

МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

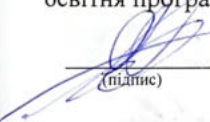
ФАКУЛЬТЕТ ФІНАНСІВ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ

КАФЕДРА ФІНАНСОВИХ РИНКІВ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА (ПРОЄКТ)

на тему: «Технології смарт-контрактів і їх роль в Блокчейн»

Здобувача вищої освіти ІІ рівня, ІІ курсу, ФМФ-22-1 групи,
спеціальності 072 «Фінанси, банківська справа та страхування»,
освітня програма «Фінансові технології»


(підпис)

Яковенко Ярослав Юрійович
(прізвище, ім'я, по батькові)

Науковий керівник


(підпис)

Діденко Людмила Вікторівна, к.е.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

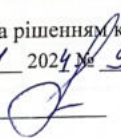
Керівник освітньо-професійної
програми


(підпис)

Корнєєв Володимир Вікторович, д.е.н., професор

Допущено до захисту за рішенням кафедри фінансових ринків та технологій
протокол від «15» 01 2024 р. 9

Завідувач кафедри


Береславська Олена Іванівна, д.е.н., професор

Реєстрація № 17 18.01.2024 Бугдєвська В.С.
(дата) (підпис відповідальної особи)

Результати перевірки до захисту 15.01.2024 [підпис]
(до захисту на доопрацювання) (дата) (підпис)

Результат захисту 5 06.02.2024 [підпис]
(оцінка) (дата) (підпис)

Голова комісії: [підпис] Тришотка А.В.
(підпис) (ініціали, прізвище)

Члени комісії:
[підпис] Береславська О.І.
(підпис) (ініціали, прізвище)
[підпис] Хорьков В.В.
(підпис) (ініціали, прізвище)
[підпис] Діденко Л.В.
(підпис) (ініціали, прізвище)

БЛАНК ОЦІНЮВАННЯ ВИПУСКНОЇ РОБОТИ

Об'єкти контролю	Діапазон оцінки в балах	Фактична кількість балів	Примітки	Дата, П.І.П.: керівника, голови комісії членів комісії, секретаря, (підписи)
ОЦІНЮВАННЯ ДИПЛОМНОЇ РОБОТИ КОМІСІЄЮ ПО ЗАХИСТУ				
1. Доповідь	від 0 до 10	10		<div>Додатковий</div> <div>ВЖ</div> <div>✓</div> <div>Prof.</div>
2. Роздатковий матеріал	від 0 до 5	5		
3. Знання теоретичного та практичного матеріалу, вміння відповідати на запитання	від 0 до 25	25		
4. Апробація (участь у конференціях)	від 0 до 10	10		
РАЗОМ БАЛІВ	від 0 до 50	50		
ЗАГАЛЬНА КІЛЬКІСТЬ БАЛІВ	від 0 до 100	92		

Оцінювання кваліфікаційної роботи науковим керівником - 42 балів.

ПЕРЕВЕДЕННЯ ОЦІНКИ ЗА 100-БАЛЬНОЮ ШКАЛОЮ ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЕКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЕКТС	Оцінка за національною шкалою	Дата	П.І.П.: голови, членів комісії, секретаря, (підпис)
92	A	5	06.02.24	<div>ВЖ</div> <div>ВЖ-1</div> <div>Prof.</div>

Правила переведення оцінок до національної шкали та шкали ЕКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЕКТС	Оцінка за національною шкалою
90-100	A	5 (відмінно)
80-89	B	4 (добре)
70-79	C	3 (задовільно)
60-69	D	
50-59	E	
35-49	FX	2 (незадовільно)

Факультет фінансів та цифрових технологій
Кафедра фінансових ринків та технологій
Спеціальність 072 «Фінанси, банківська справа та страхування»
Освітня програма «Фінансові технології»

Затверджую

Завідувач кафедри фінансових ринків
та технологій

Юлія КОВАЛЕНКО
« 15 » листопада 2022

Завдання на кваліфікаційну роботу (проект)

здобувачу вищої освіти

Яковенко Ярослав Юрійович

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи (проекту)

Технології смарт-контрактів і їх роль в Блокчейн»

Затверджена наказом ректора від 15.11.2022 р. № 1208

2. Строк здачі закінченої роботи 4.12.2023р.

3. Мета дослідження: аналіз технологій смарт-контрактів та їх ролі в блокчейн-технології з метою розкриття їхнього впливу на сучасні транзакційні системи та визначення перспектив використання в різних сферах.

Об'єкт дослідження: технології смарт-контрактів в контексті впровадження в блокчейн-мережі та їх взаємодія з іншими елементами системи.

Предмет дослідження: функціональні можливості смарт-контрактів, їх переваги та недоліки, вплив на безпеку, прозорість та автоматизацію транзакцій.

Орієнтовна база дослідження: інформація та статистичні дані, пов'язані з технологіями смарт-контрактів та їх роллю в Блокчейн.

4. Вихідні дані до роботи: електронні інформаційні ресурси, підручники, зарубіжні електронні ресурси, наукові роботи.

5. Перелік графічного матеріалу: 17 рисунків, 3 таблиці.

6. Зміст випускної кваліфікаційної (дипломної) роботи (перелік питань за кожним розділом):

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ТЕХНОЛОГІЇ С КОНТРАКТІВ І ЇХ РОЛЬ В БЛОКЧЕЙН

- 1.1. Підходи до вивчення сутності та характеристики блокчейн
- 1.2. Дослідження поняття та різновидів смарт-контрактів
- 1.3. Характеристика основних принципів роботи смарт-контрактів

РОЗДІЛ 2. АНАЛІЗ СУЧАСНОГО СТАНУ ТА РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ С КОНТРАКТІВ У БЛОКЧЕЙН

- 2.1. Дослідження сучасних тенденцій розробки смарт-контрактів
- 2.2. Аналіз реалізації блокчейн-платформи для смарт-контрактів
- 2.3. Дослідження практичного впливу технології смарт-контрактів на блокчейн

РОЗДІЛ 3. ОСНОВНІ ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ СМАРТ-КОНТРАКТІВ

7. Календарний план виконання роботи

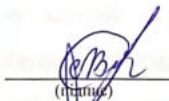
№ п/п	Назва етапів випускної кваліфікаційної (дипломної) роботи	Строк виконання етапів роботи	
		За планом	Фактично
1	2	3	4
1	Підготовка 100 % кваліфікаційної роботи та подання її на перевірку науковому керівнику	29.09.2023 р.	29.09.2023
2	Доопрацювання роботи з урахуванням зауважень керівника та подання її на повторну перевірку керівнику	31.10.2023 р.	31.10.2023
3	Попередній захист кваліфікаційної роботи	11-22.12.2023 р.	
4	Отримання відгуку наукового керівника кваліфікаційної роботи	26-29.12.2023 р.	28.12.2023
5	Рецензування кваліфікаційної роботи	02-09.01.2024 р.	28.12.2023
6	Надання кваліфікаційної роботи для перевірки на плагіат	01.11.2023 р.04.12.2023 р.	04.12.2023
7	ЗАХИСТ	05-06.02.2024 р.	06.02.2024

7. Дата видачі завдання «15» 11 2022

8. Науковий керівник кваліфікаційної роботи (проекту)

9. Гарант освітньо-професійної програми

10. Завдання до виконання отримав здобувач вищої освіти


(підпис)

Діденко Л.В.
(прізвище, ініціал)


(підпис)

Корнєєв В.В.
(прізвище, ініціал)


(підпис)

Яковенко Я
(прізвище, ініціал)

АНОТАЦІЯ

«Технології смарт-контрактів і їх роль в Блокчейн»

Мета дипломної роботи – дослідження технологій смарт-контрактів та їх ролі в блокчейн-технології задля розкриття їх впливу на сучасні транзакційні системи, а також визначення перспектив використання в різних сферах.

Завдання дипломної роботи:

1. Охарактеризувати теоретико-методологічні аспекти технології смарт-контрактів і їх роль в блокчейн;
2. Дослідити сучасні тенденції розробок для смарт-контрактів;
3. Проаналізувати реалізації блокчейн-платформи для смарт-контрактів;
4. Дослідити практичний вплив технології смарт-контрактів на блокчейн;
5. Знайти основні проблеми програмної реалізації смарт-контрактів;
6. Дослідити проблеми та знайти вирішення.

Об'єкт дослідження – технології смарт-контрактів в контексті впровадження в блокчейн-мережі та їх взаємодія з іншими елементами системи.

Предмет дослідження – функціональні можливості смарт-контрактів, їх переваги та недоліки, вплив на безпеку, прозорість та автоматизацію транзакцій.

Кваліфікаційна робота містить 59 сторінок, 17 рисунків, 3 таблиці, список використаних джерел 42 найменування, 7 додатків.

Ключові слова: блокчейн, технологія, біткойн, смарт-контракти, платформа, контракти, ринок.

Рік виконання кваліфікаційної роботи: 2023 рік.

Рік захисту роботи: 2024 рік.

ANNOTATION

«Smart Contract Technologies and Their Role in Blockchain»

The goal of the diploma thesis is to explore smart contract technologies and their role in blockchain technology to reveal their impact on modern transaction systems and identify prospects for their use in various domains.

Tasks of the diploma thesis include:

1. Characterize the theoretical and methodological aspects of smart contract technology and their role in blockchain.
2. Investigate current trends in smart contract development.
3. Analyze implementations of blockchain platforms for smart contracts.
4. Examine the practical impact of smart contract technology on blockchain.
5. Identify key issues in the software implementation of smart contracts.
6. Investigate problems and find solutions.

The object of the research is smart contract technologies in the context of their integration into blockchain networks and their interaction with other elements of the system.

The subject of the research is the functional capabilities of smart contracts, their advantages and disadvantages, and their impact on the security, transparency, and automation of transactions.

The qualification work comprises 59 pages, 17 figures, 3 tables, a list of 42 references, and 7 appendices.

Keywords: blockchain, technology, bitcoin, smart contracts, platform, contracts, market.

Year of qualification work completion: 2023.

Year of thesis defense: 2024.

ЗМІСТ

ВСТУП.....	5
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ТЕХНОЛОГІЇ СМАРТ-КОНТРАКТІВ І ЇХ РОЛЬ В БЛОКЧЕЙН.....	8
1.1. Підходи до вивчення сутності та характеристики блокчейн.....	8
1.2. Дослідження поняття та різновидів смарт-контрактів.....	14
1.3. Характеристика основних принципів роботи смарт-контрактів.....	17
РОЗДІЛ 2. АНАЛІЗ СУЧАСНОГО СТАНУ ТА РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ СМАРТ-КОНТРАКТІВ У БЛОКЧЕЙН.....	22
2.1. Дослідження сучасних тенденцій розробки смарт-контрактів.....	22
2.2. Аналіз реалізації блокчейн-платформи для смарт-контрактів.....	28
2.3. Дослідження практичного впливу технології смарт-контрактів на блокчейн.....	31
РОЗДІЛ 3. ОСНОВНІ ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ СМАРТ-КОНТРАКТІВ.....	40
ВИСНОВКИ.....	45
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	48
ДОДАТКИ	

ВСТУП

Актуальність теми. Розвиток інформаційних та цифрових технологій стає неузбагоєнною тенденцією у всіх перспективних галузях. Прогрес швидко змінює технологічний ландшафт, постійно вдосконалюючи його.

На сьогоднішній день однією з важливих галузей цифрових технологій є блокчейн. Цей інноваційний продукт виконує роль розподіленої бази даних, де інформація зберігається у вигляді послідовної ланцюжка блоків, що неперервно розширюється. Кожен блок в мережі блокчейн включає хеш попереднього запису і з'єднується з іншими блоками для підтримки набору транзакцій. Цей спосіб забезпечує розподіленість та довірливість, незалежно від централізованого контролю.

31 жовтня 2008 року Сатоші Накамото представив протокол криптовалюти Bitcoin,

вперше впроваджуючи блокчейн як розподілену інфраструктурну технологію. Ця децентралізована система дозволила користувачам безпечно обмінювати цифрову валюту "Bitcoin", уникнувши централізованого контролю.

Зі зростанням інтересу до блокчейну та його впровадження в різних секторах і галузях, багато секторів представляють значні сфери застосування блокчейну: фінансові, бізнесові, промислові, голосування та багато інших освітніх і медичних застосувань [17], [34]. Проте блокчейн — це нова технологія, і хоча існує значне хвилювання щодо його потенційних переваг, існує також значна неточна інформація та невизначеність щодо потенційної корисності блокчейну загалом.

З огляду на те, що блокчейн-сервіси та платформи набувають популярності, можна очікувати зростання популярності децентралізованих додатків (DApps) у найближчі роки. Багато компаній і розробників вже цікавляться використанням цих технологій для взаємодії з клієнтами через децентралізовану мережу.

Галузі повинні приділити увагу створенню DApps, які здатні отримати широкий розповсюдження, і, ймовірно, це лише питання часу. Таким чином, на ранніх етапах розвитку галузі особливо важливо для бізнесу почати активно розглядати можливості розробки та впровадження DApps, оскільки ці технології можуть стати важливим конкурентним перевагою.

В сучасному інформаційному суспільстві технології блокчейн стають не лише парадигмою децентралізації та безпеки, але й основою для інноваційних рішень у сферах фінансів, бізнесу та громадських послуг. Однією з ключових складових цього технологічного прориву є смарт-контракти — програми, які автоматизують та гарантують виконання умов угод у блокчейн-мережі.

Мета і завдання дослідження. Мета дипломної роботи - дослідження технологій смарт-контрактів та їхню роль в блокчейн-технології з метою розкриття їхнього впливу на сучасні транзакційні системи та визначення перспектив використання в різних сферах. З мети дипломної роботи можна поставити такі завдання:

1. Охарактеризувати теоретико-методологічні аспекти технології смарт-контрактів і їх роль в блокчейн;

2. Дослідити сучасні тенденції розробок для смарт-контрактів;
3. Проаналізувати реалізації блокчейн-платформи для смарт-контрактів;
4. Дослідити практичний вплив технології смарт-контрактів на блокчейн;
5. Знайти основні проблеми програмної реалізації смарт-контрактів;
6. Дослідити проблеми та знайти вирішення.

Об'єкт дослідження - технології смарт-контрактів в контексті їх впровадження в блокчейн-мережі та їх взаємодія з іншими елементами системи.

Предмет дослідження - функціональні можливості смарт-контрактів, їхні переваги та недоліки, вплив на безпеку, прозорість та автоматизацію трансакцій.

Інформаційна база дослідження. В дипломній роботі ми використовували електронні джерела, підручники, наукові статті, міжнародні джерела.

