікатор. Кожен блок транзакцій пов'язаний з

попереднім або, мовою комп'ютерів, є дочірнім елементом попереднього блоку, створюючи таким чином логічний ланцюжок між блоками.

Як це досягається? Кожен унікальний ідентифікатор блоку використовується для генерації унікального ідентифікатора наступного блоку. Це створює ланцюжок пов'язаних блоків або блокчейн, де зміна вмісту або порядку рядків практично неможлива. Таким чином, будь-який блок є математичним дочірнім елементом попереднього. Єдиним винятком тут є так званий «блок генезису», перший блок або рядок у даних, який *є* сиротою, оскільки йому бракує «батьків».

На рисунку 4 показано схематичне зображення трьох випадкових блоків у фіктивному блокчейні. Наприклад, блок 112 має свій унікальний ідентифікатор і містить власний набір транзакцій. Він також містить унікальний ідентифікатор попереднього блоку та унікальну позначку часу, яка реєструє дату та час додавання запису до блокчейну.

Зрозуміло, що блокчейни набагато складніші за звичайні електронні таблиці. Це, мабуть, найкраще відображається у способі додавання записів до блокчейну.

На відміну від інших традиційних реєстрів та транзакційних платформ, нові блоки можна додавати лише після досягнення консенсусу вузлами мережі. Це називається децентралізованим консенсусом, який виключає необхідність центрального довірчого органу. Саме тому блокчейн характеризується як технологія, де довіра децентралізована:

Сама мережа забезпечує довіру між усіма партнерами. Треті сторони, що засвідчують або схвалюють поточні транзакції, не потрібні, як це відбувається у традиційних фінансових операціях та багатьох інших транзакційних мережах [27].

Такий консенсус досягається не шляхом голосування, а радше за рахунок використання обчислювальної потужності вузлів у мережі [28]. Децентралізований консенсус досягається за допомогою алгоритму підтвердження роботи, який вузли повинні запустити, щоб додати новий блок до

бази даних [29]. Підтвердження роботи нагадує здогадку про те , що головоломка з числом 30 , але має набагато вищу складність. Результат доказу роботи передається між вузлами мережі, які потім можуть підтвердити або перевірити результат. Після цього блок додається до існуючого ланцюжка записів і згодом розподіляється між усіма вузлами.

Зверніть увагу, що вузли повинні конкурувати між собою, щоб розгадати головоломку. Однак, лише спеціалізовані вузли на складному обладнанні мають 25% реальний шанс розгадати головоломку.

Криптографія

Технологія блокчейн систематично використовує криптографічні інструменти. По-перше, унікальний ідентифікатор для кожного блоку – це хеш наданих вхідних даних.31 Блок транзакцій, включений до запису блокчейну, також є результатом хеш-операції. Однак хеш-функція, що використовується в останній, відрізняється від тієї, що використовується для генерації унікального ідентифікатора блоку.32 Інформація про транзакції кодується, таким чином, неозброєним оком розкриває мало її фактичного вмісту, окрім деяких основних метаданих [33]. По-друге, всі вузли та користувачі повинні використовувати криптографію з відкритим ключем, щоб бути частиною мережі та взаємодіяти один з одним. Користувачі та вузол повинні генерувати як закриті, так і відкриті ключі, останні спільно використовуються в мережі для їх ідентифікації. Створення профілю або надання особистої інформації не є обов'язковим. Дійсного відкритого ключа буде достатньо. У цьому контексті технологія блокчейн є псевдоанонімною, що різко контрастує з існуючими платформами соціальних мереж.

Вбудовані стимули

Технології блокчейну мають вбудовані економічні стимули для вузлів, які беруть участь у конкурсі Proof of Work, а також для тих, хто хоче надавати додаткові послуги, специфічні для Bitcoin або блокчейнів, або для обох. Наприклад, вузли, які вирішують задачу Proof of Work у блокчейні Bitcoin, отримують щойно викарбувані біткоїни. Крім того, вузли також можуть

стягувати плату за кожну транзакцію, сплачену в біткоїнах користувачами, що здійснюють такі транзакції. В принципі, ці стимули повинні бути достатньо великими, щоб покрити зростаючі витрати на обладнання, енергію та інші пов'язані з цим витрати на виконання Proof of Work. Конвертація біткойнів у долари США та інші валюти була однією з перших послуг, які надавали вузли. Оскільки ринкова ціна біткойнів з часом швидко зростала, біржі стали ключовим джерелом доходу для вузлів мережі. Блокчейн створив складну екосистему послуг, яка досі виявилася прибутковою. Нещодавнє зростання ціни на біткойн та інші 26 платформи на основі блокчейну прискорить таке зростання.

Блокчейни та управління

Децентралізована природа технології блокчейн у поєднанні з появою розподіленої мережевої довіри може призвести до значних порушень у традиційних процесах управління, наприклад, сприяючи більш горизонтальним та персоналізованим формам управління.

► Нові форми прямої демократії, де всі учасники мережі можуть брати участь у процесах прийняття рішень. Одним із прикладів є ідея «рідкої демократії», яка передувала блокчейну, але тепер знайшла свою ідеальну платформу [26].

► Розширення можливостей окремих осіб шляхом децентралізації та розподілу влади між ними. Цього можна досягти за допомогою програмних агентів, які діють від імені людей, на основі протоколів, попередньо узгоджених та закодованих у блокчейні [27]. Децентралізовані автономні організації38 є гарним прикладом, як і інші форми децентралізованих організацій , що працюють за допомогою смарт-контрактів [29].

► Глобальні державні послуги, адаптовані до потреб клієнтів незалежно від їхнього місцезнаходження чи національності. Не всі версії цієї ідеї передбачають занепад національної держави. Блокчейн насправді може доповнювати або покращувати державні послуги, одночасно підвищуючи прозорість та підзвітність [20].

► Створення національних держав на основі блокчейну, таких як

Bitnation . 41

► Створення нового та більш інклюзивного соціального договору. 42

Типи блокчейнів

Хоча блокчейн біткойна є публічним та відкритим для всіх, блокчейни не обов'язково повинні мати такі характеристики для розгортання та ефективного використання. блокчейни можуть бути публічними або приватними.43 В останньому випадку лише набір попередньо вибраних вузлів може бути частиною загальної мережі та обробляти транзакції. По-друге, блокчейни можуть бути бездозволеними або з дозволом. Останній вимагає автентифікації вузлів за допомогою паролів, дайджестів та/або цифрових підписів для зчитування та/або додавання нових записів до блокчейну. В результаті, приватний блокчейн може бути бездозволеним, тоді як публічний може вимагати попередньої автентифікації перед наданням прав на запис до блокчейну. У цьому випадку лише автентифіковані вузли можуть додавати нові записи до бази даних. Вищезазначене наведено в таблиці 1.1

Таблиця 1.1

Типи блокчейнів

	Без дозволу	**Дозволено**
Громадськість	Усі вузли однорангової мережі мають повний доступ до блокчейну.	Вузли повинні пройти автентифікацію, щоб отримати доступ до запису в блокчейн.
Приватний	Усі вузли в попередньо визначеній приватній мережі мають повний доступ до блокчейну.	Вузли повинні пройти автентифікацію, щоб мати доступ для читання та запису до приватного блокчейну. Або ж, лише деякі авторизовані вузли можуть записувати в блокчейн, тоді як усі інші мають доступ лише для читання.

Деякі представники приватного сектору просувають приватні блокчейни з дозволом. З іншого боку, уряди могли б розглянути публічні блокчейни з дозволом для надання певних послуг громадянам, уникаючи використання дорогих та нестійких алгоритмів підтвердження роботи [24]. Зауважте, що використання публічно-приватних або гібридних блокчейнів також є можливим

[15] Нарешті , деякі спостерігачі назвали технологію блокчейн «технологією розподіленого реєстру» (DLT), щоб підкреслити її невалютну природу [16]. Однак не всі DLT використовують блокчейни. Corda47 та Ripple48 є прикладами DLT, які не використовують блокчейни [19]. На рисунку 1.3 об'єднано все вищезазначене та наведено схематичне зображення всіх таких варіацій.

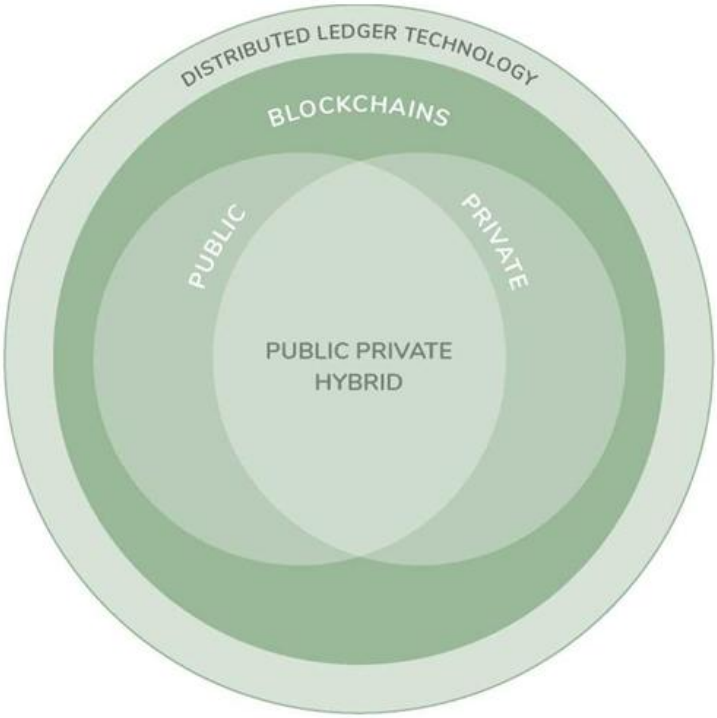

Рисунок 1.3 - Технологія розподіленого реєстру та блокчейн

1.3 Ключові риси блокчеїна

Наведена вище презентація надає необхідну інформацію для визначення ключових характеристик та принципів блокчейну. А саме:

Конфіденційність: Блокчейни не зберігають особисту інформацію та використовують приватне/публічне шифрування для автентифікації користувачів, які здійснюють транзакції. Майнінг блокчейнів для отримання особистої інформації, яку можна було б продати третім сторонам з метою отримання прибутку, неможливий.

Псевдоанонімність: Вузли та користувачі не повинні надавати імена чи особисті дані, щоб бути частиною мережі. Однак повна анонімність не досягається, оскільки пов'язування користувачів з мережевою активністю є можливим і, таким чином, може призвести до розкриття їхньої особистості.50

Цілісність: Це працює двома способами. По-перше, цілісність даних: практично неможливо змінити та підробити блоки блокчейну. Це також називається незмінністю. По-друге, цілісність користувача: метадані про транзакції, здійснені вузлом та/або кінцевим користувачем, записуються в блокчейні та можуть бути пов'язані з користувачем, який їх здійснює. Користувачі не можуть обдурити мережу або спробувати завершити недійсну транзакцію.

Розподілена довіра, управління: блокчейн успішно обходить потребу в довіреному центральному органі. Натомість довіра поширюється по всій мережі. Те саме стосується механізмів управління, де, в принципі, різні типи користувачів і вузлів мають однаковий «політичний» вплив.

Прозорість: Усі метадані та інформація блокчейну доступні всім вузлам і користувачам у режимі реального часу . Приховати або відредагувати інформацію блокчейну неможливо [11]. Розподілена прозорість є можливою , але також створює нові проблеми [12].

Безпека: Використання блокчейнів вимагає криптографічних інструментів та відкритих/приватних ключів усіма учасниками, будь то вузли чи кінцеві користувачі.

Сталий розвиток: Вбудовані економічні стимули забезпечують чіткий шлях до економічної стійкості мережі.

Відкритий код: Програмне забезпечення, необхідне для використання блокчейнів, є вільно доступним для всіх, включаючи криптографічні інструменти. Крім того, користувачі з достатніми можливостями можуть фактично допомогти вдосконалити та покращити технології блокчейн, а також виявляти помилки. Це також може сприяти поширенню інновацій блокчейну.

1.4 Обмеження блокчейну

Як технологія, що розвивається, блокчейн стикається з низкою обмежень, які можуть перешкодити широкому впровадженню не лише у фінансовому секторі, а й в інших сферах. Їх можна підсумувати наступним чином:

Масштабованість: На сьогодні блокчейн Bitcoin може додавати новий блок транзакцій лише приблизно кожні десять хвилин. Це призводить до низького обсягу транзакцій за секунду (менше п'яти), що значно менше, ніж обсяги, що повідомляються традиційними транзакційними мережами.

Розмір блоку: Вищезазначене є результатом малого розміру блоку, визначеного оригінальним вихідним кодом Bitcoin. Максимальний розмір кожного блоку становить один мегабайт, що може вмістити 2200 транзакцій. Збільшення розміру блоку наразі обговорюється, але остаточного рішення поки що не прийнято [13].

Високі витрати: Вузли майнерів використовують складне та дороге обладнання для запуску алгоритмів Proof of Work. Отже, лише певні вузли в мережі можуть ефективно конкурувати в цьому процесі, хоча теоретично всі вузли мають програмне забезпечення, необхідне для майнінгу мережі. Поняття Накамото «один процесор - один голос» більше не актуальне, оскільки витрати на обладнання та електроенергію заважають більшості вузлів брати участь у цьому процесі.

Вплив на навколишнє середовище: Побічним продуктом вищезазначеного також є доказ неефективності роботи з точки зору енергетичних ресурсів. Деякі оцінки споживання енергії свідчать про те, що до весни 2017 року споживання електроенергії біткойнами було порівнянним з використанням 280 000 домогосподарств США на рік.54 Централізація : Майнінг зараз централізований, і кілька вузлів контролюють значну частку ринку [5]. На рисунку 6 нижче зображено ринкові частки провідних вузлів або компаній-майнерів. Зауважте , що лише п'ять провідних компаній контролюють понад 50 відсотків ринку [16].

Пропускна здатність: Повноцінні вузли, які хочуть бути активними в мережі, повинні мати доступ до правильної пропускної здатності Інтернету. Повільні, ненадійні з'єднання не вітаються, особливо коли поточний розмір блокчейну перевищує 120 гігабайт [7].

Зручність використання: Технологія блокчейн вимагає безпечного управління відкритими та закритими ключами кінцевими користувачами та вузлами. Хоча існуюче програмне забезпечення для гаманців пройшло довгий шлях розвитку, втрата закритих ключів все ще є серйозним ризиком. Жодне з існуючих рішень не є стійким до фізичної крадіжки, і лише деякі можуть захистити користувачів від шкідливого програмного забезпечення [8].

Складність: технології блокчейн здаються майже незрозумілими для пересічної людини, а технічні розмови навколо них не допомагають. Лише вибрані мало хто бачить м, щоб зрозуміти технологію.

Криптографія: Використання криптографічних інструментів все ще перебуває на початковій стадії, і не можна очікувати, що пересічний користувач Інтернету почне їх використовувати в короткостроковій перспективі.

Незмінність як відповідальність: Якщо блокчейн зламано або програмний код містить помилку, яка дозволяє певний експлойт, то його незмінність може фактично стати зобов'язання. Наприклад, так сталося зі зломом Ethereum минулого року де один шахрайський вузол зміг вилучити понад 64 мільйони доларів.

Екосистема технології блокчейн справді є проактивною та вже працює над усуненням деяких із цих обмежень. Той факт, що код має відкритий вихідний код, є тут критично важливим. З іншого боку, зміни як до коду, так і до операцій блокчейну можуть бути здійснені лише за умови консенсусу або якщо більшість вузлів погодяться щодо подальших дій.

Цей графік відображає розподіл частки ринку серед провідних майнінг-пулів у біткойн-блокчейні станом на 1 квітня 2017 року. Найбільшу частку контролював AntPool (15.2%), за ним йшли F2Pool (13%) та BitFury (9.7%). Інші значні учасники включали BTCC Pool, BTC.TOP, 1Hash, ViaBTC та BW.COM з

частками від 8.9% до 5.3%. Менші пули, такі як SlushPool, Bixin, BitClub Network і Bitcoin.com, мали частки нижче 5%. Дані свідчать про високу концентрацію майнінгової потужності в кількох найбільших пулах.

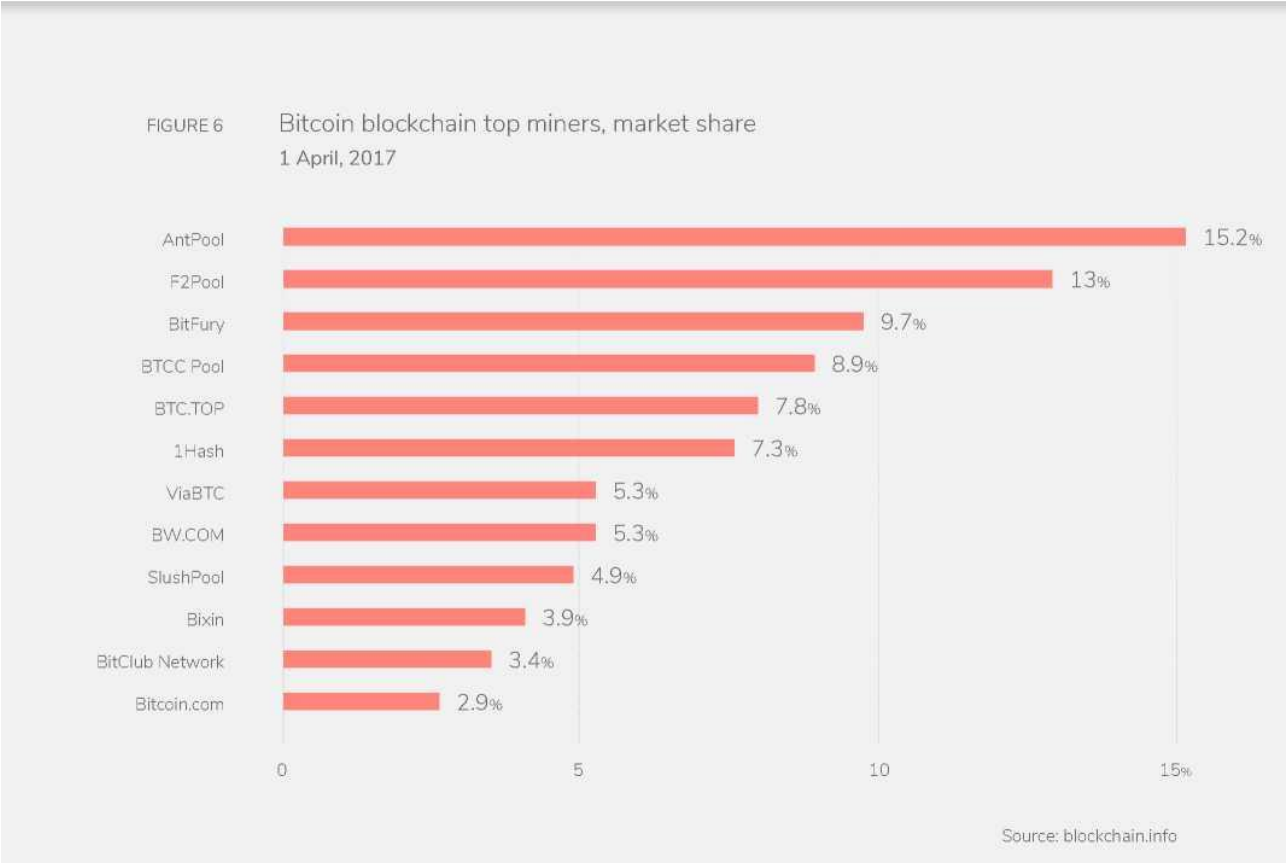

Рисунок 1.4 - Розподіл часток ринку серед основних майнерів у біткойн-блокчейні

1.5 Висновок по розділу

Блокчейн є однією з ключових технологій, що лежать в основі Bitcoin – першої успішної децентралізованої, peer-to-peer криптовалюти в історії. Біткойн був створений у 2008 році Сатоші Накамото, справжня особа якого досі залишається невідомою. Для функціонування цієї фінансової платформи був потрібний цифровий регістр для фіксації всіх транзакцій між користувачами. Таким регістром стала технологія блокчейн.

Особливості реалізації цього регістру стали основою виникнення блокчейн-технологій. Програмне забезпечення Bitcoin, створене Накамото, було опубліковане як проект з відкритим кодом (open-source), що сприяло його глобальному поширенню. У перші роки існування біткойн перебував на периферії економіки, оскільки небагато продавців визнавали криптовалюту як легітимну форму оплати.

Проте зовсім іншу роль біткойн почав відігравати в даркнеті, де став зручним анонімним платіжним засобом .

РОЗДІЛ 2 . БЛОКЧЕЙН-ДОДАТКИ

Незважаючи на те, що блокчейн є базовим рівнем, для роботи не потрібен протокол Bitcoin. Технології блокчейн можна використовувати в інших сферах і секторах, де відбуваються транзакції, взаємодії та події між учасниками. Це включає як матеріальні, так і нематеріальні активи. Бути в курсі інновацій та розвитку блокчейну – непросте завдання, оскільки цей сектор швидко розвивається у світовому масштабі [10]. Але для цієї роботи важливим є те, як це відбувається в країнах, що розвиваються . З точки зору розвитку, впровадження концепцій суспільних та приватних благ та їх забезпечення державним та приватним секторами є надзвичайно важливимх [1]. У цій статті висвітлено розвиток блокчейну стосовно цих двох типів товарів та послуг. Перш ніж вдаватися до деталей, важливо розрізняти надання послуги та запис і зберігання таких транзакцій у блокчейнах. Технологія розподіленого реєстру не спрямована на надання фактичної послуги. Швидше, вона забезпечує безпечний, приватний, прозорий та незмінний запис транзакцій, що відбуваються під час надання послуг [2] Наприклад, Велика Британія вже використовує блокчейн для здійснення соціальних виплат. Крім того, уряд створив блокчейн як хмарну послугу, доступну лише для державних установ [3]. Останнє можна розглядати як «найкращу практику» для країн, що розвиваються. Щодо документів на право власності на землю, відповідний державний орган все ще повинен видати право власності власнику. Ця видача, а також цифровий відбиток або хеш документа про право власності на землю можуть бути записані в блокчейні, щоб підтвердити право власності та його законність. Таким чином можна вирішити питання запобігання шахрайству або зміни права власності третіми сторонами. У наступних підрозділах досліджується ця еволюція з використанням вищезгаданих категорій приватних та суспільних благ та їх забезпечення приватним та/або державним сектором.

2.1 Суспільні блага

У більшості країн, що розвиваються, та країн, що розвиваються, уряди, в принципі, є основними постачальниками суспільних благ, таких як правосуддя, безпека, охорона здоров'я та освіта, серед іншого [4]. Однак це не означає, що самі уряди надають такі блага. У більшості випадків впровадження передається на аутсорсинг приватним партнерам, як комерційним, так і некомерційним. Це стосується розробки та поточного впровадження блокчейн-технологій у країнах глобального Півдня. Той факт, що місцеве регулювання значно відстає від нових технологій, створив сприятливий ґрунт для цього, як це вже сталося з іншими технологіями.