Методи дослідження включають аналіз наукової літератури, вивчення практичних застосувань, порівняльний аналіз технічних рішень в галузі блокчейну та смарт-контрактів, математичне моделювання процесів їх використання, а також статистичний аналіз результатів впровадження в різних секторах економіки.

РОЗДІЛ 1.

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ТЕХНОЛОГІЇ СМАРТ-КОНТРАКТІВ І ЇХ РОЛЬ В БЛОКЧЕЙН

1.1 Підходи до вивчення сутності та характеристики блокчейн

Технологія блокчейн набула величезної популярності в останні роки, революціонізувавши те, як ми сприймаємо управління даними, транзакції та довіру. В основі цієї новаторської технології лежить теорія блокчейну, фундаментальна концепція, яка лежить в основі її дизайну та функціональності.

Блокчейн — це розподілена база даних або книга, яка спільно використовується вузлами комп'ютерної мережі. Вони найбільш відомі своєю ключовою роллю в системах криптовалют для підтримки безпечного та децентралізованого запису транзакцій, але вони не обмежуються використанням криптовалюти. Блокчейни можна використовувати, щоб зробити дані в будь-якій галузі незмінними — термін, який використовується для опису неможливості змінювати[9].

Оскільки неможливо змінити блок, єдина довіра потрібна до точки, де користувач або програма вводить дані. Цей аспект зменшує потребу в довірених третіх сторонах, якими зазвичай є аудитори чи інші люди, які додають витрат і роблять помилки[1].

З моменту появи біткойна в 2009 році використання блокчейну вибухнуло завдяки створенню різноманітних криптовалют, програм децентралізованого фінансування (DeFi), незамінних токенів (NFT) і смарт-контрактів.

Можливо, ви знайомі з електронними таблицями чи базами даних. Блокчейн дещо схожий, оскільки це база даних, у яку вводиться та зберігається інформація. Але ключова відмінність між традиційною базою даних або електронною таблицею та блокчейном полягає в тому, як дані структуровані та доступні.

Блокчейн складається з програм, які називаються сценаріями, які виконують завдання, які ви зазвичай виконуєте в базі даних: введення інформації та отримання доступу до неї, збереження та зберігання її десь. Блокчейн є розподіленим, що означає, що кілька копій зберігаються на багатьох машинах, і всі вони повинні збігатися, щоб він був дійсним[12].

Блокчейн збирає інформацію про транзакції та вводить її в блок, подібний до комірки в електронній таблиці, що містить інформацію. Після заповнення інформація проходить через алгоритм шифрування, який створює шістнадцяткове число, яке називається хеш.

Потім хеш вводиться в наступний заголовок блоку та шифрується з іншою інформацією в блоці. Це створює серію блоків, які з'єднані разом.

Транзакції слідує за певним процесом, залежно від блокчейну, на якому вони відбуваються. Наприклад, у блокчейні біткойна, якщо ви ініціюєте транзакцію за допомогою свого криптовалютного гаманця — програми, яка надає інтерфейс для блокчейну, — це запускає послідовність подій (рис. 1.1).

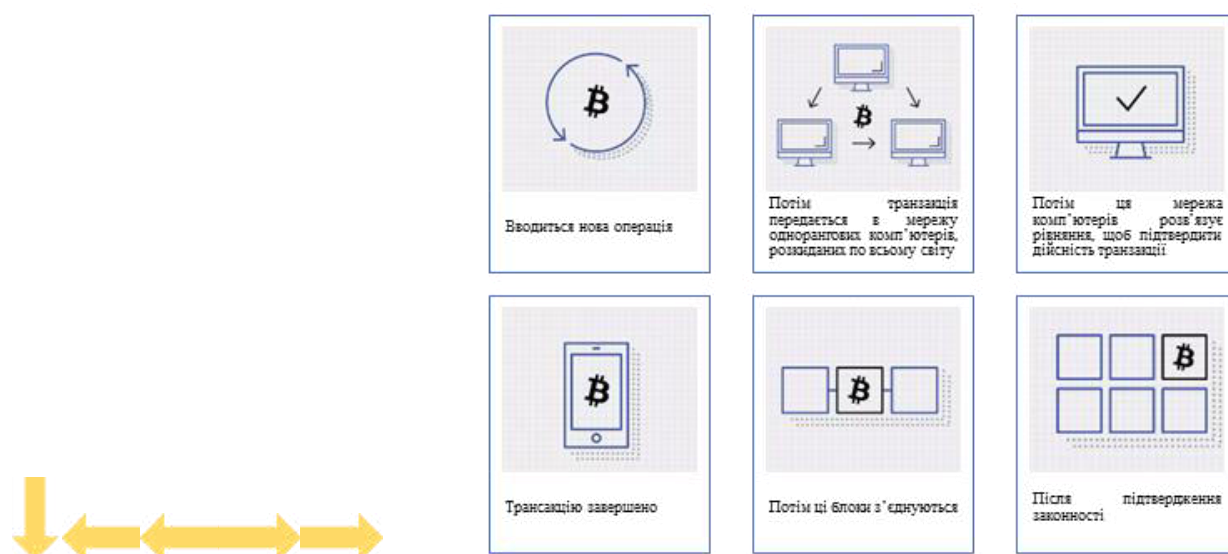


Рис. 1.1. Процеси транзакції у блокчейні біткойна

Джерело: побудовано автором на основі даних: [12]

Вся мережа працює одночасно, намагаючись «розгадати» хеш. Кожен з них генерує випадковий хеш, за винятком "nonce", скорочення від числа, використаного один раз.

Кожен майнер починає з нуля, який додається до випадково згенерованого хешу. Якщо це число не дорівнює або менше цільового хешу, значення одиниці додається до nonce і генерується новий хеш блоку. Це триває до тих пір, поки майнер не згенерує дійсний хеш, виграє гонку та отримає винагороду[10].

Після закриття блоку транзакція завершується. Однак блок не вважається підтвердженим, доки п'ять інших блоків не будуть перевірені. Підтвердження займає в мережі приблизно одну годину, оскільки в середньому це становить трохи менше 10 хвилин на блок (перший блок із вашою транзакцією та п'ять наступних блоків, помножені на 10, дорівнюють приблизно 60 хвилинам).

Не всі блокчейни дотримуються цього процесу. Наприклад, мережа Ethereum випадковим чином вибирає один валідатор з усіх користувачів, які мають ставку на ефір, для перевірки блоків, які потім підтверджуються мережею. Це набагато швидше та менш енергоємно, ніж процес біткойна.

Блокчейн дозволяє розподіляти дані в базі даних між кількома вузлами мережі — комп'ютерами або пристроями, на яких працює програмне забезпечення для блокчейну — у різних місцях. Це не тільки створює надмірність, але й підтримує точність даних. Наприклад, якщо хтось спробує змінити запис в одному екземплярі бази даних, інші вузли завадять цьому. Таким чином, жоден окремий вузол у мережі не може змінити інформацію, що зберігається в ньому[12].

Завдяки цьому розповсюдженню — і зашифрованому доказу того, що робота була виконана — інформація та історія (як і транзакції в криптовалюті) незворотні. Таким записом може бути список транзакцій (наприклад, з криптовалютою), але блокчейн також може зберігати різноманітну іншу інформацію, як-от юридичні контракти, державні ідентифікатори або інвентаризація компанії.

Через децентралізовану природу блокчейну біткойнів усі транзакції можна прозоро переглядати, маючи особистий вузол або використовуючи дослідники блокчейнів, які дозволяють будь-кому бачити транзакції, що відбуваються в реальному часі. Кожен вузол має власну копію ланцюга, яка оновлюється, коли підтверджуються та додаються нові блоки. Це означає, що якщо ви захочете, ви можете відстежувати біткойни, куди б вони не йшли.

Наприклад, раніше біржі були зламані, що призвело до втрати великої кількості криптовалют. Хоча хакери могли бути анонімними, за винятком адреси свого гаманця, криптовалюту, яку вони видобули, легко відстежити, оскільки адреси гаманців опубліковані в блокчейні[13].

Звичайно, записи, що зберігаються в блокчейні Bitcoin (як і в більшості інших), зашифровані. Це означає, що лише особа, якій присвоєно адресу, може розкрити свою особу. У результаті користувачі блокчейну можуть залишатися анонімними, зберігаючи при цьому прозорість.

Блокчейн можна використовувати для незмінного запису будь-якої кількості точок

даних. Це може бути у формі транзакцій, голосів на виборах, інвентаризації продуктів, державних ідентифікаторів, актів на будинки та багато іншого.

Наразі десятки тисяч проєктів прагнуть запровадити блокчейни різними способами, щоб допомогти суспільству, крім простого запису транзакцій, наприклад, як спосіб безпечного голосування на демократичних виборах.

Природа незмінності блокчейну означає, що шахрайське голосування стане набагато складнішим. Наприклад, система голосування може працювати так, що громадянам кожної країни буде видана одна криптовалюта або токен.

Тоді кожному кандидату буде надана конкретна адреса гаманця, і виборці надсилатимуть свій токен або криптовалюту на адресу будь-якого кандидата, за якого вони бажають проголосувати. Прозорий і відстежуваний характер блокчейну позбавить від необхідності підрахунку голосів людьми та можливості зловмисників підробляти фізичні бюлетені.

Блокчейни були проголошені руйнівною силою у фінансовому секторі, особливо з функціями платежів і банківських операцій. Однак банки та децентралізовані блокчейни суттєво відрізняються.

Щоб побачити, чим банк відрізняється від блокчейну, давайте порівняємо банківську систему з реалізацією блокчейну Bitcoin(табл1.1).

Таблиця 1.1.

Різниця банківської системи з реалізацією блокчейну Bitcoin

Особливість	Банки	Bitcoin
Час роботи	Звичайні банки відкриті з 9:00 до 17:00 у будні дні. Деякі банки працюють у вихідні, але в обмежений час. Усі банки закриті у святкові дні.	Немає встановлених годин; працює 24/7, 365 днів на рік.
Плата за транзакцію	Платежі картою: ця комісія залежить від картки та не сплачується безпосередньо користувачем. Комісія сплачується платіжним процесором магазинами та зазвичай стягується за транзакцію. Вплив цієї комісії іноді може призвести до зростання вартості товарів і послуг. • Чеки: можуть коштувати від 1 до 30 доларів США залежно від вашого банку. • АСН: перекази АСН можуть коштувати до 3 доларів США при надсиланні на зовнішні облікові записи. • Електронний переказ: вихідні внутрішні	У біткойн є змінна комісія за транзакції, яка визначається майнерами та користувачами. Ця плата може коливатися від 0 до 50 доларів, але користувачі мають можливість визначати, яку суму комісії вони готові заплатити. Це створює відкритий ринок, де, якщо користувач встановить занадто низьку комісію, його транзакція може бути не оброблена.

	банківські перекази можуть коштувати 25 доларів США. Вихідні міжнародні банківські перекази можуть коштувати 45 доларів США.	
Швидкість транзакції	• Платежі карткою: 24-48 годин • Чеки: 24-72 години для оформлення • АСН: 24-48 годин • Електронний переказ: протягом 24 годин, якщо не існує міжнародних * Банківські перекази зазвичай не обробляються у вихідні та святкові дні	Транзакції з біткойнами можуть тривати від 15 хвилин до години залежно від завантаженості мережі.
Знає правила свого клієнта	Банківські рахунки та інші банківські продукти вимагають процедур «Знай свого клієнта» (KYC). Це означає, що за законом банки зобов'язані реєструвати ідентифікаційні дані клієнта перед відкриттям рахунку.	Будь-хто або будь-що може брати участь у мережі Bitcoin без ідентифікації. Теоретично навіть сутність, оснащена штучним інтелектом, може брати участь.
Легкість переказів	Посвідчення особи державного зразка, банківський рахунок і мобільний телефон є мінімальними вимогами для цифрових переказів.	Підключення до Інтернету та мобільний телефон є мінімальними вимогами.
Конфіденційність	Інформація про банківський рахунок зберігається на приватних серверах банку та зберігається клієнтом. Конфіденційність банківського рахунку обмежується тим, наскільки захищені сервери банку та наскільки окремий користувач захищає свою власну інформацію. Якщо сервери банку будуть скомпрометовані, обліковий запис особи також буде зламано.	Біткойн може бути настільки конфіденційним, наскільки того забажає користувач. Усі біткойни можна відстежити, але неможливо встановити, кому належить біткойн, якщо він був придбаний анонімно. Якщо біткойн купується на біржі KYC, то біткойн безпосередньо прив'язується до власника облікового запису біржі KYC.
Безпека	Якщо припустити, що клієнт використовує надійні заходи безпеки в Інтернеті, як-от використання надійних паролів і двофакторної автентифікації, інформація банківського рахунку настільки ж безпечна, наскільки надійний сервер банку, який містить інформацію про обліковий запис клієнта.	Чим більшою стає мережа Bitcoin, тим більшою вона стає безпечною. Рівень безпеки, яку має власник біткойна з власним біткойном, повністю залежить від нього. З цієї причини людям рекомендується використовувати холодне зберігання для більшої кількості біткойнів або будь-якої суми, яка призначена для зберігання протягом тривалого періоду часу.
Схвалені транзакції	Банки залишають за собою право відмовити в транзакціях з різних причин. Банки також залишають за собою право блокувати рахунки. Якщо ваш банк помітить покупки в незвичайних місцях або незвичайні товари, їм може бути відмовлено.	Сама мережа біткойн не визначає, як використовується біткойн у будь-якій формі. Користувачі можуть здійснювати транзакції з біткойнами, як вважають за потрібне, але також повинні дотримуватися вказівок своєї країни чи регіону.
Арешти рахунків	Завдяки законам KYC уряди можуть легко відстежувати банківські рахунки людей і конфіскувати активи на них з різних причин.	Якщо біткойн використовується анонімно, урядам буде важко відстежити його, щоб конфіскувати.

Джерело: розроблено автором на основі даних[12]

Як ми тепер знаємо, блоки в блокчейні біткойна зберігають дані транзакцій. Сьогодні більше 23 000 інших систем криптовалюти працюють на блокчейні. Але виявилось, що блокчейн є надійним способом зберігання даних про інші види транзакцій.

Деякі компанії, які експериментують з блокчейном, включають Walmart, Pfizer, AIG, Siemens і Unilever, серед інших. Наприклад, IBM створила свій блокчейн Food Trust, щоб відстежувати шлях, який харчові продукти проходять, щоб дістатися до місця розташування[20].

Харчова промисловість бачила незліченну кількість спалахів E. coli, сальмонели та лістерії; у деяких випадках небезпечні матеріали були випадково введені в харчові продукти. У минулому потрібні були тижні, щоб знайти джерело цих спалахів або причину хвороби через те, що люди їдять.

Використання блокчейну дозволяє брендам відстежувати маршрут харчового продукту від його походження, через кожну зроблену зупинку, до доставки. Мало того, ці компанії тепер також можуть бачити все інше, з чим вони могли контактувати, дозволяючи виявити проблему набагато швидше, що потенційно рятує життя. Це один приклад блокчейну на практиці, але існує багато інших форм реалізації блокчейну.

1.2 Дослідження поняття та різновидів смарт-контрактів

Смарт-контракти є наступним кроком в еволюції технології блокчейн. Вони поєднують найкращі аспекти класичного контракту та комп'ютерної програми, дозволяючи користувачам створювати повністю автономні угоди, які можна виконувати без участі людини. Метою смарт-контрактів є виконання умов угоди, не вдаючись до послуг стороннього посередника[3].

Розумні контракти працюють з використанням комбінації коду та блокчейну, що дозволяє всім учасникам мережі отримувати доступ до інформації в будь-який час і з будь-якої точки світу. Смарт-контракт містить усі умови угоди на мові програмування, що дозволяє автоматично виконувати зобов'язання обох сторін після виконання певних попередньо встановлених умов.

Смарт-контракти наразі є однією з найцікавіших і перспективних розробок у світі технології блокчейн, оскільки вони здатні оптимізувати та захистити багато аспектів бізнес-процесів. Вони мають широкий спектр застосувань, від надання фінансових послуг до створення децентралізованих цифрових ідентифікаторів[39].

Розумний контракт — це цифрова угода, підписана та збережена в мережі блокчейн, яка виконується автоматично, коли виконуються умови контракту (T&C); T&C написані на специфічних для блокчейну мовах програмування, таких як Solidity[4].

Можна також розглядати смарт-контракти як блокчейн-програми, які дозволяють усім сторонам виконувати свою частину транзакції. Програми, що працюють на основі смарт-контрактів, часто називають «децентралізованими програмами» або «dapps».

Хоча ідея блокчейну в основному сприймається як основний технологічний драйвер біткойна, з тих пір вона перетворилася на силу, з якою доводиться рахуватися. За допомогою смарт-контрактів виробник, якому потрібна сировина, може встановити платежі, а постачальник може спланувати поставки. Потім, на основі договору між двома організаціями, платежі можуть бути автоматично перераховані продавцю під час відправлення або доставки.

Трохи про історію створення смарт-контрактів. Нік Сабо, американський комп'ютерний науковець, який розробив віртуальну валюту під назвою «Bit Gold» у 1998 році, за десять років до появи біткойна, був першим, хто запропонував розумні контракти в 1994 році. Сабо охарактеризував смарт-контракти як механізми цифрових транзакцій, які реалізують умови договору[40].

Багато передбачень, зроблених Сабо у його статті, тепер є частиною нашого повсякденного життя у спосіб, який передуює технології блокчейн. Однак реалізувати цю ідею не вдалося, оскільки тоді не існувало необхідної технології, насамперед розподіленого реєстру.

У 2008 році Сатоші Накамото представив революційну технологію блокчейн у офіційному документі. Це запобігло вказівці транзакцій в іншому блоці. Однак поява передових технологій послужила стимулом для зростання розумних контрактів. Через п'ять років блокчейн-платформа Ethereum зробила практичне використання розумних контрактів можливим. Ethereum все ще залишається однією з найпоширеніших платформ, що

дозволяють реалізувати смарт-контракти[40].

Традиційний контракт і смарт-контракт — це угоди, які зобов’язують сторони певними зобов’язаннями. Зараз на простому прикладі, я покажу в чому відмінність звичайного контракту від смарт-контракту(табл. 1.2).

Таблиця 1.2.

Відмінність смарт-контракту від звичайного контракти

	Смарт-контракт	Звичайний контракт
Носій	Алгоритм чи програма	Паперовий документ
Мова виконання	Мова програмування: Solidity, Javascript, RIDE та інші	Юридичний, канцелярит
Підстави для виконання	Умови, прописані у смарт-контракті	Закони, нормативи, договори, бажання учасників
Зміни	Після ініціалізації контракту його неможливо змінити	Можна вносити будь-якої миті
Виконання	Прописані у смарт-контракті умови виконуються автоматично усіма учасниками	Кожен учасник сам вирішує, виконувати контракт чи ні, як і за яких умов виконувати
Наслідки невиконання	Штрафи та санкції прописані у смарт-контракті, тому покарання відбувається автоматично	Щоб домогтися виконання або покарати порушника, слід звернутися до суду
Посередники	Ті, що прописані в законі	Нотаріуси, юристи, чиновники, банки, продавці, довірені особи, поручителі та інші
Створення	Потрібна допомога програміста	Потрібна допомога юриста, чиновника, нотаріуса
Носії цінності	Цифрові гроші та сертифікати	Документи, готівкові та цифрові гроші

Джерело: побудоване автором на основі даних[39]

Що стосується типів смарт-контрактів, вони класифікуються на три категорії — юридичні контракти, децентралізовані автономні організації або DAO та логічні контракти. Тут ми докладніше обговоримо кожен з трьох.

1. Розумний правовий договір

Розумні контракти гарантовані законом. Вони дотримуються структури юридичних контрактів: «Якщо це станеться, то це станеться». Оскільки смарт-контракти розміщені на

блокчейні та є незмінними, судові чи юридичні смарт-контракти пропонують більшу прозорість, ніж традиційні документи між замовниками[40].

Залучені сторони оформляють договори за допомогою цифрових підписів. Розумні юридичні контракти можуть виконуватися автономно, якщо виконуються певні передумови, наприклад, здійснення платежу після досягнення певного кінцевого терміну. У разі недотримання вимог зацікавлені сторони можуть зіткнутися із серйозними юридичними наслідками.

2. Децентралізовані автономні організації

DAO — це демократичні групи, керовані розумним контрактом, який надає їм право голосу. DAO виступає як організація, керована блокчейном, зі спільною метою, яка перебуває під колективним контролем. Ні виконавчої влади, ні президента не існує. Натомість принципи, засновані на блокчейні, вбудовані в код контракту, регулюють функціонування організації та розподіл коштів. VitaDAO є прикладом такого типу смарт-контракту, де технологія підтримує спільноту для наукових досліджень.

3. Логічні контракти програми

ALC, або логічні контракти додатків, складаються з програмного коду, який зазвичай синхронізується з різними іншими блокчейн-контрактами. Це забезпечує взаємодію між різними пристроями, як-от Інтернет речей (IoT) або інтеграція з блокчейном. На відміну від інших типів розумних контрактів, вони підписуються не між людьми чи організаціями, а між машинами та іншими контрактами.

1.3 Характеристика основних принципів роботи смарт-контрактів

Як і будь-який інший контракт, смарт-контракт є обов'язковим контрактом між двома сторонами. Він використовує код, щоб скористатися перевагами технології блокчейн, тим самим відкриваючи більшу ефективність, відкритість і конфіденційність. Виконання смарт-контрактів контролюється відносно простими операторами «якщо/коли...тоді...», написаними в коді на блокчейні.

Це кроки, необхідні для функціонування розумних контрактів.

Угода: сторони, які бажають вести бізнес або обмінюватися продуктами чи

послугами, повинні погодитися з умовами угоди. Крім того, вони повинні визначити, як працюватиме смарт-контракт, включаючи критерії, які мають бути виконані для виконання угоди[32].

Створення контракту: учасники транзакції можуть створити смарт-контракт багатьма способами, включаючи створення його самостійно або співпрацюючи з постачальником смарт-контракту. Положення договору задовані мовою програмування. На цьому етапі дуже важливо ретельно перевірити безпеку контракту.

Розгортання: коли контракт буде завершено, його потрібно опублікувати в блокчейні. Смарт-контракт завантажується в блокчейн так само, як і звичайні криптовалютні транзакції, із вставленням коду в поле даних біржі. Після підтвердження транзакції вона вважається активною в блокчейні та не може бути скасована або змінена[40].

Умови моніторингу: смарт-контракт працює, відстежуючи блокчейн або інше надійне джерело для заздалегідь визначених умов або підказок. Такими тригерами може бути будь-що, що можна підтвердити цифровим способом, як-от досягнута дата, здійснений платіж тощо.

Виконання: коли параметри тригера виконуються, смарт-контракт активується відповідно до оператора «якщо/коли...тоді...». Це може реалізовувати лише одну чи кілька дій, як-от передача коштів постачальнику або реєстрація права власності покупця на актив.

Запис: результати виконання контракту оперативно публікуються в блокчейні. Система блокчейн перевіряє виконані дії, реєструє їх виконання як обмін і зберігає укладену угоду на блокчейні. Цей документ доступний у будь-який час[40].

Розумні контракти можна використовувати для керування багатьма транзакціями, від переказу грошей між сторонами до складних бізнес-процесів, таких як нарахування заробітної плати та управління запасами. Це пов'язано з їх можливостями: автоматизація рутинних завдань, виключення посередників, і, відповідно, зниження транзакційних витрат, зменшення помилок через людський фактор. Завдяки цим можливостям технологія смарт-контрактів знаходить своє застосування в багатьох сферах:

DeFi (децентралізовані фінанси) — це термін, який стосується використання смарт-контрактів для фінансових операцій. Його часто використовують як синонім криптовалютного кредитування, але насправді він охоплює набагато більше, ніж просто

кредитування. Децентралізоване фінансування можна використовувати різними способами: однорангова торгівля криптовалютою, торгівля деривативами через біржу деривативів, децентралізовані біржі (DEX) тощо[39].

Смарт-контракти також можна використовувати для краудфінансування. Краудсорсингове фінансування – це процес залучення грошей від великої кількості інвесторів (зазвичай невеликих сум). Це стало популярним способом фінансування нових підприємств, проектів у соціальних мережах і навіть фільмів. Такі сервіси, як Kickstarter і Indiegogo, є прикладами платформ, що використовують подібну систему[39].

DAO — це децентралізована організація, яка використовує технологію блокчейн для забезпечення прозорості фінансів і управління. Основна мета організації цього типу — зменшити потребу в централізованих органах влади, зменшити операційні витрати та підвищити ефективність. Найпоширенішим варіантом використання є автоматизація певних бізнес-функцій, таких як управління фондами та прийняття рішень.

GameFi — це інноваційна тенденція, яка об'єднує дві найпопулярніші індустрії — ігри та блокчейн. Проект — це екосистема, яка об'єднує гравців, розробників, видавців, впливових людей і рекламодавців. Мета полягає в тому, щоб створити децентралізований ринок, де всі учасники можуть безпосередньо взаємодіяти один з одним. Система використовує смарт-контракти для забезпечення безпеки коштів користувачів, можливості надсилання та отримання платежів[30].

Розумні контракти є важливою частиною технології блокчейн, тому вони часто використовуються в ICO (первинні пропозиції токенів) для контролю над випуском токенів. Алгоритми запрограмовані на ідентифікацію користувачів, які вклали свої кошти в проект, і внесення їх до загального реєстру. Після реєстрації користувачі автоматично отримують необхідну кількість токенів.

Окрім керування розповсюдженням токенів, смарт-контракти автоматизують нарахування шляхом ідентифікації користувачів-інвесторів і допомагають перевірити їх легітимність шляхом автоматичного моніторингу відповідей користувачів на транзакції[39].

Інші застосування смарт-контрактів:

- Охорона здоров'я: Обмін даними пацієнтів і керування ними, включаючи історію хвороби, інформацію про страхування та іншу особисту інформацію.

- IoT (Інтернет речей): автоматизуйте керування пристроями IoT, включаючи їх розташування, функціональність і статус.
- Страхування: управління претензіями щодо страхових полісів. Розумні контракти можуть усунути шахрайство та зменшити витрати шляхом автоматизації таких процесів, як перевірка вимог і розподіл виплат.
- Азартні ігри: забезпечення чесних і прозорих умов для гравців. Розумні контракти можуть усунути шахрайство та зменшити витрати завдяки автоматизації перевірки виплат.
- Обсяг поставки: відстеження руху товару від пункту відправлення до пункту призначення з гарантією своєчасної та повної оплати товарів та послуг.
- Вибори: смарт-контракти можна використовувати для автоматизації процесу голосування та точного підрахунку голосів, виключаючи помилки та фальсифікації.
- Мистецтво та медіа: відстеження прав власності на твори мистецтва та медіа.
- Оподаткування: автоматизація розрахунків і збору податків.

Отже, смарт-контракти представляють собою програмні коди, розгорнуті на блокчейн-платформі, які автоматизують виконання угод, не потребуючи посередницьких служб. Вони визначають умови та наслідки угод, забезпечуючи автономність, безпеку та довіру в транзакціях. Роль смарт-контрактів в блокчейні полягає в створенні децентралізованих та прозорих систем, сприяючи автоматизації і забезпеченню надійності угод між сторонами. Це інноваційне рішення в області фінансів, логістики, медицини та багатьох інших галузях, що перетворює спосіб укладання угод і підвищує рівень довіри в електронних транзакціях.

РОЗДІЛ 2.

АНАЛІЗ СУЧАСНОГО СТАНУ ТА РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ СМАРТ-КОНТРАКТІВ У БЛОКЧЕЙН

2.1. Дослідження сучасних тенденцій розробки смарт-контрактів

Розумний контракт — це угода між двома або більше сторонами, яка зберігається в блокчейні, наприклад Ethereum або EOS. Кожен такий контракт має попередньо визначений набір правил і умов і автоматично виконується, коли ці умови виконуються. Ці контракти гарантовані консенсусом усієї мережі блокчейнів. Ніхто не може їх змінити, якщо вся мережа не схвалить зміни. Це робить розумні контракти одним із найбезпечніших і найпотужніших інструментів для створення угод між різними сторонами. Ось як ваш бізнес може отримати користь від розробки розумних контрактів[8].

Як і будь-який традиційний контракт, смарт-контракти — це угоди щодо правил, які визначають відносини між різними сторонами. Однак смарт-контракти також пропонують ряд додаткових переваг(табл. 2.1).

Таблиця 2.1.