Державні послуги

В принципі, технології блокчейн можна використовувати для надання державних послуг, що включають загальну обробку та управління публічними документами, які, принаймні в багатьох країнах, що розвиваються, людям важко отримати. У більш загальному плані, блокчейни можна використовувати для підтримки загального забезпечення більшості суспільних благ громадян та зацікавлених сторін, особливо тих, що вимагають особистої взаємодії та потребують індивідуальної ідентифікації.66 Неявний зв'язок між технологією блокчейн та електронним урядуванням 67 справді існує, і зараз його досліджує обрана група блокчейн-стартапів. Procivis 68 , швейцарський стартап, незабаром запустить магазин додатків на основі блокчейну, який надаватиме громадськості вибрані державні послуги. Він також пропонуватиме клієнтам послуги ідентифікації.

Нещодавно Україна підписала угоду з BitFury 70 про підтримку надання державних послуг громадянам, серед інших видів діяльності. [7] Дубай також приєднався до хвилі технології блокчейн і тепер планує стати повноцінним містом блокчейн до 2020 року в рамках своєї поточної ініціативи Smart Dubai. [2] Будучи інформаційно насиченою галуззю, служби охорони здоров'я можуть отримати особливу користь від технологій розподіленого реєстру. Натомість,

сектор освіти не зміг привернути великого інтересу з боку блокчейн-стартапів та консорціумів.74 Більшість наведених нижче прикладів показують, як блокчейн-технології можуть підтримувати широкий спектр розумних урядових програм та ініціатив.

Земельні титули

Реєстрація прав власності на землю була, мабуть, першою сферою, де відбулося планування та потенційне впровадження технології блокчейн у країні, що розвивається. У 2015 році уряд Гондурасу підписав угоду з Factom , американським стартапом , про використання блокчейнів для управління реєстрацією прав власності на землю та допомоги в боротьбі з шахрайством та корупцією. Як це сталося? Спочатку до стартапу звернувся місцевий фонд, що пропагує лібертаріанські цінності, а потім активно будував місток між технологічною компанією та центральним урядом. Згодом було підписано конфіденційну угоду. Однак через кілька місяців проєкт зупинився з причин, які досі незрозумілі.

Минулого року аналогічні ініціативи були також запущені в Грузіїn [7] та Гані [8]. У випадку Грузії, всесвітньо відомий економіст Ернандо де Сото є членом дорадчої ради BitFury, блокчейн-стартапу, який реалізує цю ініціативу [9]. Випадок Гани, мабуть, цікавіший, оскільки місцевий некомерційний стартап BitLand [8] використовує блокчейн Bitcoin для управління правом власності на землю та врегулювання земельних спорів. BitLand тісно співпрацює з місцевими установами, чиїм мандатом є видача свідоцтв про право власності на землю, і які готові спробувати нові технології для вирішення питань , що залишаються невирішеними протягом десятиліть. BenBen81 – ще один стартап у Гані, який працює над тією ж темою . Хоча ініціативи в Гані, здається, зазнали невдачі, Швеція успішно просуває власний проект оформлення прав власності на землю, виходячи таким чином за межі етапу підтвердження концепції [12]. У будь-якому разі, це, здається, свідчить про те, що розгортання блокчейну в країнах , що розвиваються, стикається зі складними викликами.

Послуги ідентифікації

Як згадувалося раніше, Namecoin розробила ключову технологію для потенційного захисту та автентифікації особистості, сприяння свободі слова та запобігання стеженню. Кілька стартапів вже працюють над сервісами ідентифікації на основі блокчейну.83 Наприклад, OneID84 надає, серед іншого , послуги багатофакторної автентифікації та єдиного входу.85 Це видається однією з найперспективніших галузей для успішного застосування технологій блокчейн, що підтверджується зростанням кількості стартапів, що працюють у цій галузі. Ідентифікація на основі технології блокчейн може бути ефективно використана для управління паспортами, свідоцтвами про народження та шлюб, національними та виборчими посвідченнями особи, а також для обробки програм електронного проживання, серед іншого. Однак деякі критики стверджують, що існуючі технології цифрової ідентифікації працюють добре та є набагато масштабованішими, ніж ті, що використовують блокчейн-платформи.86 Обмеження масштабованості технології блокчейн можуть перешкодити масовому впровадженню в країнах з великим населенням , таких як Індія та Китай.

Свобода слова

Такі стартапи , як FlorinCoin88 та Publicism [8,9], по-різному сприяють свободі слова.90 Перша створила розподілений реєстровий додаток (Dapp) під назвою Alexandria , який має на меті бути децентралізованим сховищем знань та інформації, якими безпосередньо керують кінцеві користувачі. Одним із його застосувань є збереження цензурований цифровий контент, який зазвичай швидко зникає з Інтернету. Floricoin покращив блокчейн, запровадивши можливість додавання коментарів до блоків у ланцюжку. Publicism пропонує підтримку журналістам, які стикаються з цензурою в багатьох країнах, дозволяючи журналістам використовувати псевдоніми для захисту своєї особистості. MazaCoin, [9] метою якого є підтримка корінних та індивідуальних громад США, нещодавно почав використовувати свою платформу для захисту свободи слова та зберігання фотографій протестів у блокчейні.

Боротьба з корупцією

Національний демократичний інститут США (NDI) співпрацює з BitFury тим самим стартапом, який займається оформленням прав власності на землю в Джорджії , для просування антикорупційних зусиль за допомогою платформи під назвою Blockchain Trust Accelerator.95 Мета полягає у сприянні розробці блокчейн-додатків, які можуть сприяти відкритому уряду та прозорості. Запущений у червні 2016 року, акселератор поки що не має багато інформації про те, як розвивається.

Виборчі процеси

Різні виборчі процеси також виграли від впровадження та використання технологій блокчейн. Follow My Vote [9] – це стартап, який використовує розподілені реєстри для проведення процесів голосування та запобігання шахрайству та крадіжці особистих даних. Однією з потенційних переваг є те, що виборці, які використовують блокчейн, можуть будь-коли перевірити свій вибір голосування за допомогою своїх закритих ключів. [7] Україна – одна з країн, яка вийшла на цей шлях. Країна використовуватиме E-vox , [8] розподілений реєстр на базі Ethereum, для місцевих виборів. Впровадження вже розпочалося в кількох містах. [9] Однак однією з ключових проблем є доступ до закритих ключів, які хакери можуть отримати різними способами, [10] або виборці можуть запропонувати позичити чи продати свої закриті ключі з метою отримання економічної вигоди. Щойно це стане життєздатним методом, буде цікаво порівняти голосування за допомогою блокчейну з голосуванням через Інтернет, яке вже використовується в Естонії.

Нові форми управління

Деякі блокчейн-платформи прагнуть замінити або принаймні імітувати уряд. Найкращим прикладом є Bitnation [2], яка дозволяє користувачам створювати власні країни без кордонів, що пропонують низку послуг своїм громадянам. Ці країни мають власні конституції, а деякі навіть пропонують базовий дохід своїм громадянам.

Допомога та розвиток

Лондонська компанія Aid:Tech, можливо, є першим стартапом у сфері

блокчейн-технології, який підтримав гуманітарні та розвивальні зусилля на Близькому Сході.104 Компанія пропонує систему ваучерів, яку можна використовувати навіть у найскладніших ситуаціях, і допомагає забезпечити безпечне досягнення фінансових ресурсів кінцевими пунктами призначення. Bitnation тепер також пропонує підтримку біженцям. [5] З боку ООН, ЮНІСЕФ (Дитячий фонд ООН) виділив 100 000 доларів США на підтримку стартапу 9Needs106 і планує зробити те саме для ще п'яти-десяти стартапів [7]. Needs працює над інноваціями у сфері охорони здоров'я та розвитку. ПРООН (Програма розвитку ООН) підтримує грошові перекази та фінансові інструменти в Сербії та Молдові, а також планує незабаром розширити свою діяльність на інші країни [8]. UNWFP (Всесвітня продовольча програма ООН) оголосила про пілотний проект технології блокчейн з використанням Ethereum для надання фінансової підтримки нужденним у Йорданії, спираючись на результати меншої ініціативи в Пакистані. Згідно з одним звітом, сім установ ООН досліджують та/або використовують технології блокчейн для підтримки своїх операцій та програм

Впровадження технології блокчейн у країнах, що розвиваються, поки що не призводить до суттєвих збоїв на тривалій основі. Більшість із них орієнтовані на пропозицію, функціонують як самостійні ініціативи, не пов'язані з поточними програмами, а місцеві установи відіграють лише пасивну роль з незначним рівнем сталого володіння. Місцеві економічні та політичні виклики залишаються серйозними і залишатимуться такими, якщо впровадження технології блокчейн не застосує більш комплексного підходу. У цьому світлі, ініціативи технології блокчейн, задіяні в ширших програмах розумного уряду та сервісах ідентифікації, ймовірно, мають найкращі шанси на успіх у середньостроковій перспективі.

2.2 Приватні товари

Надання приватних товарів в екосистемі блокчейну має внутрішній

компонент фінансової стійкості, який працює як магніт для залучення постачальників – за умови конкурентоспроможності цін. Незважаючи на це, мільярди людей у всьому світі не мають доступу до таких товарів, особливо у випадку банківських послуг. Коли ж вони мають мінімальний доступ, бідні люди повинні платити надзвичайно високі збори за користування приватними послугами, як ми бачимо на прикладі грошових переказів. [11] Сільське господарство – це ще один сектор, де поширені приватні товари, і сектор, який забезпечує засоби до існування більшості бідного населення світу. [12] Права інтелектуальної власності також є сферою, де технології блокчейну можуть бути ефективними для захисту цифрових і нецифрових активів і забезпечення потоку роялті творцям та новаторам.

Банківські обслуговування для небанківських

M-Pesa, продукт мобільних інновацій у Кенії, був першою успішною спробою надати базові банківські послуги тим, хто знаходиться внизу піраміди. Сьогодні понад 90 країн використовують подібні схеми, обслуговуючи майже півмільярда людей. Однак майже два мільярди людей досі не мають доступу до базових банківських послуг. [13] що блокчейн допоможе завдяки BitPesa. [14] BitPesa, кенійський стартап, керований експатами, підтримує транзакції та платежі між африканськими підприємствами та рештою світу за допомогою блокчейну Bitcoin. В принципі, платформа відкрита для всіх, включаючи малі та мікропідприємства, які можуть використовувати ці послуги для розширення свого бізнесу. Таким чином, BitPesa помітно відрізняється від M-Pesa, але навіть попри це, юридичний спір між ними триває вже кілька місяців [15]. BitPesa активно працює в Демократичній Республіці Конго, Кенії, Нігерії, Танзанії та Уганді, а також має партнерів у США та Китаї. Окрім платежів, BitPesa також обмінює біткойни на місцеві валюти, а також долари США та інші валюти.

BitSoko 116 – ще один кенійський стартап, який пропонує біткоїн-гаманець на базі Android, щоб зменшити відносно високі транзакційні витрати інших платформ мобільних грошей, таких як M-Pesa. Такі витрати коливаються від чотирьох до десяти відсотків, і BitSoko прагне знизити ці комісії до менш ніж

піввідсотка. Він також пропонує більш безпечну та прозору платформу, використовуючи переваги блокчейну Bitcoin. У 2015 році BitSoko отримав підтримку від Фонду Гейтса, щоб по суті створити портфель послуг, які стартап пропонує сьогодні [17]. Хоча вони планують підтримувати звичайні телефони найближчим часом, платформа додатків доступна лише для смартфонів, що обмежує її охоплення та зручність використання тими, хто може дозволити собі дорожчий смартфон. У цьому контексті вона все ще значно відстає від M-Pesa та інших платформ мобільних грошей. Зауважте, що як BitPesa, так і BitSoko також підтримують грошові перекази.

У квітні 2017 року Фонд Гейтса запустив власну ініціативу, спрямовану на підтримку надання фінансових послуг бідним. Ініціатива забезпечить уряду рамки для використання технології блокчейн, а також продемонструє її обмеження з точки зору масштабу та управління.

Грошові перекази (також відомі також ребітанції

Грошові перекази, ймовірно, є однією з найбільш конкурентних сфер в екосистемі блокчейну, безсумнівно, завдяки величезному розміру ринку та прибутковості. Тільки у 2015 році грошові перекази склали понад 500 мільярдів доларів США, причому 25 відсотків надійшло лише зі США [19]. Цього року середня світова вартість грошових переказів становила майже сім з половиною відсотків, причому в Африці середні витрати вищі. Використання традиційних банків тягне за собою набагато вищі витрати, до 11 відсотків, тоді як передплачені картки залишаються найдоступнішими, в середньому на рівні 1,75 відсотка [12] в галузі технології блокчейн вже є жорсткою. Дійсно, близько 30 стартапів та компаній вже пропонують послуги з рефінансування в багатьох країнах [11]. Гарним прикладом тут є Abra, [2] стартап з Філіппін, який нещодавно отримав фінансову підтримку від міжнародного венчурного капіталу. Використовуючи блокчейн Bitcoin, стартап тепер планує розширитися на інші країни. Зауважте, що поточний додаток доступний лише для смартфонів, тому користувачі, які не мають доступу до таких пристроїв, повинні використовувати комп'ютер або подібний пристрій для доступу до його послуг.

Іншим прикладом є Rebit, [23] також розташована на Філіппінах, яку підтримує більша компанія, метою якої є просування біткойна в країні [24], і яку можна використовувати для надсилання грошей на Філіппіни з будь-якої точки світу. Компанія стверджує, що не стягує плату за користування послугою, але вимагає від користувачів купувати біткойни для використання сервісу. Одержувачі отримують місцеву валюту, оскільки Rebit виконує конвертацію (таким чином зберігаючи біткойни), і отримують сповіщення електронною поштою та SMS. Щодо розвитку, ПРООН нещодавно оголосила про запуск пілотного проекту з використанням блокчейну для грошових переказів у Сербії, [25] тоді як ЮНІСЕФ досліджує технології блокчейн для грошових переказів.126 Через відносно велику частку ринку, яку займає цей сектор, грошові перекази здаються одним із найпривабливіших і, отже, конкурентоспроможних секторів, коли йдеться про впровадження технології блокчейн. Abra та BitPesa [27] є двома з шести провідних компаній з грошових переказів, що використовують технологію блокчейн, але їх легко можна витіснити, оскільки інші компанії почнуть зростати та завойовувати частку ринку.

Сільське господарство

Хоча сільськогосподарський сектор у промислово розвинених країнах значною мірою залежить від використання різних технологій, це, безумовно, не стосується більшості країн, що розвиваються. Фактично, цей сектор має один із найнижчих рівнів інвестицій у технології, особливо серед дрібних фермерів. Мобільні технології дещо змінили це, надаючи виробникам інформацію та послуги, включаючи ціноутворення. Тому не бракує блокчейн-стартапів, що з'являються для підтримки цього сектору. Загальні застосування включають: відстеження продуктів та ланцюгів поставок; сприяння платежам виробникам; стеження за цінами для забезпечення справедливої оплати за продукцію; та покращення сільського господарства, що підтримується громадами. [28] Наприклад, Skuchain [29] використовує смарт-контракти для відстеження ланцюгів поставок сільськогосподарської продукції (а також використовується в багатьох інших секторах). [13] Однак, здається, що він також вимагає рівня

складності, який може бути вищим за середньостатистичного бідного дрібного фермера у більшій частині країн глобального Півдня. Farmshare [21] підтримує сільське господарство на основі громад, яке сприяє розвитку комунальних форм власності та спільних трудових процесів для розвитку місцевої економіки. Farmshare також використовує смарт-контракти та децентралізовані додатки (Dapps) для просування місцевих продуктів та забезпечення розподілу платежів між громадами-учасниками.

Bitmari , ще один африканський сервіс біткоїн-гаманців для надсилання грошей, підтримує акселератор та траст для жінок-фермерів у Зімбабве. [13] Проєкт використовує краудфандинг для збору біткоїнів, а потім надає фінансування жінкам-фермерам, які, як очікується, отримають технічну допомогу від експертів.

Продовольча безпека

Коли йдеться про продовольчу безпеку та підтримку малих фермерів і кооперативів, AgriLedger [15] здається беззаперечним лідером. Використовуючи блокчейн та мобільний додаток, що працює на смартфонах, AgriLedger дозволяє фермерам відстежувати всі транзакції, надаючи унікальні ідентифікатори кожному кінцевому користувачеві. Зрозуміло, що додаток вимагає доступу до мобільних мереж із доступом до даних. Незрозуміло, чи має стартап якісь плани пропонувати офлайн-доступ.

Права інтелектуальної власності

Як незмінна, розподілена та прозора платформа з вбудованими фінансовими токенами, технологія блокчейн видається ідеально підготовленою для підтримки захисту прав інтелектуальної власності. Одним із яскравих прикладів є створення реєстрів інтелектуальної власності (ІВ) на основі технології блокчейн, де власники ІВ можуть зберігати хешовані цифрові сертифікати своєї ІВ і навіть використовувати платформу для отримання роялті від тих, хто використовує їхні винаходи за допомогою смарт-контрактів [3]. Цікаво , що ця галузь досі отримала відносно мало уваги з боку екосистеми технології блокчейн. Ascribe [3] – один із стартапів, що працює в цій галузі та

зосереджується на захисті інтелектуальної власності митців. Компанія використовує блокчейн Bitcoin, але розробила протокол з відкритим кодом, який взаємодіє з першим і дозволяє користувачам реєструвати інтелектуальну власність. Митці можуть отримувати сертифікати атрибуції, сертифікати власності та керувати ліцензуванням своїх робіт третім сторонам.

Проблеми піратства можна було б ефективно вирішити таким чином, але захист інтелектуальної власності на основі технології блокчейн повинен працювати синхронно з урядами та законодавцями, щоб зробити його юридично застосовним, – і саме це може стримувати розробку та впровадження блокчейнів у цій галузі. З іншого боку, питання, пов’язані з добросовісним використанням інтелектуальної власності, можуть зазнати негативного впливу режиму інтелектуальної власності на основі технології блокчейн.

Більшість ініціатив у сфері технології блокчейн, спрямованих на цю вибрану групу приватних благ, мають великий потенціал, але ще не розпочали свою діяльність. [14] Деякі з них вже припинили або взагалі призупинили свою діяльність, тоді як інші намагаються генерувати стабільні доходи. Це може бути симптомом жорсткої конкуренції серед стартапів на ринку, який все ще перебуває на зародковому рівні та де вкрай необхідний венчурний капітал є дефіцитним. Прогрес, зумовлений технологією блокчейн, у таких сферах, як банківська справа для бідних та сільське господарство, є незначним і затьмарений іншими технологіями, такими як мобільні телефони. У цьому світлі грошові перекази та цифрові гроші на даний момент здаються найбільш перспективними сферами.

Огляд застосувань технології блокчейн показує, що бар'єри для входу залишаються високими порівняно з іншими технологіями, такими як мобільні додатки. Мобільні інновації швидко поширилися в країни, що розвиваються, незважаючи на нижчий рівень технологічних навичок та обмежений доступ до Інтернету, і поява понад 100 технологічних центрів на африканському континенті є переконливим доказом цього. Інновації в технології блокчейн, схоже, вимагають вищого рівня знань та можливостей. Хоча технологічні центри

та технопідприємці активно працюють у країнах, що розвиваються, протягом багатьох років, впровадження блокчейну на місцевому рівні було відносно повільним – і, звичайно, не таким вражаючим, як у випадку мобільних технологій. Але це не означає, що ініціативи щодо блокчейну приречені на провал у країнах глобального Півдня. Навпаки, у більшості випадків технологія тестується в кількох секторах, і вперше. Деякі стартапи в країнах глобального Півдня справді використовують технології блокчейн, але розгортають прості платформи, розроблені на Півночі; і хоча сучасні тенденції свідчать про те, що інновації в галузі блокчейну здебільшого відбуваються на Півночі, впровадження відбувається в усьому світі, що швидко вплине на інноваційні екосистеми також у країнах глобального Півдня.

2.3 Висновки по розділу

У країнах, що розвиваються, блокчейн дедалі частіше використовується для покращення надання громадських благ — від реєстрації земельних прав та цифрової ідентифікації до боротьби з корупцією та забезпечення прозорості виборів. Хоча більшість ініціатив поки що мають експериментальний характер, вони демонструють значний потенціал для підвищення ефективності державних

РОЗДІЛ 3. БЛОКЧЕЙНИ ТА РОЗВИТОК ЛЮДИНИ

У попередньому розділі було розглянуто широкий спектр застосувань технології блокчейн, які можуть мати значення для розвитку. Хоча можна зробити висновок, що спектр застосувань широкий, загальна глибина все ще невелика. Багато з описаних вище ініціатив все ще знаходяться на папері або ось-ось розпочнуться, тоді як інші повністю функціонують, але обслуговують лише дуже мало клієнтів та зацікавлених сторін, а багато з них також зазнали невдачі. Можливо, це результат того, що технологія все ще перебуває на початковій стадії розвитку та тільки вступає на стадію зростання. Незважаючи на це, фахівці з розвитку, які шукають інноваційні рішення для подолання традиційних прогалин у розвитку, повинні мати достатнє нетехнічне розуміння потенціалу, який технології блокчейн можуть мати для підтримки та вдосконалення програм розвитку. У цьому розділі це досліджується за допомогою аналітичної основи, з додатковою перспективою «управління» для подальшого пояснення потенціалу блокчейну для покращення демократичного управління.

3.1 Інфраструктура та інфоструктура

Мільярди людей не мають доступу до Інтернету, і більшість із них проживає в країнах, що розвиваються [14]. Крім того, хоча міські центри країн глобального Півдня мають доступ до найновіших технологій та широкосмугового зв'язку, ті, хто живе в сільській місцевості та маргіналізованих громадах, а також ті, хто занадто бідний, щоб купити доступ або технологічні інструменти, не мають такого доступу. Таким чином, малоймовірно, що люди, які живуть у таких умовах, зможуть стати вузлами мережі технології блокчейн або зможуть ефективно запускати програмне забезпечення для гаманців, щоб хоча б отримати вигоду від цієї технології як кінцеві користувачі [1]. Звичайно, це не є унікальним для блокчейну, але це впливає на те, як ця технологія повинна бути розгорнута та використана, якщо кінцевою метою втручань є сприяння

розвитку людського потенціалу серед тих, хто соціально виключений. Унікальністю блокчейнів є необхідне та широке використання криптографічних інструментів, що вимагає розробки іншого типу інфраструктури або інфоструктури: інфраструктури відкритих ключів [14]. Інфраструктура відкритих ключів, яка охоплює ролі, політики та процедури, необхідні для забезпечення електронної передачі інформації, ще не існує в багатьох країнах, що розвиваються. Це створює серйозні перешкоди для систематичного використання технології блокчейн і особливо актуально для ефективного та прозорого надання суспільних благ розподіленим способом. Не дивно, що прихильники вже запропонували розгортання децентралізованої інфраструктури відкритих ключів з використанням технології блокчейн, таким чином обходячи традиційну централізовану модель.

З точки зору кінцевого користувача, регулярне використання криптографічних інструментів може бути серйозним викликом. Нещодавнє дослідження студентів американських коледжів, багато з яких є «цифровими аборигенами», показує, що навіть серед цієї групи населення необхідно подолати величезні перешкоди, перш ніж криптографічні інструменти стануть мейнстрімом [16]. Так само інформатору Еду Сноудену було важко спілкуватися з журналістами, оскільки більшість не могли користуватися такими інструментами, не кажучи вже про встановлення відповідного програмного забезпечення на свої ноутбуки. Тут виникають два окремих питання. Одне — це використання таких інструментів. Друге стосується управління закритими та відкритими ключами кінцевих користувачів. Як згадувалося раніше, блокчейн-гаманці можуть забезпечувати і, безумовно, забезпечували зручні інтерфейси, що сприяють створенню та використанню криптографії з відкритим ключем, навіть якщо Кінцевий користувач може не до кінця розуміти, як це працює [17]. Але користувачі повинні мати можливість керувати своїми закритими ключами та безпечно зберігати їх десь, якимось чином. Ці дві проблеми разом можуть виявитися занадто складними для населення з відносно низьким рівнем освіти та грамотності, яке стикається із соціальною ізоляцією.