Переваги смарт-контрактів

Гарантований результат	Смарт-контракти є самовиконуваними. Після виконання узгоджених умов договір виконується автоматично. Це позбавляє від необхідності судового розгляду або ручного примусового виконання контракту.
Точність	Щоб уникнути помилок транзакцій, умови кожного смарт-контракту мають бути визначені з великою точністю. Це робить розумні контракти дуже точними.
Прозорість	Технологія блокчейн базується на принципах децентралізації та прозорості. Це гарантує, що умови контракту видимі всім у блокчейні та не можуть бути оскаржені.
Безпека	Ступінь криптографічної безпеки смарт-контрактів гарантує, що вони не можуть бути підроблені. Крім того, через розподілену природу цих контрактів не може статися втрата даних.
Швидкість	На відміну від стандартних бізнес-процедур, розумні контракти виконуються негайно, що робить їх високоефективними.
Довіра	Природа розумних контрактів робить їх надійними інструментами, які усувають можливість маніпуляцій або помилок.
Незалежність	Технологія смарт-контрактів не покладається на залучення третіх сторін або посередників.
Економія	Завдяки автоматизованому характеру цих контрактів вони зменшують потребу в посередниках, а також витрати, пов'язані з помилками обробки.

Джерело: побудоване автором на основі даних[30]

Розробка смарт-контракту, також відомого як його життєвий цикл, проходить кілька етапів. Це гарантує, що бізнес-вимоги правильно визначені та забезпечені технологією. Ось як розробляється смарт-контракт:

1. Визначте бізнес-логіку та вимоги

Залучені сторони визначають конкретні бізнес-умови смарт-контракту та повідомляють їх розробнику.

2. Розробіть архітектуру смарт-контракту

Після визначення бізнес-логіки розробники проєктують архітектуру контракту, щоб представити цю логіку. Це служить схемою під час процесу розробки.

3. Розробіть смарт-контракт

Цей етап передбачає написання коду смарт-контракту для обраної платформи блокчейн (наприклад, Ethereum, EOS тощо). Цей крок також включає модульне тестування, щоб визначити, чи виконується контракт, як задумано.

4. Внутрішня ревізія

Виконується внутрішній аудит через локальний блокчейн, а потім через тестову

мережу. Аудит перевіряє, чи контракт функціонує належним чином і чи відповідає всім стандартам безпеки.

5. Розгортання на блокчейні

Контракт розгортається на ринку, на якому він буде працювати.

6. Прості розумні контракти

Ця категорія включає контракти, які мають правові наслідки для сторін, які не виконують свою частину угоди. Вони також відомі як розумні юридичні контракти.

7. Складні розумні контракти

Складні контракти включають децентралізовані автономні організації (DAO) і контракти логіки додатків (ALC). DAO є формою блокчейн-спільноти. Ця спільнота працює та регулюється набором правил за допомогою ряду смарт-контрактів. ALC представляють взаємодію між розумними контрактами та Інтернетом речей (IoT). ALC служать для перевірки та підтримки зв'язку між пристроями в IoT[30].

Розробка контракту на блокчейні Ethereum вимагає специфічного інженерного підходу, який відрізняється від того, який застосовують більшість веб- та мобільних розробників. На відміну від сучасних мов програмування, які підтримують широкий спектр зручних типів даних для зберігання та маніпуляції, розробник контракту відповідає за внутрішню організацію та маніпулювання даними на більш глибокому рівні. Це означає, що розробник повинен звертати увагу на деталі, які зазвичай не є предметом уваги в інших мовах програмування. Наприклад, від нього може залежати реалізація методу з'єднання рядків або перетворення рядків у нижній регістр, завдання, з якими розробники інших мов зазвичай не стикаються.

Крім того, платформа Ethereum і мова програмування Solidity постійно розвиваються на високих темпах, і розробники стикаються з постійними змінами у функціоналі платформи та в області безпеки через додавання нових інструкцій та виявлення нових помилок та ризиків безпеки. Розробники повинні усвідомлювати, що написаний сьогодні код може не скомпільоватися протягом кількох місяців або, принаймні, йому може знадобитися переробка.

Смарт-контракти в Ethereum зазвичай написані мовами вищого рівня, які потім компілюються в байт-код EVM. Такі мови включають LLL (Low-level Lisp-like Language)

[22], Serpent (аналог мови Python) [27], Viper (мова, схожа на Python) [16], та Solidity (аналог мови JavaScript) [33]. LLL і Serpent були розроблені на початкових етапах розвитку платформи, тоді як Viper наразі знаходиться в процесі розробки і призначений для заміни Serpent. Найбільш відомою і широко використовуваною з них є мова Solidity.

Solidity - це високорівнева мова програмування, яка є Тьюрінг-повною, із синтаксисом, аналогічним JavaScript. Вона статично типізована, підтримує спадковість і поліморфізм, а також має бібліотеки та складні типи, визначені користувачем. При використанні Solidity для розробки контрактів їх структура схожа на класи в об'єктно-орієнтованих мовах програмування. Код контракту складається зі змінних і функцій, які зчитують і змінюють їх, подібно до традиційного імперативного програмування. Solidity визначає спеціальні змінні (msg, block, tx), які завжди доступні у глобальному просторі імен і містять властивості для отримання інформації про транзакцію виклику та блокчейн, такі як вихідна адреса, кількість ефіру та дані, передані разом із транзакцією виклику.

Ще однією важливою та зручною функцією у Solidity є так звані модифікатори. Модифікатори можна описати як закриті блоки коду, які розширюють функції, змінюючи їх потік виконання коду. Цей підхід відповідає парадигмі умовно-орієнтованого програмування (COP), що ставить своєю метою уникнення умовних шляхів у тілах функцій.

Модифікатори можна використовувати для легкої зміни поведінки функцій, просто додаючи їх у список, розділений пробілами, після імені функції. Один з типових сценаріїв використання модифікаторів - перевірка певних умов перед виконанням функції.

Ще однією важливою та організованою особливістю Solidity є події. Події - це сигнали, які смарт-контракти можуть спричинити. Користувачі та програми можуть слухати ці події в блокчейні без додаткових витрат і реагувати на них відповідно. Крім того, події можуть використовуватися для реєстрації. Коли події викликаються, вони зберігають свої аргументи в журналі транзакцій, спеціальній структурі даних в блокчейні, яка залишається в історії блоків. Ці журнали пов'язані з адресою контракту і можуть ефективно використовуватися за межами блокчейну.

Для розробки, компіляції та тестування створеного смарт-контракту можна використовувати середовище розробки Remix IDE. Remix IDE [25] - це програмне забезпечення для створення веб-версій Ethereum, яке дозволяє розробляти смарт-контракти

Solidity. Розробник контракту працює на віртуальній машині JavaScript, наданій у Remix. Після налагодження контракту його можна опублікувати в Ethereum або на будь-якому блокчейні, що підтримує смарт-контракти Solidity [26]. Це середовище розробки застосовується на всіх етапах розробки смарт-контрактів користувачами на різних рівнях кваліфікації. Воно не потребує складної настройки, сприяє швидкому циклу розробки та має багатий вибір плагінів з інтуїтивно зрозумілим графічним інтерфейсом. Інструмент постачається у двох формах - як веб-додаток (рис. 2.1) або як десктоп-додаток (рис. 2.2), а також як розширення для VSCode [25].

Дане середовище розробки дозволяє:

- Створювати смарт-контракти (додаток А)
- Компілювати смарт-контракти (додаток Б)
- Розгортати смарт-контракти (додаток В)
- Тестувати смарт-контракти (додаток Г).

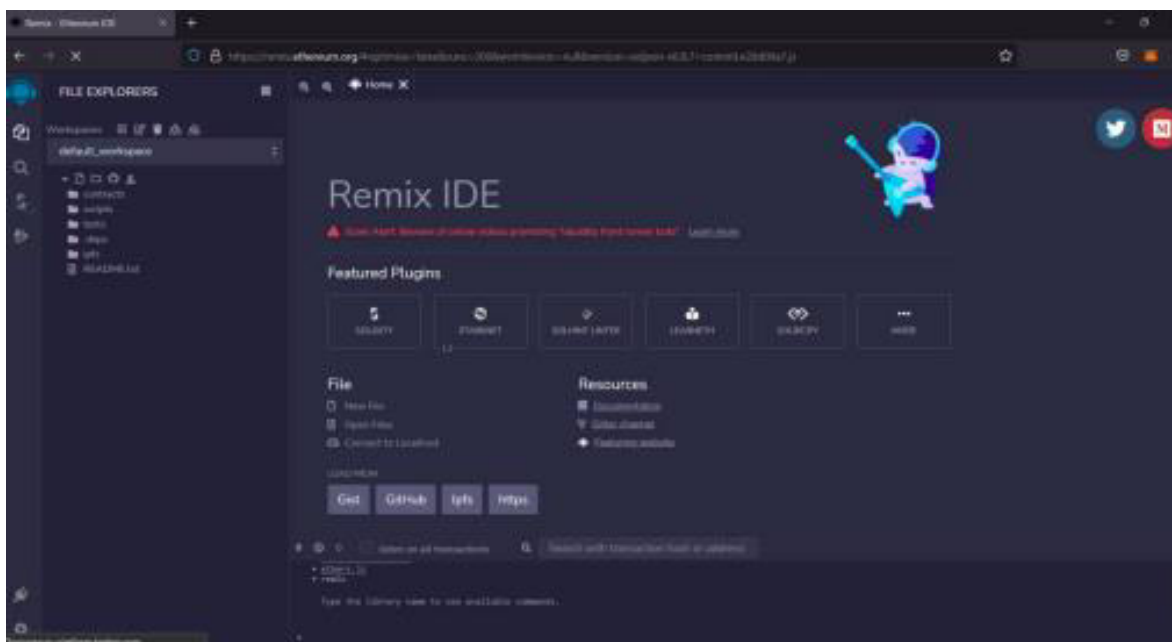


Рис. 2.1. Remix IDE web

Джерело:[26]

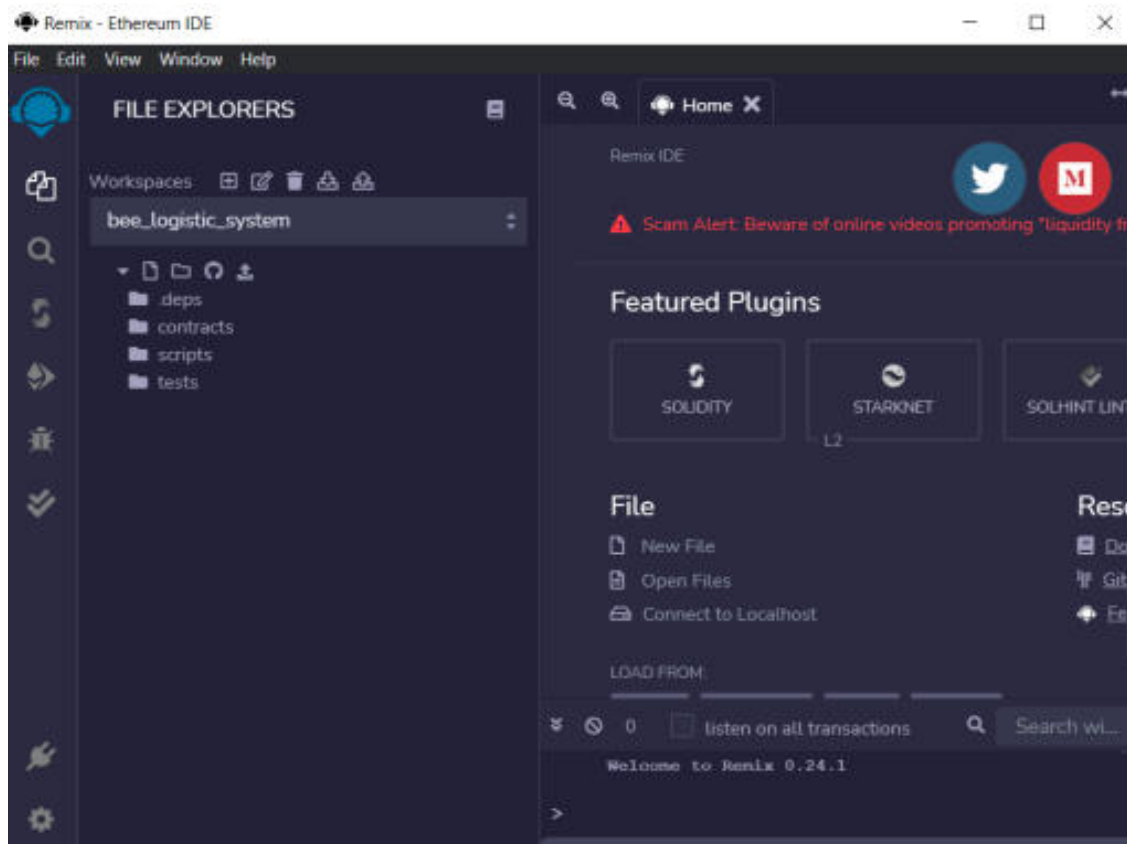
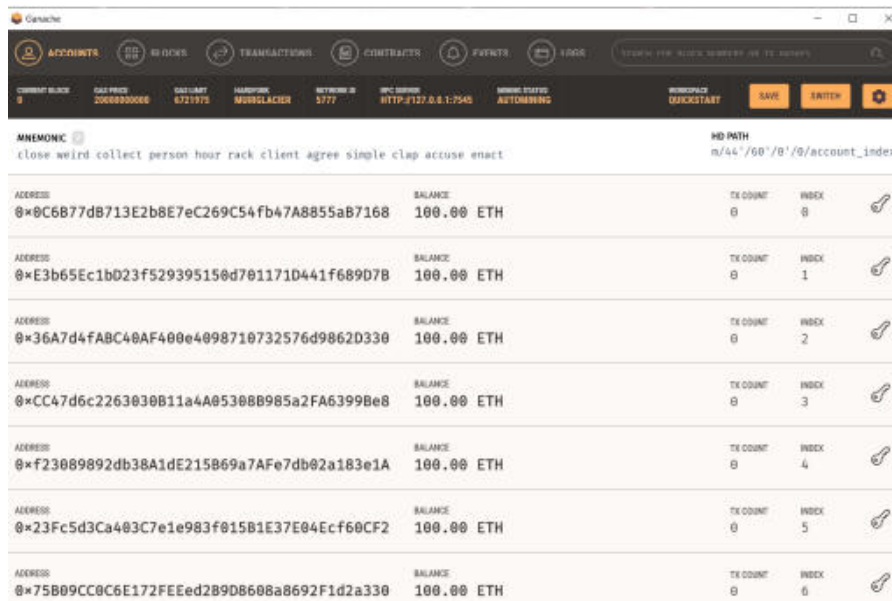


Рис. 2.2. – Remix IDE desktop

Джерело:[25]

Для локального розгортання створеного смарт-контракту використаємо програмне забезпечення Ganache.

Ganache - це інструмент для створення особистого блокчейну (рисунок 2.3), який призначений для швидкого розроблення розподілених додатків на платформах Ethereum і Corda. Ganache можна використовувати на всіх етапах розробки, що дозволяє розробникам створювати, розгортати та тестувати свої додатки в безпечному та детермінованому середовищі [19].



ADDRESS	BALANCE	TX COUNT	INDEX
0x0C6B77dB713E2b8E7eC269C54Fb47A8855aB7168	100.00 ETH	0	0
0xE3b65Ec1bD23f529395150d701171D441f689D7B	100.00 ETH	0	1
0x36A7d4fABC40AF400e4098710732576d9862D330	100.00 ETH	0	2
0xCC47d6c2263030B11a4A05308B985a2FA6399Be8	100.00 ETH	0	3
0xF23089892db38A1dE215869a7AFe7db02a183e1A	100.00 ETH	0	4
0x23Fc5d3Ca403C7e1e983f015B1E37E04EcF60CF2	100.00 ETH	0	5
0x75B09CC0C6E172FEEed289D8608a8692F1d2a330	100.00 ETH	0	6

Рис. 2.3. Ganache створений локальний блокчейн з акаунтами

Джерело:[19]

Ganache доступний у двох варіантах: UI та CLI. Ganache UI – це програма з графічним інтерфейсом, яка підтримує технології Ethereum і Corda (див. Додаток Д). Інший варіант – це інструмент командного рядка ganache-cli (раніше відомий як TestRPC), який призначений для розробки на платформі Ethereum [19]. Для розгортання смарт-контракту ми обираємо використання версії Ganache з графічним інтерфейсом.

2.2. Аналіз реалізації блокчейн-платформи для смарт-контрактів

За останні роки ринок смарт-контрактів пережив безпрецедентний сплеск, революціонізуючи спосіб укладання угод і операцій між різними промисловості. З появою технології блокчейн з'явилися смарт-контракти безпечна, прозора та ефективна альтернатива традиційним паперовим договорам. Це революційна технологія знайшла застосування у фінансах, управлінні ланцюгами поставок, реальному нерухомість та багато інших секторів. Компанії все частіше використовують розумні контракти автоматизувати процеси, усунути посередників і скоротити витрати. Ринок кишить з інноваційними стартапами та визнаними гравцями, кожен з яких пропонує рішення для смарт-контрактів прагнучи зайняти нішу в цій галузі, що розвивається. Оскільки ринок продовжує зрілого, ми можемо очікувати збільшення впровадження смарт-контрактів, що відкриває шлях для а децентралізоване та безнадійне майбутнє[15].

Одним із ключових факторів зростання цього ринку є все більше визнання потенціалу переваги смарт-контрактів. Ці переваги включають покращену прозорість, підвищена безпека та спрощені операції. В результаті обидва підприємства і уряди активно вивчають можливість впровадження смарт-контрактів для оптимізації процесів і забезпечення відповідності. Крім того, на ринку спостерігається поява сумісні платформи смарт-контрактів, які забезпечують повну інтеграцію з існуючими систем і мереж. Ця сумісність має вирішальне значення для широкого впровадження дає змогу створювати складні міжланцюгові програми смарт-контрактів, які можуть революціонізувати такі галузі, як фінанси, охорона здоров'я та логістика[41].

У 2022 році розмір ринку смарт-контрактів оцінювався в 190,34 мільйона доларів США та, як очікується, досягне 1077,7 мільйона доларів США до 2030 року та зросте на 24,2% за прогнозований період 2023–2030 років(рис.2.4).

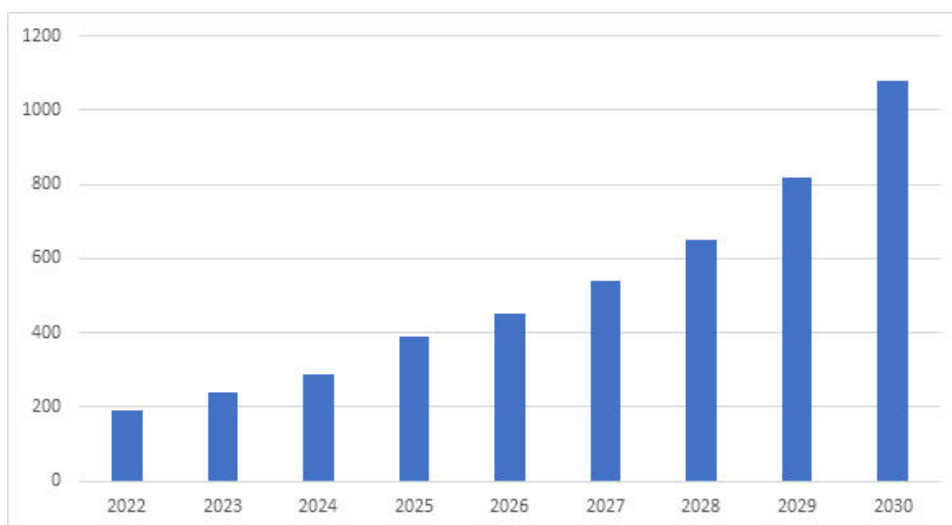


Рис. 2.4. Розмір ринку смарт-контрактів 2023-2030 (дол. США)

Джерело: розроблено автором на основі даних[41]

Грошові дочірні компанії, витрати на страхування, регулювання власності, розірвання контрактів, авторизація кредиту, грошове адміністрування, механізми краудфандингу та законні цикли є прикладами блискучого використання політики. Оскільки смарт-контракти включають кілька основних характеристик, включаючи незалежність, децентралізацію та незалежність. Смарт-контракти можуть допомогти вирішити питання як мінімум між двома людьми, а також між колегами. У виробничій мережі Рада директорів використовує чудові угоди, оскільки вони враховують такі свободи власності, коли речі проходять через структуру. Вони також можуть бути використані для отримання захищених даних. Люди також можуть претендувати на свій передовий характер, який включає комп'ютеризовані ресурси та інформацію, за допомогою блискучих угод. зберігаються на Blockchain, пошук фреймворку надзвичайно складний у світлі того факту, що скорочення всієї організації вимагатиме величезної потужності обробки.

24 травня 2022 року організація EY випустила для громадськості другу ітерацію інструменту EY Blockchain Analyzer: Smart Contract & Token Review. Тепер користувачі можуть створювати індивідуальні процедури тестування та симулювати транзакції в блокчейні Ethereum перед їх виконанням, використовуючи дані мережі в реальному часі в останній версії. Нова версія розширює свої можливості за межі звичайних валют, таких як ERC-20, і дозволяє розробникам і командам тестування співпрацювати[41].

Ринок розділений на Bitcoin Ethereum, NXT і Sidechains на основі платформи

Blockchain. У 2021 році Ethereum мав найбільшу частку ринку, і очікується, що він буде розвиватися з довгостроковим позитивним складним річним темпом зростання (CAGR) протягом прогнозованого періоду. У 2021 році біткойн був другим за величиною ринком, і очікується, що він зростатиме з позитивним CAGR протягом прогнозованого періоду.

Ринок розділений на Ethereum Namecoin, Ripple, Rootstock (RSK) та інші на основі технології. У 2021 році Ethereum мав найбільшу частку ринку, і очікується, що він буде розвиватися з довгостроковим позитивним CAGR протягом прогнозованого періоду. У 2021 році другим за величиною ринком були підщепи (RSK), які, за прогнозами, зростуть із позитивним CAGR протягом прогнозованого періоду.

Залежно від кінцевого користувача ринок поділяється на автомобільний, державний, управління ланцюгами поставок та інші. У 2021 році держава займала найвищу частку ринку, і очікується, що вона буде розвиватися з довгостроковим позитивним CAGR протягом усього прогнозованого періоду. У 2021 році управління ланцюгами поставок було другим за величиною ринком із прогнозованим позитивним CAGR протягом прогнозованого періоду.

Світовий ринок смарт-контрактів поділений на п'ять регіонів: Північна Америка, Європа, Азіатсько-Тихоокеанський регіон, Південна Америка, Близький Схід і Африка. Через високий рівень прийняття нових товарів і технологій у регіоні Північна Америка, ймовірно, буде лідером на ринку смарт-контрактів протягом прогнозованого періоду. Використання смарт-контрактів у Північній Америці також вище, ніж у середньому по всьому світу в інших галузях, окрім BFSI.

2.3. Дослідження практичного впливу технології смарт-контрактів на блокчейн

Технологія блокчейн із кожним роком поширюється і набуває стратегічного значення, охоплюючи безліч галузей – від фінансових інститутів до сфери охорони здоров'я. Вартість активів у світі блокчейну становить понад 1,2 трильйона доларів. Ця сума співставна з річним валовим внутрішнім продуктом такої країни, як Іспанія. Загальний багаторічний тренд цієї вартості – до збільшення, незважаючи на сезонні сплески та падіння. У світлі цього, підтримання превентивних заходів стає більш пріоритетним

завданням, ніж будь-коли.

За даними компанії Dune Analytics, кількість нових смарт-контрактів у мережі Ефіріуму в березні досягла 1 971 632. Таким чином, зростання склало 75% порівняно з показниками лютого.

Аналітики зазначили, що за останні 12 місяців це було рекордне збільшення числа нових смарт-контрактів – середньомісячний приріст за рік становить лише 670 тисяч(рис. 2.5).

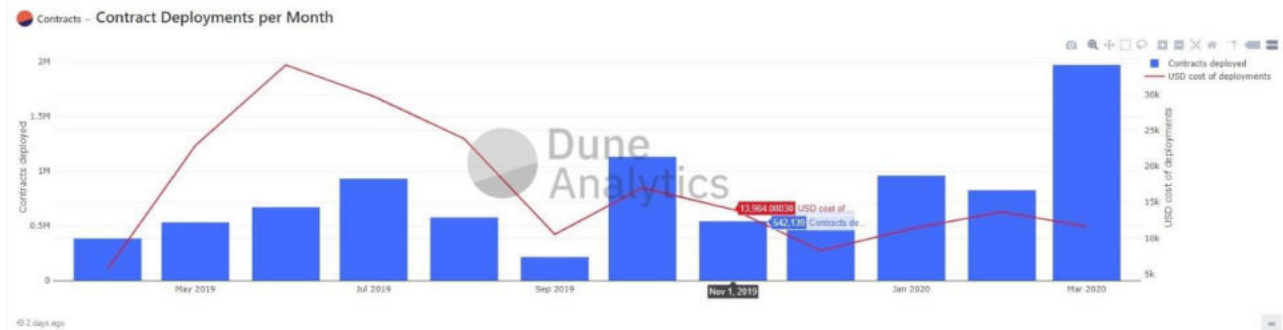


Рис.2.5. Річний аналіз збільшення нових смарт-контрактів

Джерело: [14]

Зростання числа нових смарт-контрактів збіглося зі зниженням вартості розміщення. Зараз у середньому розробникам потрібно близько \$11600 для того, щоб випустити свій смарт-контракт. Зниження вартості стало ознакою те, що прийняття Ефіріуму стає дедалі ширшим, особливо у порозі застосування Ефіриума 2.0(додаток Ж).

Цікаво, що незважаючи на запуск значної кількості смарт-контрактів, у мережі Ефіріуму не було зафіксовано помітне зростання кількості транзакцій. Швидше за все, більшість смарт-контрактів або ще не використовуються, або поки що не стали популярними серед користувачів. Аналітики вважають, що Ефіріум стає все популярнішим, а запуск Ефіріуму 2.0 може допомогти зростанню курсу ЕТН. На думку партнера MetaCartel Ventures DAO Адама Кокрана (Adam Cochran), запуск проекту може призвести до «великого економічного зрушення» у суспільстві та популяризації проектів децентралізованого фінансування (DeFi).

Крах Terra LUNA/UST, Celsius, Voyager Digital, Three Arrows Capital і останньої саги про FTX, зробили 2022 рік складним та нестабільним для багатьох представників галузі[11].

За даними CoinMarketCap, загальна капіталізація крипторинку станом на кінець листопада зменшилася до 821 мільярда доларів США, у той час як злочинність у ланцюгу

збільшилася у своїй частоті та витонченості по мірі розвитку галузі. Станом на 22 листопада 2022 року, було зафіксовано 290 інцидентів з безпекою із загальними збитками понад 3,6 мільярда доларів США, як задокументовано SlowMist Hacked (архів інцидентів, пов'язаних із блокчейном)(рис.2.6).

[SlowMist Hacked Statistical]:

Total 2022 hack event(s) 290 ;

The total amount of money lost by blockchain hackers is about \$ 3,631,139,366.15 ;

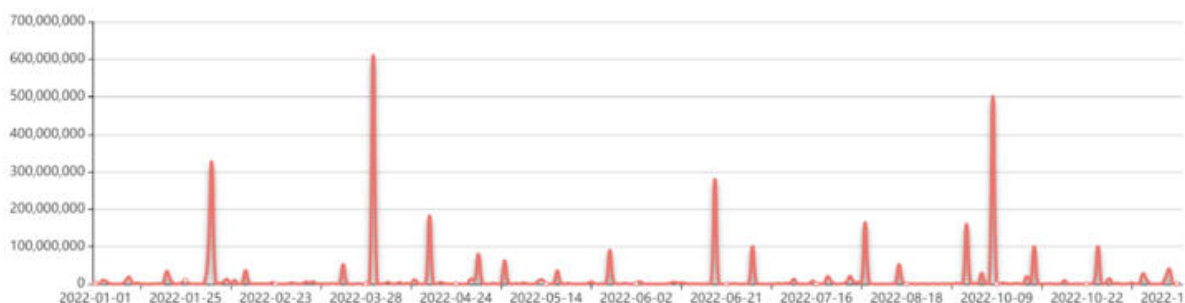


Рис. 2.6. Загальна капіталізація крипторинку

Джерело: [11]

Правила були основою поточної дискусії про те, як зменшити криптозлочинність. Ефективне регулювання ринку, захист роздрібних користувачів, забезпечення стійкості до деяких системних викликів — це одні з найактуальніших питань, які потребують вирішення.

З іншого боку, цей рік також наблизив регулюючі органи та широку громадськість до крипто та блокчейн технологій. У результаті політика, пов'язана із крипто також стає більш прозорою, що зрештою сприятиме загальному зростанню індустрії блокчейна.