Як обговорювалося в розділі 3 вище, кілька стартапів з країн, що розвиваються, досягли відносного успіху у використанні блокчейнів, незважаючи на обмежене використання з боку клієнтів. Більшість із них використовують блокчейн біткойна. Однак жоден із цих стартапів не впроваджує інновації для адаптації коду до місцевих умов або розробки нових функцій, і, на відміну від мобільних додатків, децентралізовані додатки (Dapps) також не розробляються. Це переконливо свідчить про те, що для реалізації цього на місцевому рівні потрібні технічні навички вищого рівня. Такі країни, як Гана та Кенія, отримали вигоду від існуючих технологічних центрів та мереж для використання блокчейнів і таким чином створили інноваційну екосистему, яка могла б підтримувати їхній місцевий розвиток. Це могло б стати стартовим майданчиком для інновацій блокчейну в країнах глобального Півдня в середньостроковій перспективі, особливо якщо стануть доступними венчурний капітал або інші зовнішні фінансові механізми, включаючи допомогу в розвитку.

3.2 Політика та регулювання

Як і у випадку з багатьма іншими технологіями, що сприяють так званій економіці спільного використання, [8] технологія блокчейн, очолювана зростанням популярності біткойна, випереджає місцеву політику та регулювання. Хоча промислово розвинені країни вже почали наздоганяти, це, безумовно, не стосується більшості країн, що розвиваються, де політичний та регуляторний потенціал все ще перебуває на початковому етапі. Цей розрив сприяє використанню технологій розподіленого реєстру на глобальному Півдні не лише для місцевих стартапів, а й для тих, що базуються на Півночі. Що стосується останнього, то ця група країн може стати місцями, де будуть розгортатися пілотні проекти та прототипи для перевірки концепції, а також підвищити експертизу стартапів та конкурентну перевагу в глобальному масштабі. Власне, це вже відбувається в кількох країнах, що розвиваються.

Відсутність національної політики щодо інфраструктури відкритих

ключів у цих країнах також спочатку може розглядатися як подальший стимул для розвитку блокчейнів, хоча, з іншого боку, це також може стати проблемою, якщо виникнуть проблеми безпеки, пов'язані з управлінням відкритими ключами, такі як крадіжка ключів або незаконне використання ключів [9]. Якщо це так У такому разі, політики інфраструктури відкритих ключів справді необхідні, навіть якщо фактична реалізація здійснюється за допомогою децентралізованих моделей з використанням технологій блокчейн. Оскільки більшість стартапів, що використовують блокчейн, дотримуються біткойна, політика та регулювання криптовалют також є важливими. Це включає послуги, що пропонують конвертацію біткойнів або альткоїнів у місцеву валюту, а також використання криптовалют як законного платіжного засобу. Крім того, місцева політика та правила також важливі з міркувань безпеки в країнах, де процвітають конфлікти та насильницький екстремізм, а фінансування такої діяльності слід ретельно контролювати, щоб запобігти її глобальному поширенню.

Як і у випадку з деякими попередніми інтернет-технологіями, блокчейни також можуть сприяти подальшому зменшенню деяких, якщо не всіх, форм центрального уряду. Дійсно, однією з мотивацій, що спонукали Накамото до розробки біткойна, була реакція урядів на світову економічну кризу 2007/2008 років [15]. Багато ранніх прихильників блокчейну біткойна були лібертаріанцями, які розглядали нову технологію як найефективніший інструмент для остаточного усунення державного втручання [1]. Розподілений характер технології в поєднанні з новою формою децентралізованої довіри та розподіленого консенсусу забезпечує основу для таких поглядів. Однак це не обов'язково означає, що блокчейн нерозривно пов'язаний з такими поглядами, і ніхто серйозно не очікує, що держава зникне найближчим часом. Фактично, і як описано в попередньому розділі, багато блокчейн-стартапів безпосередньо співпрацюють з урядом для впровадження технології на рівні штатів. Зовсім недавно творець Ethereum змінив своє сприйняття актуальності лібертаріанської філософії на поточному політичному етапі.

Питання, яке досі значною мірою ігнорували, – це потенціал блокчейну

для підтримки та посилення децентралізації управління в межах певної національної держави. Децентралізація штатів, яку також називають місцевим управлінням, була ключовим питанням розвитку, і багато країн, що розвиваються, вже мають загальну політику децентралізації. Однак місцеві органи влади стикаються зі серйозними фінансовими проблемами та проблемами з потенціалом і не здатні надавати суспільні блага. Блокчейн Таким чином, технологія може принести реальні переваги місцевим органам влади. Аргумент на користь децентралізованих або розподілених державних послуг, який просувають експерти з блокчейну, може стати чудовою взаємовигідною можливістю.

Інституційний потенціал

Використання нових технологій країнами, що розвиваються, вимагає, окрім фіскальних ресурсів, інституційного потенціалу, який сприятиме їхньому впровадженню на сталій основі. Такий потенціал не обмежується знаннями технологій, а також включає адміністративний та управлінський потенціал, а також чіткі правила гри, встановлені законодавством та застосовні в усьому світі. Багато країн, що розвиваються, все ще створюють та розвивають такий потенціал, що серйозно обмежує їхню здатність долучатися до процесу, коли з'являються технологічні інновації, такі як блокчейн та інші. Навпаки, установи країн, що розвиваються, можуть використовувати блокчейн, імпортуючи ноу-хау та досвід та/або використовуючи місцевий досвід, якщо він є, поза урядом. Справжня проблема полягає в тому, що такі ініціативи можуть бути нестійкими в середньостроковій перспективі. Зазвичай вони здійснюються ізольовано, відокремлені від інших державних установ та діють поза політичними процесами, які розподіляють фіскальні ресурси державним установам.

З інституційної точки зору, також важливо врахувати, як блокчейни слід використовувати в державному секторі. Хоча поточна точка зору передбачає, що технології блокчейн повинні повністю замінити існуючі процеси, також можна розглядати цю технологію як доповнюючу та підкріплюючу процеси, [3] окрім впровадження інновацій у державному секторі. Зрештою, важливо розрізняти

розробку та впровадження блокчейн-ініціатив. Хоча державні установи повинні бути залучені до першої, остання може здійснюватися приватними партнерами (комерційними та некомерційними). прибуток), які мають кращу кваліфікацію для цього. Саме це й сталося з розробкою мобільних додатків у країнах, що розвиваються. Однак, схоже, це не стосується поточних пілотних проектів технології блокчейн, і це може мати негативні наслідки для масштабування таких пілотних проектів та забезпечення їхньої довгострокової - стійкості.

3.3 Управління блокчейнами

Заклики до нового суспільного договору порушують ключові питання щодо блокчейну: хто керує, хто розроблятиме такий договір і як можна врахувати всі думки? [4] Швидка відповідь від табору блокчейну є прямою: Ніхто не відповідає, оскільки за замовчуванням у цьому немає потреби [5] Фактично, всі відповідають, оскільки управління здійснюється лише на основі консенсусу. Такий консенсус, у свою чергу, базується на алгоритмах, [15] які дозволяють користувачам і вузлам майже автоматично узгоджувати результати процесу. Однією з основних ідей цього управління на основі алгоритмічного консенсусу є децентралізована автономна організація (DAO). Групи людей, які прагнуть досягти спільного результату, бізнес-цілі або політичного втручання, збираються разом і домовляються про низку принципів, які закодовані в програмному забезпеченні. Потім програмне забезпечення бере під контроль загальну операцію та відводить на задній план людей, яким більше не потрібно взаємодіяти між собою. Тут виникає кілька проблем, які можна виділити наступним чином:

Кодування: Хто фактично займається кодуванням? Як їх відбирали? Кодування передбачає переклад угод між членами DAO на певну мову програмування, включаючи машинне навчання, яка запускає смарт-контракт і автоматично запускає певні події за виконання певних умов.

Розуміння коду: Хто насправді може читати та перевіряти код? Більшість

блокчейнів використовують програмне забезпечення з відкритим вихідним кодом, що означає, що кожен має доступ до коду. Але користувачі повинні мати змогу читати та розуміти сам код. За аналогією, читання безкоштовної книги, скажімо, китайською мовою, вимагає, щоб читач знав цю мову. В іншому випадку безкоштовна книга не матиме цінності для потенційного читача, незалежно від вартості. Тим, хто не може читати код, доведеться шукати довірених третіх сторін, які можуть гарантувати, що код відображає те, що було узгоджено.

Масштабованість: блокчейни мають добре відомі обмеження щодо масштабованості. Хоча майбутні інновації в цьому секторі можуть допомогти вирішити цю проблему, прагнення обмежити кількість блокчейнів до певного рівня. Мінімум може бути контрпродуктивним. Якщо ж ця кількість натомість зросте, то сумісність між блокчейнами стане більшою проблемою. Крім того , як зростання технології блокчейн до мільярдів користувачів і вузлів вплине на досягнення децентралізованого консенсусу? Питання демократичного представництва в мережі можуть виникнути найближчим часом.

Довіра проти управління: Той факт, що довіра децентралізована та знеособлена і натомість розміщена в розподіленій мережі, не означає автоматично посиленого управління [9]. Наприклад , вузли та користувачі, які не були частиною початкового дизайну блокчейну, не брали участі в процесі та не брали участі в рішеннях щодо управління, прийнятих тими, хто був. Користувачі або приєднуються за певних умов, але також можуть вільно перейти кудись ще, якщо їм це не подобається.

Ці проблеми вказують на той факт, що блокчейни, навіть будучи децентралізованими та розподіленими, не можуть гарантувати відсутність ієрархій та нерівності між вузлами. Фактично, саме це зараз і відбувається, коли йдеться про майнінг блокчейну [16]. Те саме можна сказати про блокчейн-кодерів, розробників та технопідприємців, які займаються розробкою блокчейну, всі з яких , здається, мають привілейоване становище в мережі та можуть мати значну владу над усіма іншими вузлами. Таким чином, нерівність у

децентралізованій мережі є можливою.

Зрештою, деякі ентузіасти блокчейну, здається, підтримують точку зору, що алгоритми, запрограмовані обраними кількома особами, можуть або повинні керувати суспільством і, можливо, навіть замінити індивідуальні взаємодії. [16] Однак алгоритми не є нейтральними і не є одразу прозорими для більшості [2] Можливо, потрібна децентралізована мережа, яка забезпечує прозорість і демократичне управління алгоритмами. З точки зору управління та розвитку, більшість із вищезазначеного передбачає значний рівень розвитку демократичних інститутів та демократичних цінностей. Фактичну актуальність для конкретної країни, що розвивається, слід оцінювати в кожному окремому випадку. Але в принципі, чим нижчий рівень розвитку людського потенціалу, тим складніше буде систематично впроваджувати технологію блокчейн.