Лише у жовтні 2022 року було зафіксовано понад 20 атак на пов'язані з Web 3 проєкти та трейдинг платформи. Більшість із них були атаками та зловмисним використанням через недоліки безпеки у коді проєктів. Було запущено багато кросчейн мостів із нульовою комісією та швидкими транзакціями для швидкого залучення користувачів та проєктів до екосистеми — усе це зроблено за рахунок ігнорування безпеки як найважливішого питання. Кросчейн мости мають високий рівень ліквідності, але незначну децентралізацію, і більшість повноважень зосереджено у мультипідписних гаманцях: коли хакери отримують доступ до підписів, вони здійснюють повний контроль. Окрім того, перевірки безпеки кросчейн мостів є нечастими та спільноти надають небагато з

точки зору моніторингу безпеки. У результаті, кросчейн мости часто стають популярною мішенню для хакерів. Зі збільшенням кількості пов'язаних з безпекою інцидентів ми очікуємо, що більше проєктів визнають цінність аудиту в майбутньому. Ґрунтуючись на глибоких знаннях і досвіді, накопичених SlowMist у сфері безпеки блокчейну, ми вважаємо, що для проєктів дуже важливо проходити всебічний аудит безпеки фронт/бек-енду (front/back-end) та контракту в комбінації з іншими методами, такими як використання винагород за помилки для покращення безпеки проєкту протягом його поточної роботи та розвитку[11].

У 2021 році почалося розширення кількох проєктів L1 разом із Solana, Avalanche та іншими, а у 2022 році, ця тенденція продовжилася, коли Aptos та Sui привернули значне фінансування інвесторів і увагу ЗМІ. Незважаючи на те, що Ethereum Merge від PoW до PoS не принесло суттєвого покращення вартості транзакцій або швидкості, ця тема масштабованості буде продовжуватися серед інших L1. Також були розроблені різні проєкти другого рівня (Layer 2) для зменшення навантаження на мережевий рівень та підвищення його ефективності. Масштабовані rollup платформи, такі як Arbitrum, продовжуватимуть залучати інтерес як середнього по тривалості, так і довгострокового рішення проблеми перевантаження мережі Ethereum.

Невирішена трилема блокчейна — безпека, масштабованість та швидкість — не може бути досягнута одночасно, а це означає, що тепер існує кілька L1, які задовольняють різні вимоги користувачів. Отже, ми очікуємо подальшого розвитку кросчейн рішень, де EVM та не EVM сумісні ланцюги з'єднані для досягнення взаємодії та сумісності. Ці розробки мають дати спільноті можливість знайти баланс між швидким кросчейн мостом, достатньою ліквідністю та безпечною взаємодією з користувачем[11].

Важливість відстеження ончейн злочинів також є більш помітною. Ончейн дані можуть принести величезну користь аналітиці блокчейна та розслідуванням боротьби з відмиванням грошей, і ми вже починаємо бачити безліч ончейн платформ та інструментів для відстеження й аналізу. Завдяки агрегації даних цих інструментів відстеження, користувачі можуть виявити таку інформацію, як місцезнаходження своїх коштів та визначити, чи пов'язані їхні активи з викраденими коштами. Найближчим часом, інструменти відстеження продовжуватимуть розвиватися та додаватимуть більше

можливостей для розслідувань щодо відмивання грошей.

Навіть з усіма різноманітними продуктами некастодіальних гаманців (гаманців із самостійним зберіганням) доступними зараз, втрата приватних ключів та початкових фраз продовжує залишатися дуже поширеною причиною багатьох випадків крадіжок криптовалют. Для вирішення цієї проблеми, резервні копії, такі як багатостороннє обчислення (MPC), отримали місце у центрі уваги протягом останніх місяців як життєздатне рішення проблеми одноточкового резервного копіювання.

За допомогою технології MPC (Multi-Party Computation), коли приватний ключ спочатку генерується, його можна розділити на кілька шардів і розподілити серед групи осіб. Цей спеціальний метод дозволяє відновлювати оригінальний закритий ключ, якщо це необхідно. Очікується, що найближчим часом з'явиться рішення з відкритим вихідним кодом, яке відповідатиме галузевим стандартам у цій області.

У 2022 році DAO (Децентралізовані автономні організації) стали однією з найгарячіших тем у криптосфері, незважаючи на те, що більшість організацій DAO та інструменти для їх створення ексклюзивні для екосистеми Ethereum і менш розвинені на інших блокчейн-платформах (L1). Те, як DAO зможуть вирішити проблеми стимулювання, реалізувати кросчейн управління активами та можливості взаємодії, а також розширити варіанти використання, стане ключовим аспектом на наступному етапі їхнього розвитку.

Раніше основна кількість транзакцій NFT оброблялася в екосистемі Ethereum. Проте можливо, що у найближчі роки транзакції NFT будуть все частіше проводитися в різних блокчейн-мережах. Таким чином, проекти, які полегшують такі транзакції, матимуть великий попит. Геймінг-індустрія стає перспективним новим напрямком для NFT додатків, і в 2023 році очікується зростання кількості нових гравців і розробників ігор, пов'язаних з NFT.

Аналізуючи звіти, такі як SlowMist про безпеку блокчейну та протидію відмиванню грошей (AML), Chainalysis про криптозлочинність та інші аналітичні звіти, можна відзначити, що у першій половині 2022 року в блокчейні сталося 185 значущих інцидентів безпеки. Ці інциденти призвели до збитків у розмірі до 920 мільйонів доларів[13]. Важливо відзначити, що цей показник нижчий на 54% порівняно з першою половиною 2022 року, коли збитки складала приблизно 2 мільярди доларів (рис. 2.7).

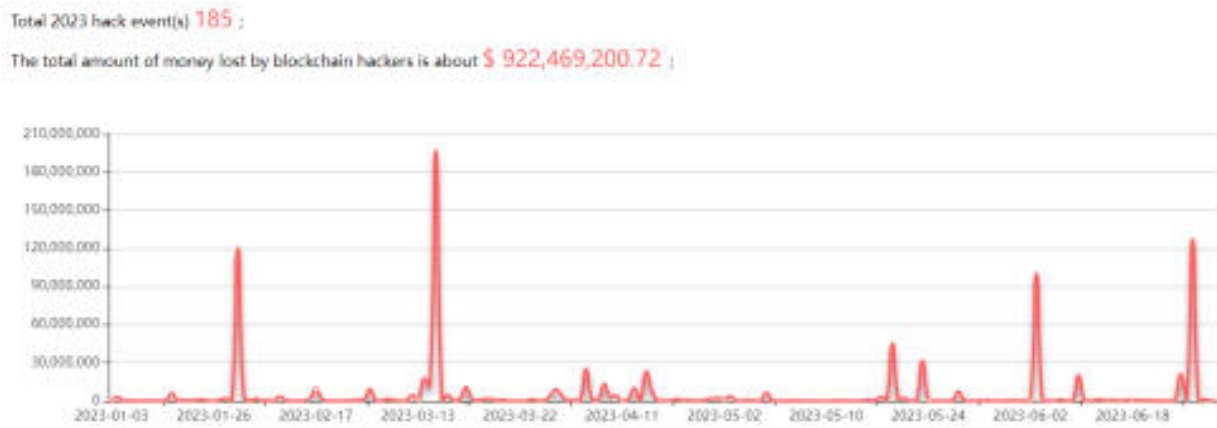


Рис. 2.8. Аналіз збитковості блокчейну у 2023 році

Джерело: [13]

Сектори DeFi, NFT і Cross-chain Bridge зазнали найбільших втрат – було зафіксовано 131 інцидент і збитки на суму близько 487 мільйонів доларів. Незважаючи на меншу кількість інцидентів на торгових платформах, у публічній мережі та криптогаманцях, вони також понесли значні фінансові втрати.

Платформи криптоміксингу, такі як Tornado Cash і eXch, стали об'єктом підвищеної уваги користувачів і широко використовуються для сумнівних транзакцій.

Фішингові афери, організовані групами, такими як Pink Drainer, Vemon Drainer, Monkey Drainer, Pussy Drainer і Inferno Drainer, продовжують становити серйозну загрозу для блокчейн-спільноти[14].

Атаки програм-вимагачів активно розвиваються, і злочинці змогли виманити майже 450 мільйонів доларів. Це число перевищує попередній рік більш ніж в півтора рази, що свідчить про агресивніші тактики і амбіційні цілі злочинців (рис. 2.9).

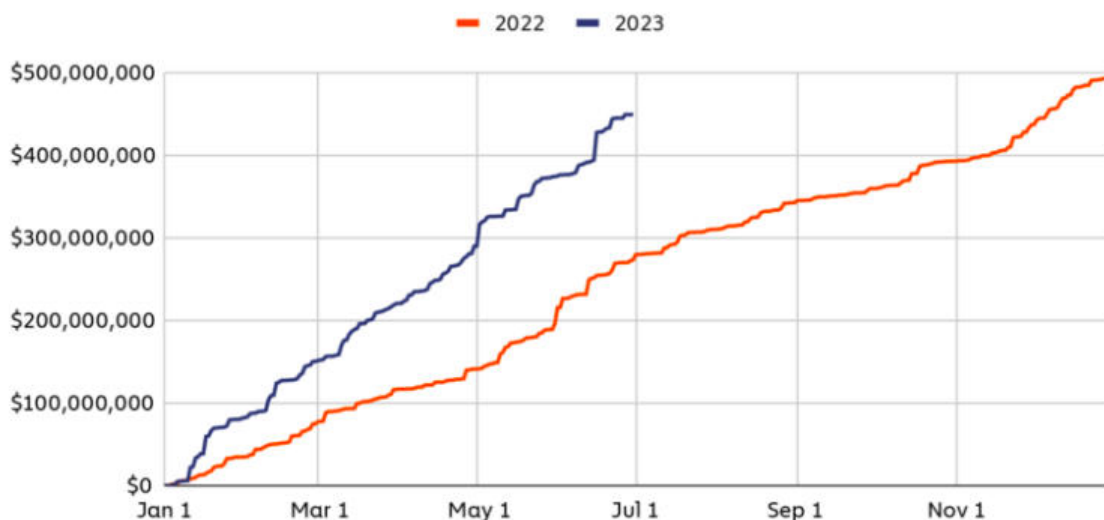


Рис. 2.9. Сукупний річний дохід від програм-вимагачів 2022 та 2023 роки

Джерело: [14]

Шахрайство та зломи залишаються одними з найприбутковіших видів криптозлочинності, і збиток від шахрайських схем з підробленою особистістю збільшився майже на 50% порівняно з попереднім роком. Аферисти, які видають себе за представників влади, продовжують завдавати значні фінансові збитки своїм жертвам.

Важливою особливістю поточного ландшафту загроз є посилення геополітичних мотивів у криптозлочинності. Групи з Північної Кореї залишаються інкубатором хакерської активності та становлять значну загрозу в кіберзлочинному ландшафті[14].

Хакерські угруповання, пов'язані з Північною Кореєю, дедалі активніше використовують російські біржі, відомі відмиванням незаконних криптоактивів. У цьому році обсяг викрадених криптовалют, пов'язаних із північнокорейськими хакерськими угрупованнями, такими як Lazarus Group, перевищив 340 мільйонів доларів.

Північнокорейські угруповання відповідають за майже 30% усіх викрадених криптовалют унаслідок хакерських атак у 2023 році. Навіть при зниженні кількості інцидентів, аналітики Chainalysis попереджають, що це не обов'язково свідчить про загальне поліпшення криптовалютної безпеки або зниження рівня кіберзлочинності.

У другій половині поточного року кількість криптовалютних зломів збільшилася майже на 60% порівняно з аналогічним періодом минулого року, що призвело до втрати майже 686 мільйонів доларів. Особливо важливим є інцидент, пов'язаний зі зломом Mixin, який стався 25 вересня 2023 року, і внаслідок його зловмисники викрали близько 200 мільйонів доларів[13].

У першій половині 2023 року у 10 інцидентах вкрадені кошти були успішно відновлені. З вкрадених 232 мільйонів доларів значна сума, а саме 219 мільйонів доларів, була повернута. Цей тренд підкреслює важливість надійних стратегій безпеки, співпраці в галузі розслідувань інцидентів, ефективних переговорів і винагород.

Аналітики Chainalysis також відзначають локальні позитивні зміни у галузі криптотранзакцій. У середині 2023 року спостерігається зниження обсягу незаконних транзакцій на 65% порівняно з попереднім роком (рис. 2.10).

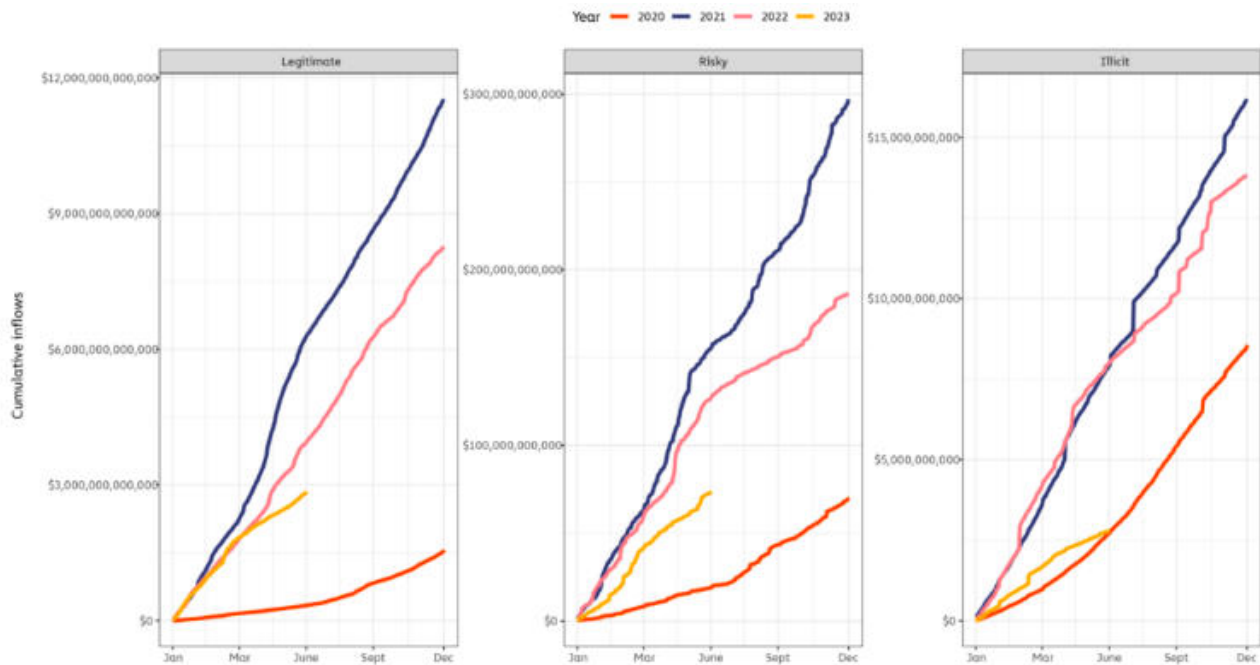


Рис.2.10. Сукупний приплив до законних ризикованих і незаконних послуг за роками (приблизно червень 2023 р.)