У рамках виконання роботи було поставлено завдання розробити смарт-контракт для управління користувачами та їхніми транзакціями в мережі Ethereum. У роботі передбачалося створення програмного забезпечення, яке б забезпечувало функціонал реєстрації та видалення користувачів, виконання транзакцій між ними, а також збереження й перегляд історії операцій. Контракт мав бути безпечним, сумісним із Ethereum Virtual Machine (EVM) і придатним для використання в децентралізованих системах. У цьому розділі роботи описано процес розробки смарт-контракту, починаючи від аналізу вимог і закінчуючи його тестуванням та розгортанням, із детальним висвітленням технічних рішень, що приймалися в процесі. На початковому етапі роботи було проведено аналіз вимог до системи. У роботі передбачалося, що смарт-контракт повинен надавати адміністраторам повний контроль над управлінням користувачами, включаючи можливість їх додавання та видалення. Користувачі, зі свого боку, мали отримувати право виконувати транзакції лише після реєстрації, а також мати доступ до історії своїх операцій. Важливим аспектом, який враховувався в роботі, була безпека: контракт мав бути захищеним від несанкціонованого доступу та потенційних атак, таких як повторний вхід. Крім того, у роботі ставилася мета забезпечити ефективне використання ресурсів блокчейну, щоб

мінімізувати витрати газу під час виконання операцій. Для реалізації смарт-контракту в роботі було обрано мову програмування Solidity версії ^0.8.0, яка забезпечує сучасні засоби безпеки, зокрема захист від арифметичних помилок. Як середовище розробки використовувався Remix IDE, що дозволяє зручно компілювати, тестувати та розгортати контракти через веб-інтерфейс. У роботі також було вирішено використовувати тестову мережу Ropsten для перевірки функціональності контракту, оскільки вона імітує реальну мережу Ethereum без необхідності витрачати реальні кошти. Для взаємодії з блокчейном застосовувався гаманець MetaMask, який інтегрується з Remix і забезпечує безпечне підключення до мережі.

У процесі роботи було розроблено структуру смарт-контракту, який отримав назву BlockchainManager. У роботі передбачалося, що контракт базуватиметься на двох основних структурах даних. Перша структура, названа User, містила інформацію про користувача: його адресу в мережі Ethereum, роль (адміністратор, користувач або відсутність ролі) та статус реєстрації. Друга структура, Transaction, зберігала дані про транзакції, включаючи адреси відправника та отримувача, суму й час виконання. Для організації даних у роботі використовувалися відображення (mapping): одне для зберігання інформації про користувачів, інше - для історії транзакцій. Додатково було введено змінну userCount, яка відстежувала кількість зареєстрованих користувачів і полегшувала аналіз масштабів системи. Писання коду контракту розпочалося з реалізації конструктора, який автоматично призначав роль адміністратора особі, що розгортає контракт. У роботі це рішення обґрунтовувалося необхідністю забезпечити наявність хоча б одного користувача з повними правами одразу після розгортання. Для фіксації ключових дій у роботі було додано події (events): UserRegistered для логування реєстрації, TransactionExecuted для транзакцій і UserRemoved для видалення користувачів. Ці події забезпечували прозорість і дозволяли зовнішнім системам відстежувати зміни в контракті. Основні функції контракту розроблялися з урахуванням вимог безпеки та функціональності. У роботі було реалізовано функцію registerUser, яка дозволяла адміністратору

додавати нових користувачів, перевіряючи, чи не була адреса вже зареєстрована. Для обмеження доступу до цієї функції в роботі було створено модифікатор onlyAdmin, який перевіряв роль викликача. Функція removeUser забезпечувала видалення користувачів, але з умовою, що адміністратор не може видалити іншого адміністратора, щоб уникнути втрати контролю над системою. Функція executeTransaction відповідала за виконання транзакцій між зареєстрованими користувачами, записуючи дані в історію обох сторін. Для перегляду історії в роботі було реалізовано функцію getTransactionHistory, яка повертала масив транзакцій для вказаної адреси. Модифікатор onlyRegistered гарантував, що транзакції можуть виконувати лише зареєстровані користувачі. Безпека контракту була ключовим аспектом, який розглядався в роботі. Для захисту від несанкціонованого доступу використовувалися модифікатори та перевірки умов через оператор require. Наприклад, у функції executeTransaction перевірялося, чи зареєстрований отримувач і чи є сума транзакції ненульовою. У роботі також було враховано захист від атак повторного входу шляхом уникнення зовнішніх викликів у критичних функціях. Код оптимізувався для зменшення витрат газу, зокрема через використання оператора delete для очищення даних під час видалення користувачів.

Нижче наведено повний код смарт-контракту, який було розроблено в роботі:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract BlockchainManager {
    enum Role { None, User, Admin }
    struct User {
        address userAddress;
        Role role;
        bool isRegistered;
    }
    struct Transaction {
        address from;
        address to;
        uint256 amount;
```

```
        uint256 timestamp;
    }

    mapping(address => User) public users;
    mapping(address => Transaction[]) public transactionHistory;
    uint256 public userCount;

    event UserRegistered(address indexed user, Role role);
    event TransactionExecuted(address indexed from, address indexed to, uint256
amount);
    event UserRemoved(address indexed user);

    modifier onlyAdmin() {
        require(users[msg.sender].role == Role.Admin, "Only admin");
        _;
    }
    modifier onlyRegistered() {
        require(users[msg.sender].isRegistered, "User not registered");
        _;
    }

    constructor() {
        users[msg.sender] = User(msg.sender, Role.Admin, true);
        userCount = 1;
        emit UserRegistered(msg.sender, Role.Admin);
    }

    function registerUser(address _userAddress) public onlyAdmin {
        require(!users[_userAddress].isRegistered, "User already registered");
        users[_userAddress] = User(_userAddress, Role.User, true);
        userCount++;
        emit UserRegistered(_userAddress, Role.User);
    }

    function removeUser(address _userAddress) public onlyAdmin {
        require(users[_userAddress].isRegistered, "User not registered");
        require(users[_userAddress].role != Role.Admin, "Cannot remove admin");
        delete users[_userAddress];
        userCount--;
        emit UserRemoved(_userAddress);
    }
```

```
        function executeTransaction(address _to, uint256 _amount) public
onlyRegistered {
            require(users[_to].isRegistered, "Recipient not registered");
            require(_amount > 0, "Amount must be positive");
            Transaction memory newTransaction = Transaction(msg.sender, _to, _amount,
block.timestamp);
            transactionHistory[msg.sender].push(newTransaction);
            transactionHistory[_to].push(newTransaction);
            emit TransactionExecuted(msg.sender, _to, _amount);
        }

        function getTransactionHistory(address _user) public view returns
(Transaction[] memory) {
            return transactionHistory[_user];
        }
    }
```

Лістинг 3.1 - Код смарт-контракту

Тестування контракту проводилося в роботі за допомогою Remix IDE та тестової мережі Ropsten. У процесі тестування було перевірено всі основні функції: реєстрація користувачів, виконання транзакцій, видалення користувачів і перегляд історії. Наприклад, було створено кілька тестових адрес, які реєструвалися через registerUser, після чого виконувалися транзакції між ними за допомогою executeTransaction. Результати записувалися в історію, яка успішно відображалася через getTransactionHistory. У роботі також було протестовано сценарії помилок, такі як спроба виконання транзакції незареєстрованим користувачем або видалення адміністратора, що підтвердило коректність роботи перевірок безпеки. Розгортання контракту в роботі здійснювалося через Remix IDE. Після компіляції коду з використанням компілятора Solidity ^0.8.0 контракт розгортався в мережі Ropsten за допомогою MetaMask. У роботі було збережено адресу контракту для подальшої взаємодії.

Користувачі могли викликати функції через інтерфейс Remix або підключити контракт до зовнішнього додатку через бібліотеку Web3.js. Наприклад, для реєстрації користувача викликалася функція registerUser(0x123...), а для виконання транзакції - executeTransaction(0x456...,

100). У результаті роботи було створено функціональний смарт-контракт, який відповідає поставленим вимогам. Реалізована система забезпечує управління користувачами та транзакціями, гарантує безпеку та прозорість операцій. У роботі було досягнуто мети створення надійного інструменту для адміністрування блокчейну, який може бути використаний як основа для подальших розробок, наприклад, додавання підтримки токенів або розширених ролей.

Продовжуючи розробку смарт-контракту BlockchainManager, було вирішено розширити його функціональність і поглибити аналіз технічних аспектів. Писався новий код для реалізації функції, яка дозволяла б адміністраторам тимчасово блокувати можливість користувачів виконувати транзакції, що могло бути корисним для управління ризиками або в разі підозрілої активності. Крім того, розроблявся детальний аналіз безпеки для захисту від специфічних атак, таких як front-running і gas griefing. Також створювався простий фронтенд-додаток для взаємодії з контрактом, а витрати газу аналізувалися для забезпечення економічності. Нова функція, названа restrictUserTransactions, була додана до контракту.

Вона дозволяла адміністраторам встановлювати або знімати обмеження на виконання транзакцій для конкретного користувача. Для цього в структуру User було додано поле isRestricted, яке вказувало, чи заблоковано транзакції користувача. Функція перевіряла, чи є користувач зареєстрованим, і змінювала статус обмеження, викликаючи нову подію UserRestrictionUpdated. У функції executeTransaction було додано перевірку, щоб заблоковані користувачі не могли відправляти транзакції. Це рішення розроблялося з урахуванням гнучкості: адміністратор міг швидко реагувати на небажану поведінку, не видаляючи користувача повністю.

Ось оновлений код контракту з новою функцією:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract BlockchainManager {
    enum Role { None, User, Admin }
```

```
    struct User {
        address userAddress;
        Role role;
        bool isRegistered;
        bool isRestricted;
    }
    struct Transaction {
        address from;
        address to;
        uint256 amount;
        uint256 timestamp;
    }

    mapping(address => User) public users;
    mapping(address => Transaction[]) public transactionHistory;
    uint256 public userCount;

    event UserRegistered(address indexed user, Role role);
    event TransactionExecuted(address indexed from, address indexed to, uint256
amount);
    event UserRemoved(address indexed user);
    event UserRestrictionUpdated(address indexed user, bool isRestricted);

    modifier onlyAdmin() {
        require(users[msg.sender].role == Role.Admin, "Only admin");
        _;
    }
    modifier onlyRegistered() {
        require(users[msg.sender].isRegistered, "User not registered");
        require(!users[msg.sender].isRestricted, "User is restricted");
        _;
    }

    constructor() {
        users[msg.sender] = User(msg.sender, Role.Admin, true, false);
        userCount = 1;
        emit UserRegistered(msg.sender, Role.Admin);
    }

    function registerUser(address _userAddress) public onlyAdmin {
        require(!users[_userAddress].isRegistered, "User already registered");
        users[_userAddress] = User(_userAddress, Role.User, true, false);
```

```
            userCount++;
            emit UserRegistered(_userAddress, Role.User);
        }

        function removeUser(address _userAddress) public onlyAdmin {
            require(users[_userAddress].isRegistered, "User not registered");
            require(users[_userAddress].role != Role.Admin, "Cannot remove admin");
            delete users[_userAddress];
            userCount--;
            emit UserRemoved(_userAddress);
        }

        function restrictUserTransactions(address _userAddress, bool _restrict) public
onlyAdmin {
            require(users[_userAddress].isRegistered, "User not registered");
            require(users[_userAddress].role != Role.Admin, "Cannot restrict admin");
            users[_userAddress].isRestricted = _restrict;
            emit UserRestrictionUpdated(_userAddress, _restrict);
        }

        function executeTransaction(address _to, uint256 _amount) public
onlyRegistered {
            require(users[_to].isRegistered, "Recipient not registered");
            require(!users[_to].isRestricted, "Recipient is restricted");
            require(_amount > 0, "Amount must be positive");
            Transaction memory newTransaction = Transaction(msg.sender, _to, _amount,
block.timestamp);
            transactionHistory[msg.sender].push(newTransaction);
            transactionHistory[_to].push(newTransaction);
            emit TransactionExecuted(msg.sender, _to, _amount);
        }

        function getTransactionHistory(address _user) public view returns
(Transaction[] memory) {
            return transactionHistory[_user];
        }
    }
```

Лістинг 3.2 - Код контракту з новою функцією

Аналіз безпеки розроблявся з урахуванням нових загроз. Зокрема, розглядалася атака front-running, коли зловмисник може перехопити транзакцію restrictUserTransactions, щоб виконати власну транзакцію до блокування. Для зменшення цього ризику було додано перевірки, які не дозволяють змінювати статус обмеження для адміністраторів. Також аналізувалася атака gas griefing, коли зловмисник може намагатися перевантажити контракт, викликаючи функції з високими витратами газу. Для захисту функція executeTransaction була оптимізована, щоб мінімізувати операції з масивами, а функція restrictUserTransactions використовувала лише одну зміну стану, що робило її економною. Інтеграція з фронтендом розширювалася шляхом створення веб-додатку на JavaScript із бібліотекою Web3.js. Розроблявся простий інтерфейс, де користувачі могли підключити MetaMask, зареєструватися, виконувати транзакції, блокувати інших користувачів (якщо вони адміністратори) та переглядати історію. Нижче наведено приклад коду для виклику функції restrictUserTransactions:

```
async function restrictUser(web3, contract, account, userAddress, restrict) {
    try {
        await contract.methods.restrictUserTransactions(userAddress,
restrict).send({ from: account });
        console.log(`User ${userAddress} restriction set to ${restrict}`);
    } catch (error) {
        console.error("Error restricting user:", error);
    }
}
```

Лістинг 3.3 - Код для виклику функції restrictUserTransactions:

Цей код інтегрувався в HTML-сторінку з кнопками для виклику функцій, що дозволяло адміністраторам легко керувати обмеженнями через браузер. Тестування показало, що інтерфейс коректно обробляє події, такі як UserRestrictionUpdated, і відображає зміни в реальному часі. Аналіз витрат газу проводився для нової функції restrictUserTransactions. Тестування в Remix показало, що виклик функції коштує приблизно 30,000 одиниць газу, що є економним завдяки мінімальним змінам стану. Для порівняння, функція

executeTransaction споживала до 70,000 одиниць через подвійний запис у масиви. Оптимізація передбачала уникнення складних циклів і використання простих операцій, таких як зміна булевого значення. У майбутньому планується реалізувати обмеження розміру історії транзакцій, щоб ще більше зменшити витрати. Тестування нової функції проводилося в Ropsten. Адміністратор реєстрував користувача, викликав restrictUserTransactions для блокування, після чого користувач намагався виконати транзакцію, отримуючи помилку. Зняття обмеження дозволяло відновити функціональність. Ці тести підтвердили коректність реалізації та її безпеку. Розробка показала, що контракт може бути застосований у системах, де потрібен динамічний контроль доступу, таких як децентралізовані фінансові платформи.

Розробка смарт-контракту BlockchainManager тривала з метою підвищення його універсальності та підготовки до використання в реальних сценаріях. Писалася нова функція, яка дозволяла б адміністраторам тимчасово призупиняти всі транзакції в контракті, наприклад, у разі виявлення вразливостей або необхідності оновлення. Крім того, аналізувалася масштабність контракту, створювалися автоматичні тести за допомогою Hardhat, а також досліджувалися потенційні сценарії застосування в децентралізованих системах. Нова функція, названа pauseContract, була додана до контракту. Вона дозволяла адміністраторам призупиняти або відновлювати виконання транзакцій для всіх користувачів. Для цього було введено глобальну змінну isPaused, яка перевірялася в функції executeTransaction. Функція pauseContract змінювала стан контракту, викликаючи подію ContractPaused для логування. Розроблялася ця функція з урахуванням безпеки: лише адміністратори могли викликати її, а перевірки забезпечували, що контракт не залишиться в некоректному стані.

Це рішення було важливим для реальних систем, де швидке реагування на проблеми може запобігти значним втратам. Ось оновлений код контракту з новою функцією:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
```

```
contract BlockchainManager {
    enum Role { None, User, Admin }
    struct User {
        address userAddress;
        Role role;
        bool isRegistered;
        bool isRestricted;
    }
    struct Transaction {
        address from;
        address to;
        uint256 amount;
        uint256 timestamp;
    }

    mapping(address => User) public users;
    mapping(address => Transaction[]) public transactionHistory;
    uint256 public userCount;
    bool public isPaused;

    event UserRegistered(address indexed user, Role role);
    event TransactionExecuted(address indexed from, address indexed to, uint256
amount);
    event UserRemoved(address indexed user);
    event UserRestrictionUpdated(address indexed user, bool isRestricted);
    event ContractPaused(bool isPaused);

    modifier onlyAdmin() {
        require(users[msg.sender].role == Role.Admin, "Only admin");
        _;
    }
    modifier onlyRegistered() {
        require(users[msg.sender].isRegistered, "User not registered");
        require(!users[msg.sender].isRestricted, "User is restricted");
        _;
    }
    modifier whenNotPaused() {
        require(!isPaused, "Contract is paused");
        _;
    }

    constructor() {
```

```
            users[msg.sender] = User(msg.sender, Role.Admin, true, false);
            userCount = 1;
            isPaused = false;
            emit UserRegistered(msg.sender, Role.Admin);
        }

        function registerUser(address _userAddress) public onlyAdmin {
            require(!users[_userAddress].isRegistered, "User already registered");
            users[_userAddress] = User(_userAddress, Role.User, true, false);
            userCount++;
            emit UserRegistered(_userAddress, Role.User);
        }

        function removeUser(address _userAddress) public onlyAdmin {
            require(users[_userAddress].isRegistered, "User not registered");
            require(users[_userAddress].role != Role.Admin, "Cannot remove admin");
            delete users[_userAddress];
            userCount--;
            emit UserRemoved(_userAddress);
        }

        function restrictUserTransactions(address _userAddress, bool _restrict)
public onlyAdmin {
            require(users[_userAddress].isRegistered, "User not registered");
            require(users[_userAddress].role != Role.Admin, "Cannot restrict admin");
            users[_userAddress].isRestricted = _restrict;
            emit UserRestrictionUpdated(_userAddress, _restrict);
        }

        function pauseContract(bool _pause) public onlyAdmin {
            isPaused = _pause;
            emit ContractPaused(_pause);
        }

        function executeTransaction(address _to, uint256 _amount) public
onlyRegistered whenNotPaused {
            require(users[_to].isRegistered, "Recipient not registered");
            require(!users[_to].isRestricted, "Recipient is restricted");
            require(_amount > 0, "Amount must be positive");
            Transaction memory newTransaction = Transaction(msg.sender, _to, _amount,
block.timestamp);
            transactionHistory[msg.sender].push(newTransaction);
```

```
            transactionHistory[_to].push(newTransaction);
            emit TransactionExecuted(msg.sender, _to, _amount);
        }

        function getTransactionHistory(address _user) public view returns (Transaction[] memory) {
            return transactionHistory[_user];
        }
    }
```

Лістинг 3.4 - Оновлений код контракту з новою функцією

Аналіз масштабованості контракту проводився для оцінки його здатності обробляти велику кількість користувачів і транзакцій. Розроблявся підхід до оцінки обмежень, пов'язаних із використанням масивів у transactionHistory. Тестування показало, що збереження історії для кожного користувача може стати проблематичним при тисячах транзакцій, оскільки операції з масивами збільшують витрати газу. Для вирішення цього було запропоновано в майбутньому додати функцію очищення старих записів або обмеження розміру історії, наприклад, до 100 транзакцій на користувача. Щодо кількості користувачів, контракт теоретично може підтримувати десятки тисяч, оскільки відображення (mapping) ефективно масштабується, але кожен виклик registerUser додає витрати газу. Писався план оптимізації, який включав використання зовнішніх оракулів для зберігання історії транзакцій, щоб зменшити навантаження на контракт.

Автоматичні тести розроблялися з використанням фреймворку Hardhat для перевірки нової функції pauseContract. Писався тестований сценарій на JavaScript, який розгортав контракт, реєстрував користувачів, призупиняв контракт і перевіряв, чи блокується виконання транзакцій. Нижче наведено приклад тесту:

```
const { expect } = require("chai");

describe("BlockchainManager Pause", function () {
    let contract, admin, user1, user2;
```

```
            beforeEach(async function () {
                [admin, user1, user2] = await ethers.getSigners();
                const               BlockchainManager               =               await
ethers.getContractFactory("BlockchainManager");
                contract = await BlockchainManager.deploy();
                await contract.deployed();
                await contract.registerUser(user1.address);
                await contract.registerUser(user2.address);
            });