Джерело:[14]

Незважаючи на тимчасове зниження активності криптозлочинності через сезонне зменшення активності блокчейнів і посилення заходів їхньої безпеки, загальна тенденція втрат від інцидентів безпеки залишається висхідною. Еволюція блокчейн-екосистеми з кожним роком породжує нові виклики і змушує нас дедалі серйозніше думати про питання безпеки. Це вказує на необхідність постійного вдосконалення заходів забезпечення безпеки та реагування на нові виклики у сфері криптовалют і блокчейн-технологій[2].

Одне ми знаємо напевно: блокчейн стане рушійною силою багатьох розробок у всьому світі. З нетерпінням чекаємо на світ сумісного блокчейну, світ розширеної потужності з мультічейн балансом, зрілою технологією та екологічно стабільною екосистемою.

РОЗДІЛ 3.

ОСНОВНІ ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ СМАРТ-КОНТРАКТІВ

З моменту появи технології блокчейн смарт-контракти охопили цифровий світ. Розумні контракти виконуються автоматично та мають потенціал для збільшення власного капіталу завдяки використанню однорангової мережі для зберігання інформації про контракти та ефективнішого використання її, ніж традиційні методи. У цій системі не може бути жодних коригувань чи підкupu, лише код. Високоякісні смарт-контракти також мають потенціал для зниження транзакційних витрат шляхом усунення непотрібних посередників із розробки та виконання контрактів. Однак, поряд із усім потенціалом, існують значні проблеми зі смарт-контрактами.

Індустрії починають розглядати смарт-контракти як новий інструмент для підвищення точності та зниження комісії за багато своїх угод. Логістика та транспортування, страхування, благодійність, сільське господарство, охорона здоров'я, енергетика та фінансовий сектор адаптуються до розумних контрактів. У сільському господарстві їх можна використовувати для відстеження продуктів від ферми до столу. У логістиці розумне виконання контрактів допомагає керувати ланцюгом поставок[2].

Але розумні контракти далеко не повсюдні. Від тонкощів кодування до обміну матеріальними благами, потрібно вирішити багато проблем, перш ніж ми зможемо очікувати розвитку смарт-контракту в універсальному масштабі. Давайте розглянемо основні проблеми, з якими вони стикаються, і спробуємо знайти рішення.

1. Безпека та конфіденційність

Безпека смарт-контрактів була основною темою досліджень і розробок принаймні після сумнозвісного злому 2016 року, коли хакер, який скористався вразливістю в коді, витягнув з The DAO ефір, який на той час вартував близько 60 мільйонів доларів.

Розумні контракти використовують переваги технології розподіленої книги на блокчейнах. За своєю природою вони є відкритими та доступними для читання. Питання, яке постає перед розробниками та дослідниками смарт-контрактів: як підвищити безпеку смарт-контрактів без збільшення витрат?

Використовуючи однорангову мережу, контракти відкриті для таких загроз, як помилки впорядкування подій і помилки повторного входу, коли хакери можуть вводити шкідливі дані для бажаного результату. Як правило, для отримання прибутку[29].

Існують різні можливості для контролю безпеки, і нові інноваційні технології програмного забезпечення продовжують розвиватися. Серед останніх технічних досягнень:

Проект блокчейну Hyperledger розробив приватні замкнуті середовища для різних галузей. Його елементи керування конфіденційністю надаватимуть доступ лише до тих даних, які ви хочете оприлюднити, і лише між «дозволеними» учасниками мережі.

Збільшення використання криптографії може зробити дані публічними, але доступними для читання лише тим, хто залучений. Однак використання програмного забезпечення для криптографії на смарт-контракті коштує дорого, що частково підриває привабливість смарт-контрактів.

Ще одна альтернатива — створення гібридних рішень для зберігання даних. Такі розумні контракти використовують деякі зовнішні сховища даних у поєднанні з вибіркоким використанням хмарних обчислень замість того, щоб повністю покладатися на блокчейн. Це також може зменшити витрати. Блокчейни самі по собі можуть бути дорогими в обслуговуванні, а їх вибіркоче використання може підвищити безпеку та економічну ефективність.

Пакети SDK Hedera надають окремим особам і компаніям інструменти, необхідні для вирішення проблем безпеки та відповідності під час створення надійних систем. Наприклад, розробники фінансових додатків можуть інтегрувати KYC (знай свого клієнта) і AML (захист від відмивання грошей) у свої системи без залучення централізованої організації.

2. Правові виклики

Розумні контракти мають потенціал для прискорення транскордонних транзакцій фінансів, товарів і послуг, усунувши посередників. Однак смарт-контракти повинні відповідати законам різних країн, і навіть тоді може бути важко гарантувати, що вони будуть дотримуватись у різних країнах. Уряди зрештою також можуть захотіти регулювати ці транзакції та угоди, перевернувши мету використання однорангових мереж, повернувшись до третьої сторони, яка перевіряє процес.

Інші блокпости заважають використанню смарт-контрактів. Ще однією ключовою

особливістю смарт-контрактів є їх незмінність. Після укладення угоди та закріплення коду контракту не існує простого способу скасувати або змінити його. Отже, якщо відбудуться зміни в законодавстві або дві сторони досягнуть нової взаємної згоди, що тоді? Ймовірно, смарт-контракт доведеться перервати та створити новий. А це може коштувати дорого.

Потім є питання даних. Для простих юридичних контрактів, таких як свідоцтва про шлюб, оцифрувати легко. Для галузей із кількісними даними, таких як фінанси чи сільське господарство, розумні контракти можна кодифікувати відносно просто. Але не всі контракти використовують кількісні показники, тож як їх можна обчислити?

Існують також деякі основні міжнародні закони, які перешкоджають більш широкому легальному використанню розумних контрактів. Наприклад, Європейський Союз погодився з Європейським загальним регламентом захисту даних, який гарантує, що громадяни мають «право бути забутих». Вони можуть вимагати видалення цифрової інформації про них. Але якщо громадянин пов'язаний цифровою юридичною угодою, про нього, можливо, не можна забувати[30].

Крім того, для того, щоб смарт-контракти були юридично освячені, можливо, громадськості потрібно отримати більше розуміння кодування. Чи доведеться суддям вивчати мову розумних контрактів, щоб вести цифрові справи?

3. Довіра до оракулів

«Оракули» — це джерела даних, на які покладаються смарт-контракти, щоб перевірити, чи виконуються деякі критерії контракту. Вони можуть бути найслабшою ланкою в маніпулюванні розумним контрактом. Якщо будь-який вузол блокчейну контракту зламаний, він може зареєструвати фальсифіковані дані, які потім стають незмінними в розподіленій книзі, потенційно запускаючи автоматичне виконання результату смарт-контракту[38].

У довгостроковій перспективі додатків смарт-контрактів потрібно буде створити політики для врахування помилкових даних у обмеженому робочому середовищі, яке містить оракули. Проблеми можуть виникати через збої в роботі обладнання, помилки хакерів або ситуації, коли середовище заважає оракулу збирати або ділитися даними. Або ж часом компанія-оракул може просто припинити діяльність і припинити збирати та поширювати інформацію.

4. Проблеми зручності використання

Через дизайн смарт-контрактів і їх дуже специфічне застосування розробка смарт-контрактів вимагає спеціальних навичок розробки програмного забезпечення.

На відміну від традиційної розробки програмного забезпечення, смарт-контракти вимагають від розробників знання бізнесу та розуміння нетрадиційних мов програмування, насамперед Solidity. Вони також повинні розуміти формальні методи криптографії та мереж.

Вкрай важливо, щоб смарт-контракти були правильно закодовані з міркувань безпеки. Деякі розробники запропонували нові мови розумних контрактів, тоді як інші працюють над створенням програмного забезпечення, яке може «перевіряти факти» коду, щоб переконатися, що він виконує те, що він повинен робити. Навіть для функціонального коду смарт-контракту програмне забезпечення не читатиме помилки чи вразливості. Отже, міцні технічні знання та правильне кодування з самого початку є найкращою гарантією від атак.

5. Проблеми впливу

Нарешті, є проблема масштабу. Зараз Visa може обробляти близько 24 000 транзакцій щосекунди. Ethereum, найбільший блокчейн для смарт-контрактів, може обробляти лише 14 транзакцій на секунду. Щоб підвищити вплив і ефективність смарт-контрактів у нашому суспільстві, необхідно прискорити швидкість обміну інформацією в блокчейні, підвищити безпеку, а також збільшити доступність для програмістів і громадськості.

ВИСНОВКИ

Отже, дослідивши таку значиму тему для нашого суспільства, а саме: технології смарт-контрактів і їх роль в блокчейн, можемо зробити такі висновки:

1. Блокчейн представляє собою революційну технологію, яка змінює парадигму зберігання та обміну даними. Його сутність полягає в створенні розподіленої, недоступної для змін бази даних, де кожен блок інформації забезпечується шифруванням та підписом, гарантуючи надійність і невідмінність даних. Характеристики блокчейну включають децентралізацію, прозорість, невідмінність, автентичність і безпеку. Ця технологія знаходить застосування в різних галузях, від фінансів та управління постачанням до охорони здоров'я та голосування, вирішуючи проблеми централізованих систем. З блокчейном сполучаються високі стандарти безпеки та децентралізованість, визначаючи його значущість в епоху цифрових інновацій.

Смарт-контракти стали важливою складовою сучасних блокчейн-технологій, розширюючи можливості та функціональність цих систем. Поняття смарт-контрактів базується на ідеї автоматизації та автономності виконання угод, вбудованих в коді блокчейн-мережі.

Різновиди смарт-контрактів включають у себе прості та складні. Прості смарт-контракти використовуються для базових функцій та угод, тоді як складні розширюють можливості, дозволяючи взаємодіяти з іншими контрактами та виконувати більш складні умови.

Смарт-контракти можуть бути використані в різних галузях, включаючи фінанси, логістику, медицину та багато інших. Вони дозволяють автоматизувати процеси, зменшити витрати та забезпечити більшу прозорість та безпеку.

Однак разом з усією своєю перевагою, смарт-контракти також стикаються з викликами, такими як безпека програмного забезпечення та невизначеність правового статусу. Важливо продовжувати дослідження та розвиток цієї технології, забезпечуючи її вдосконалення та широке впровадження в різні сфери діяльності.

2. Сучасні тенденції розробки смарт-контрактів визначаються стрімким розвитком блокчейн-індустрії та зростанням інтересу до децентралізованих фінансів (DeFi) і

токенізації активів. Розширення функціональності мови програмування Solidity, вдосконалення безпеки та стандартизація смарт-контрактів відіграють важливу роль у розвитку цієї технології. Крім того, виникають нові підходи, такі як використання конфіденційних смарт-контрактів та розвиток крос-ланцюгових мостів для покращення інтеграції між блокчейнами. Наслідуючи ці тенденції, розробники продовжують вдосконалювати інструменти та методології для надійного та безпечного розгортання смарт-контрактів, що відкриває шлях до нових можливостей у світі децентралізованих технологій.

3. Аналіз реалізації блокчейн-платформи для смарт-контрактів свідчить про важливість та активний розвиток цієї технології в різних галузях. Використання мови програмування Solidity, модифікаторів та подій у смарт-контрактах відкриває можливості для створення надійних та ефективних децентралізованих додатків. Розгортання смарт-контрактів за допомогою середовища розробки Remix IDE та локального тестування за допомогою Ganache сприяє прискоренню циклу розробки. Важливим аспектом залишається також питання безпеки, зокрема в контексті використання приватних ключів та заходів з відмивання грошей. Загальною тенденцією в сфері реалізації блокчейн-платформ для смарт-контрактів є постійне вдосконалення та адаптація до зростаючих потреб ринку децентралізованих технологій.

4. Дослідження практичного впливу технології смарт-контрактів на блокчейн вказує на значущий розвиток та впровадження цієї технології в різні галузі. Смарт-контракти забезпечують автоматизацію та безпеку укладання угод, зменшуючи ризики та вартість транзакцій. Їхня реалізація викликає активний інтерес у сферах децентралізованих фінансів, нерухомості та галузей, де необхідна довіра та прозорість. Зростаюча популярність смарт-контрактів свідчить про їхню ключову роль у розвитку блокчейн-екосистеми та перетворенні традиційних моделей бізнесу.

5. Проблеми програмної реалізації смарт-контрактів є важливим викликом для широкого впровадження цієї технології. Вони включають у себе питання безпеки, які можуть призвести до вразливостей та втрат коштів, а також складнощі в розробці, тестуванні та аудиті смарт-контрактів. Низька масштабованість та вартість транзакцій також становлять виклики для розвитку децентралізованих додатків. Розв'язання цих проблем вимагає спільних зусиль розробників, безпекових експертів та галузевих лідерів для

створення стандартів та інфраструктури, що сприятимуть стабільному та безпечному функціонуванню смарт-контрактів.