            it("should pause and unpause contract", async function () {
                await contract.pauseContract(true);
                await   expect(contract.connect(user1).executeTransaction(user2.address,
100)).to.be.revertedWith("Contract is paused");
                await contract.pauseContract(false);
                await contract.connect(user1).executeTransaction(user2.address, 100);
                const history = await contract.getTransactionHistory(user1.address);
                expect(history.length).to.equal(1);
            });
        });
```

Лістинг 3.5 - Тест

Тести підтвердили, що функція pauseContract коректно блокує та розблоковує транзакції, а подія ContractPaused правильно логується.

Сценарії використання контракту аналізувалися для реальних додатків. Розроблявся план адаптації контракту для децентралізованих систем голосування, де користувачі могли б "голосувати" через транзакції, а адміністратори - керувати доступом і призупиняти голосування за потреби. Наприклад, кожен голос міг би представлятися як транзакція з нульовою сумою, а історія транзакцій - фіксувати результати. Інший сценарій включав використання контракту в системах лояльності, де транзакції представляли б нарахування балів. Ці ідеї показували гнучкість контракту та його потенціал для розширення.

Тестування нової функції проводилося в Ropsten через Remix IDE. Адміністратор викликав pauseContract(true), після чого транзакції блокувалися для всіх користувачів. Після виклику pauseContract(false) функціональність

відновлювалася. Витрати газу для pauseContract склали приблизно 25,000 одиниць, що підтвердило її економічність. Розробка цього етапу підкреслила важливість механізмів аварійного зупинення та гнучкості для реальних блокчейн-додатків.

Розробка смарт-контракту BlockchainManager стала комплексним процесом, який охопив усі етапи створення програмного забезпечення для блокчейну. Писався код, який із кожною ітерацією ставав більш функціональним і безпечним, а аналіз технічних аспектів дозволив підготувати контракт до реального використання.

Спочатку створювався базовий функціонал, що включав реєстрацію та видалення користувачів, виконання транзакцій і збереження їхньої історії. Контракт розроблявся з урахуванням безпеки, використовуючи модифікатори доступу та перевірки умов, щоб захистити від несанкціонованих дій і атак, таких як повторний вхід. Пізніше функціонал розширювався. Додавалася функція restrictUserTransactions, яка дозволяла адміністраторам тимчасово блокувати транзакції окремих користувачів, що було корисно для управління ризиками. Розроблялася нова функція pauseContract, яка забезпечувала можливість зупиняти всі транзакції в контракті, наприклад, у разі виявлення вразливостей. Ці доповнення робили контракт більш гнучким і придатним для критичних систем, де потрібен швидкий контроль. Аналіз безпеки проводився на всіх етапах. Розглядалися атаки, такі як front-running і gas griefing, а також додавалися перевірки для захисту від маніпуляцій. Оптимізація газу була ключовим аспектом: функції, такі як restrictUserTransactions і pauseContract, споживали мінімальні ресурси, тоді як executeTransaction оптимізувалася для зменшення витрат на операції з масивами. Масштабованість аналізувалася з урахуванням обмежень на кількість транзакцій, із планами майбутньої оптимізації через зовнішні оракули або обмеження історії

Інтеграція з фронтендом розроблялася для підвищення зручності. Створювався веб-додаток на Web3.js, який дозволяв користувачам через браузер підключати MetaMask, керувати користувачами, виконувати транзакції та

переглядати історію. Тестування, як ручне в Remix IDE, так і автоматичне через Hardhat, підтвердило надійність усіх функцій. Сценарії використання, такі як децентралізоване голосування чи системи лояльності, показали потенціал контракту для реальних додатків. Розгортання в тестовій мережі Ropsten дозволило перевірити контракт у реальних умовах. Кожна функція тестувалася на коректність, а витрати газу аналізувалися для економічності. У підсумку контракт став не лише академічним проєктом, а й практичним інструментом, готовим до адаптації під різні децентралізовані системи. Розробка показала, як ретельне планування, тестування та ітеративне вдосконалення можуть створити надійне блокчейн-рішення.

3.4 Висновки по розділу

Незважаючи на потенціал блокчейн-технологій, у країнах, що розвиваються, їх широкомасштабне впровадження ускладнене через відсутність доступу до Інтернету, цифрову нерівність та нестачу інфраструктури відкритих ключів. Навіть серед освічених користувачів спостерігається низький рівень володіння криптографічними

ВИСНОВКИ

Впровадження та широке використання технологій блокчейн стикаються з викликами, які вже знайомі фахівцям з ІКТ для розвитку. Можливо, новим інгредієнтом у цій суміші є складність самої технології блокчейн. Це створює додаткові проблеми та перешкоди як з точки зору впровадження технології, так і її поширення серед кінцевих користувачів та зацікавлених сторін. Це, безумовно, стосується ситуацій, коли розвиток інфраструктури та місцеві потужності нижчі за середні світові показники. Технологія блокчейн все ще перебуває на початковій стадії розвитку та підтримується відносно невеликою, але висококваліфікованою групою новаторів та технопідприємців. Разом вони могли б вирішити більшість, якщо не всі, обмеження та проблеми, висвітлені в цій статті. Таким чином, інноваційний потенціал блокчейну є великим. Хоча це багато говорить про технологію блокчейн, ще зарано робити остаточні висновки про те, як вона розвиватиметься протягом наступних п'яти років. Наразі ажіотаж навколо неї є лідируючим фактором. Але поточні дані щодо впровадження технології блокчейн показують, що вона все ще перебуває на стадії підтвердження концепції.

Багато блокчейн-додатків, розглянутих у цій статті, вже використовуються на практиці. Але більшість із них працюють у невеликому масштабі, мають небагато клієнтів та/або охоплюють небагато зацікавлених сторін, особливо в країнах, що розвиваються. Кілька урядів зробили цей крок і намагаються використати технологію блокчейн для усунення прогалин у наданні суспільних благ. Однак більшість із них працюють у пілотному режимі та не мають чітких довгострокових стратегій. Заміна поточних ініціатив або запуск нових на автономних блокчейн-платформах лише затримає впровадження блокчейну. Найкращим підходом для країн, що розвиваються, є впровадження блокчейн-технологій для доповнення або розширення поточних програм та ініціатив. Це може знизити бар'єри для входу, одночасно збільшуючи шанси на сталий розвиток початкових інвестицій у блокчейн-технології у

середньостроковій перспективі, враховуючи місцеві потреби та прогалини в розвитку.

Проблеми зручності використання також можуть обмежувати поширення блокчейну в країнах, що розвиваються. Широке використання криптографічних інструментів у бідних країнах стикається з серйозними викликами, особливо якщо ініціативи технології блокчейн спрямовані на найбідніші верстви населення. Припущення, що кожен бенефіціар повинен використовувати та керувати закритими та відкритими ключами, є нереалістичним. Відсутність інфраструктури відкритих ключів у більшості країн, що розвиваються, лише посилить цю ситуацію. Єдиний спосіб вийти з цього глухого кута — розробити альтернативи, які нададуть кінцеві користувачі мають доступ до криптографічних інструментів через посередників, таких як громадські організації, малі підприємства та місцеві органи влади. Ключовим моментом тут є те, що кінцевим користувачам не потрібно володіти технологією або безпосередньо використовувати її, щоб отримати вигоду від її розгортання.

Ширші ініціативи технології блокчейн, пов'язані з розумним урядуванням, здаються найкращими для того, щоб зробити блокчейн ключовим каталізатором у наданні суспільних благ. Грошові перекази та цифрові гроші у сфері приватних благ також мають великий потенціал; однак вони можуть не сприяти економічній та фінансовій інтеграції тих, хто знаходиться внизу піраміди. Хоча технологія блокчейн є стандартним носієм децентралізації, ця стаття показала, що майнінг схильний до централізації та концентрації. На ранніх етапах існування блокчейну Bitcoin кожен, хто мав ноутбук або ПК, міг майнити мережу. Сьогодні це можуть зробити лише деякі люди, які мають фінансові ресурси та обладнання для цього та можуть дозволити собі оплачувати високі рахунки за електроенергію. Те саме стосується поняття консенсусу. Технологія блокчейн замінює людський консенсус алгоритмічним консенсусом. Проблема тут полягає не лише в автоматизації консенсусу, але й у представництві та масштабі. Децентралізовані автономні організації та мережі блокчейн невеликі за кількістю залучених людей. 164 Більшість користувачів блокчейну є

клієнтами, які використовують програмне забезпечення для гаманців, і тому не є частиною жодного процесу формування консенсусу, алгоритмічного чи ні. На сьогоднішній день технологія блокчейн здається ідеальною для операцій малого масштабу, враховуючи її відсутність масштабованості та інші обмеження, виділені в цій статті.

Технології блокчейну можуть незабаром порушити розвиток. Однак, це ще лише початок, оскільки ця технологія швидко розвивається. Успіх у країнах, що розвиваються, залежатиме від ефективності блокчейну для сприяння розвитку людства. А це, у свою чергу, залежатиме від того, як будуть вирішуватися теми, висвітлені в попередньому розділі. Одних лише алгоритмів буде недостатньо. Як Інтернет, так і мобільні технології спричинили позитивні зміни в практиці розробки, але не в тій мірі, яка очікувалася на момент їхньої появи. У цьому світлі інше актуальне питання полягає в тому, чи можуть технології блокчейн сприяти глибшим рівням порушень у процесах розробки, ніж їхні попередники. Потенціал є. Але для досягнення такого впливу на процеси розробки потрібні більш цілеспрямовані дії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Antonopoulos A. M. *Mastering Bitcoin: Programming the Open Blockchain.* - 3rd ed. - O'Reilly Media, 2021. - 408 с. - Режим доступу: https://www.oreilly.com/library/view/mastering-bitcoin/9781098100711/

2. Bashir I. *Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained.* - 4th ed. - Packt Publishing, 2020. - 818 с. - Режим доступу: https://www.packtpub.com/product/mastering-blockchain-fourth-edition/9781839213199

3. Nakamoto S. *Bitcoin: A Peer-to-Peer Electronic Cash System.* -White Paper, 2008. - 9 с. - Режим доступу: https://bitcoin.org/bitcoin.pdf

4. Buterin V. *Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform.* - White Paper, 2014. - 36 с. - Режим доступу: https://ethereum.org/en/whitepaper/

5. Swan M. *Blockchain: Blueprint for a New Economy.* - O'Reilly Media, 2015. - 152 с. - Режим доступу: https://www.oreilly.com/library/view/blockchain/9781491920473/

6. Smaho O. *Perspectives of Blockchain Technology Development in the Global Financial Market.* - Економіка та суспільство, 2024. - No. 60. - С. 1–10. - Режим доступу: https://doi.org/10.32782/2524-0072/2024-60-69

7. Tapscott D., Tapscott A. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.* - Penguin Random House, 2016. - 368 с. - Режим доступу: https://www.penguinrandomhouse.com /books/534706/blockchain- revolution-by-don-tapscott-and-alex-tapscott/

8. Dannen C. *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming.* - Apress, 2017. - 197 с. - Режим доступу: https://www.apress.com/gp/book/9781484225349

9. Prusty N. *Building Blockchain Projects.* - Packt Publishing, 2017. - 266 с. - Режим доступу: https://www.packtpub.com/product/building-blockchain-projects/9781787122147

10. Morabito V. *Business Innovation Through Blockchain: The B³ Perspective.* — Springer, 2017. - 185 с. - Режим доступу: https://www.springer.com/gp/book/9783319484778

11. Mougayar W. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology.* - Wiley, 2016. - 208 с. - Режим доступу: https://www.wiley.com/en-us/The+Business+Blockchain-p-9781119300311

12. Hileman G., Rauchs M. *Global Blockchain Benchmarking Study.* — Cambridge Centre for Alternative Finance, 2017. - 122 с. - Режим доступу: https://www.jbs.cam.ac.uk/insight/2017/global-blockchain-benchmarking-study/

13. Zheng Z., Xie S., Dai H.-N., et al. *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.* — IEEE 6th International Congress on Big Data, 2017. - С. 557–564. - Режим доступу: https://doi.org/10.1109/BigDataCongress.2017.85

14. Yaga D., Mell P., Roby N., Scarfone K. *Blockchain Technology Overview.* — NIST Internal Report 8202, 2018. - 66 с. - Режим доступу: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

15. Bonneau J., Miller A., Clark J., et al. *SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies.* - IEEE Symposium on Security and Privacy, 2015. - С. 104–121. - Режим доступу: https://doi.org/10.1109/SP.2015.14

16. Raval S. *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology.* - O'Reilly Media, 2016. - 176 с. - Режим доступу: https://www.oreilly.com/library/view/decentralized-applications/9781491924532/

17. Dhillon V., Metcalf D., Hooper M. *Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You.* — Apress, 2021. — 380 с. — Режим доступу: https://www.apress.com/gp/book/9781484265338

18. Laurence T. *Blockchain for Dummies.* — 3rd ed. — Wiley, 2021. — 256 с. — Режим доступу: https://www.wiley.com/en-us/Blockchain+For+Dummies%2C+3rd+Edition-p-9781119721529

19. Herlihy M. *Blockchains from a Distributed Computing Perspective.* — Communications of the ACM, 2019. — Vol. 62, No. 2. — С. 78–85. — Режим

доступу: https://doi.org/10.1145/3209623

20. Frankenfield J. *Blockchain Explained: How It Works, Benefits, and Challenges.* - Investopedia, 2024. - 10 с. - Режим доступу: https://www.investopedia.com/terms/b/blockchain.asp

21. Solidity Team. *Solidity Documentation: The Smart Contract Programming Language.* - 2024. - Режим доступу: https://docs.soliditylang.org/en/latest/

22. Chainlink Labs. *Chainlink Documentation: Decentralized Oracles for Smart Contracts.* - 2024. -Режим доступу: https://docs.chain.link/

23. IBM. *Hyperledger Fabric Documentation: A Blockchain Platform for Enterprise.* - 2024. - Режим доступу: https://hyperledger-fabric.readthedocs.io/en/latest/

24. Ethereum Foundation. *Ethereum Development Documentation: Building dApps.* - 2024. - Режим доступу: https://ethereum.org/en/developers/docs/

25. Wohrer M., Zdun U. *Smart Contracts: Security Patterns in the Ethereum Ecosystem and Solidity.* - IEEE International Workshop on Blockchain Oriented Software Engineering, 2018. - С. 2–8. - Режим доступу: https://doi.org/10.1109/IWBOSE.2018.8327565

26. ConsenSys. *Truffle Suite Documentation: Smart Contract Development Framework.* -2024. - Режим доступу: https://trufflesuite.com/docs/

27. Narayanam R., Rajaraman S. *Blockchain Application Development with Hyperledger.* - Packt Publishing, 2019. - 422 с. - Режим доступу: https://www.packtpub.com/product/hands-on-blockchain-with-hyperledger/9781788994521

БІБЛІОГРАФІЧНА ДОВІДКА

Тема бакалаврської роботи: " Інтеграція програмування з блокчейном"

Обсяг пояснювальної записки: 56 аркушів

Дата закінчення дипломної роботи 10 червня 2024р.

Підпис студента _____