Для вирішення проблем програмної реалізації смарт-контрактів необхідно акцентувати увагу на підвищенні безпеки через аудит та тестування, навчання розробників, стандартизацію та вдосконалення протоколів блокчейну для забезпечення масштабованості та швидкодії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Блокчейн, ICO і смарт-контракти: хто і як робить "легкі гроші" на незрозумілих словах. URL: <https://www.epravda.com.ua/publications/2018/07/16/638722/>
2. Прогноз проблем безпеки для технологій блокчейн у 2024 році. URL: <https://www.h-x.technology.ua/blog-ua/top-blockchain-security-threats-in-2024-ua>
3. Смарт-контракти та платформи для їх реалізації. URL: <https://www.cryptohuckers.club/2019/04/smart-kontrakty-ta-platformy-dlya-ih-realizacii.html>
4. Смарт контракт: розумний код рулить. URL: <https://nachasi.com/crypto/2020/12/08/smart-kontrakt/>
5. Термінал у смартфоні – не межа. Які фінтех-тренди очікуються в Україні найближчим часом. URL: <https://finance.liga.net/ua/all/opinion/terminal-v-smartfone-ne-predel-kakie-finteh-trendy-ojidayutsya-v-ukraine>
6. Технологія блокчейн та її роль в екосистемі Bitcoin. URL: https://lb.ua/economics/2023/04/13/550425_tehnologiya_blokcheyn_ii_rol.html
7. Тренди блокчейну 2023. URL: <https://www.eternitylaw.com/ua/novyny/blockchain-trends-2023/>
8. Що таке смарт-контракти і які принципи їх роботи?. URL: <https://lexinform.com.ua/yuridychna-praktyka/shho-take-smart-kontrakty-i-yaki-pryntsyipy-yih-roboty/>
9. Що таке блокчейн і як він працює?. URL: <https://academy.binance.com/uk/articles/what-is-blockchain-and-how-does-it-work>
10. Що таке блокчейн? Пояснюємо простими словами. URL: <https://blog.whitebit.com/uk/what-is-blockchain-technology/>
11. 2023 CMC Crypto Playbook: тенденції розвитку блокчейну - стаття від аудитора смарт-контрактів SlowMist. URL: <https://coinmarketcap.com/academy/uk/article/2023-cmc-crypto-playbook-blockchain-development-trends-by-smart-contract-auditor-slowmist>
12. Blockchain facts: what is it^ how it works^ and how it can be used. URL: <https://www.investopedia.com/terms/b/blockchain.asp#citation-33>

13. Blockchain security and AML Report. URL: [https://www.slowmist.com/report/first-half-of-the-2023-report\(EN\).pdf](https://www.slowmist.com/report/first-half-of-the-2023-report(EN).pdf)
14. Crypto Crime Mid-year Update: Crime Down 65% Overall, But Ransomware Headed for Huge Year Thanks to Return of Big Game Hunting. URL: <https://www.chainalysis.com/blog/crypto-crime-midyear-2023-update-ransomware-scams/>
15. Dannen Chris. Introducing Ethereum and solidity. Vol. 1. Berkeley: Apress, 2017
Hargreaves Andy, and Michael T. O'Connor. "Solidarity with solidity: The case for collaborative professionalism." Phi Delta Kappan 100, no. 1 (2018): 20-24.
16. Ethereum/viper: New experimental contract-oriented, pythonic programming language. // viper документація. URL: <https://ethereum-viper.readthedocs.io/en/latest/>
17. F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," Telematics Informat., vol. 36, с. 55–81, Березень, 2019.
18. Ferretti Stefano, and Gabriele D'Angelo. "On the ethereum blockchain structure: A complex networks theory perspective." Concurrency and Computation: Practice and Experience 32, no. 12 (2020): e5493.
19. Ganache . URL: <https://trufflesuite.com/docs/ganache/>
20. IBM.. URL: <https://www.ibm.com/products>
21. Most Popular Smart Contract Security Challenges. URL: <https://101blockchains.com/smart-contract-security-challenges/>
22. M. Alharby and A. van Moorsel. Blockchain-based Smart Contracts: A Systematic Mapping Study. arXiv preprint arXiv:1710.06372, 2017.
23. Na Dong Gyu, Jung Hwan Baek, Jin Yong Sung, Ji-Hoon Kim, Jae Kyun Kim, Young Jun Choi, and Hyobin Seo. "Thyroid imaging reporting and data system risk stratification of thyroid nodules: categorization based on solidity and echogenicity." Thyroid 26, no.4 (2016): 562-572.
24. Pavlyshenko Bohdan M. "Bitcoin Price Predictive Modeling Using Expert Correction." In 2019 XIth International Scientific and Practical Conference on Electronics and Information Technologies (ELIT), pp. 163-167.
25. Remix IDE // Середовище розробки, установник, документація. URL: <https://remix->

project.org/

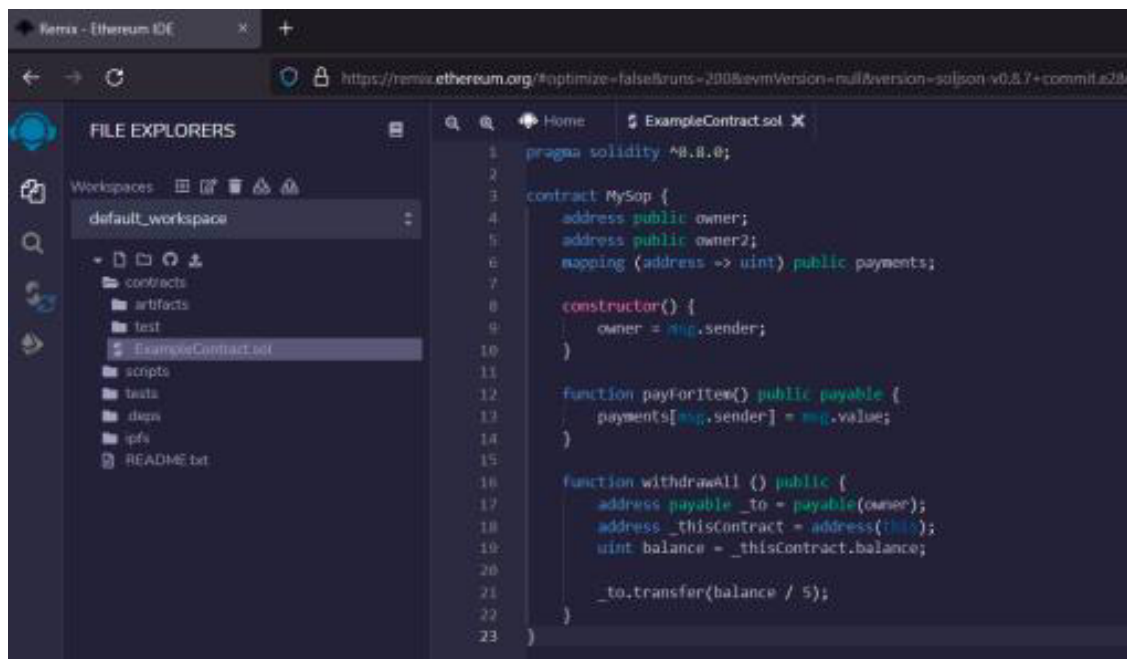
26. Remix IDE Usage . URL: <https://dudochkin-victor.github.io/edgeware/contribute-and-engage/develop/edgeware-smart-contracts/deploy-an-evm-contract/using-remix-ethereum-ide/>
27. Serpent // Serpent документація. URL: https://ethereumbuilders.gitbooks.io/guide/content/en/serpent_features.html
28. Singh Madhusudan, and Shiho Kim. "Blockchain technology for decentralized autonomous organizations." In Advances in computers, vol. 115, pp. 115-140. Elsevier, 2019.
29. Smart Contract Challenges. URL: <https://hedera.com/learning/smart-contracts/smart-contract-challenges>
30. Smart Contract Development. URL: <https://limechain.tech/blockchain-development/smart-contract-development/#:~:text=What%20is%20Smart%20Contract%20Development,when%20those%20conditions%20are%20met.>
31. Smart Contracts Market. URL: <https://www.snsinsider.com/reports/smart-contracts-market-1542>
32. SMART CONTRACTS: TYPES AND APPLICATION. URL: <https://rva.solutions/blog/smart-contracts-types-and-application>
33. Solidity // Solidity документація. URL: <https://docs.soliditylang.org/en/latest/>
34. T. McGhin, K.-K.-R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," J. Netw. Comput. Appl., vol. 135, c. 62–75, Червень, 2019.
35. The Essence of the Blockchain. URL: <https://miracl.com/blog/the-essence-of-the-blockchain/>
36. The Essence of Blockchain Theory: Unleashing Trust, Transparency, and Decentralization. URL: <https://medium.com/@tesla8877/the-essence-of-blockchain-theory-unleashing-trust-transparency-and-decentralization-b1b698008efe>
37. The Top 5 Blockchain App Development Trends for 2023. URL: <https://www.infuy.com/blog/the-top-5-blockchain-app-development-trends-for-2023/#:~:text=In%202023%2C%20we%20will%20see,in%2Dgame%20assets%20as%20N>

[FTs.](#)

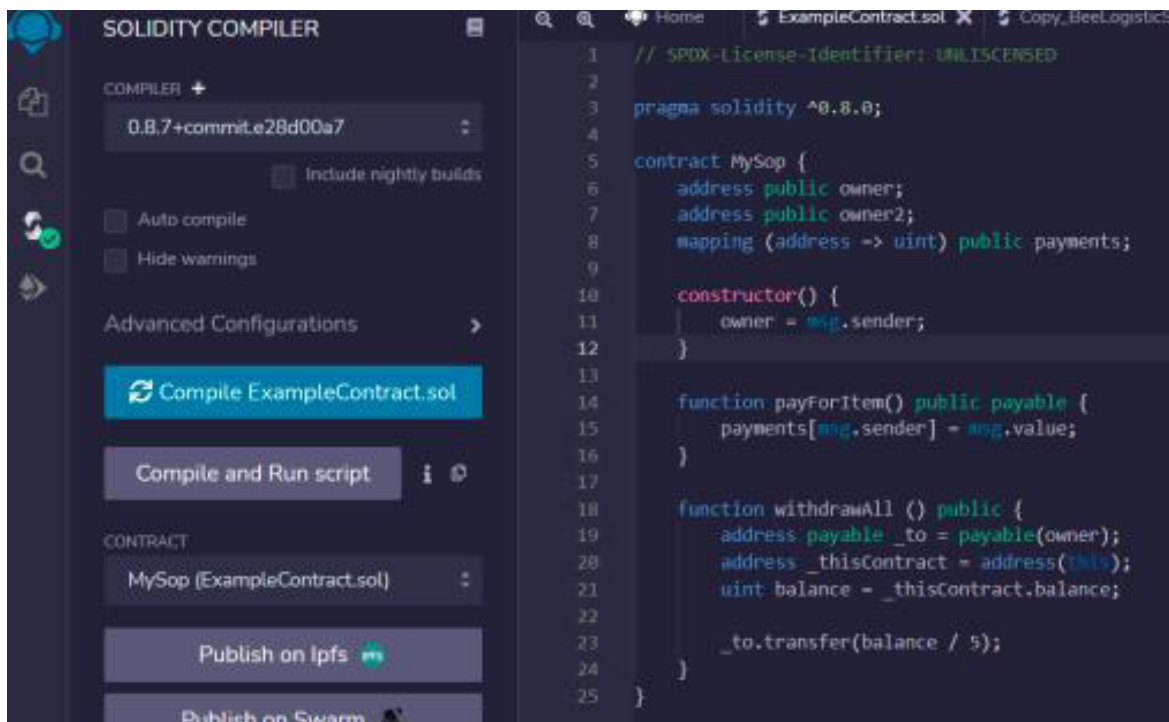
38. Understanding the Downsides of Smart Contracts in Blockchain. URL: <https://www.section.io/engineering-education/understanding-the-downsides-of-smart-contracts-in-blockchain/>
39. WHAT ARE SMART CONTRACTS?. URL: https://klona.ua/en/blog/blockchain_smart-contract-en/what-are-smart-contracts
40. What Are Smart Contracts? Types, Benefits, and Tools. URL: <https://www.spiceworks.com/tech/innovation/articles/what-are-smart-contracts/>
41. Yugandhara R.Y. Smart Contracts Market Size, Growth, Trends Report 2023-2030. URL: https://www.researchgate.net/publication/371347872_Smart_Contracts_Market_Size_Growth_Trends_Report_2023-2030
- 42.5 Smart Contract Development Trends To Watch In 2023. URL: <https://blog.cryptostars.is/5-smart-contract-development-trends-to-watch-in-2023-3716afec22d2>

ДОДАТКИ

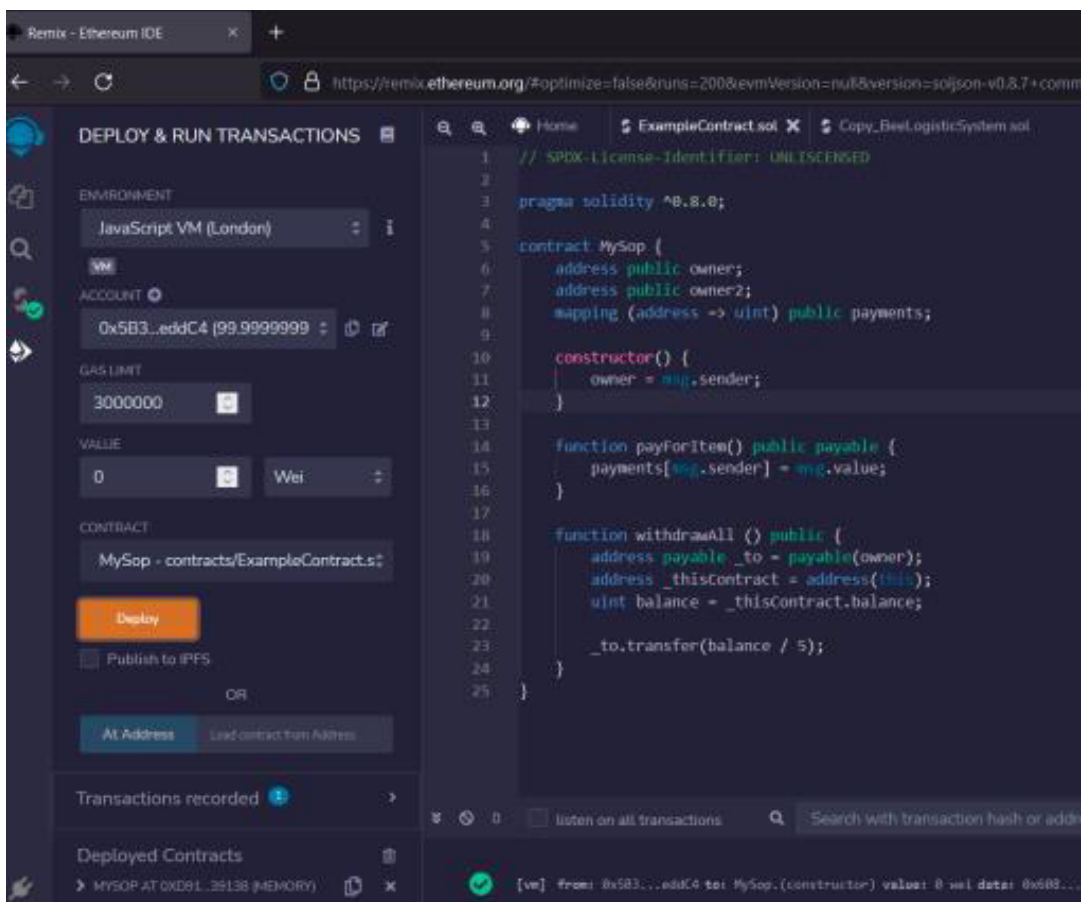
Remix IDE створення контракту[26]



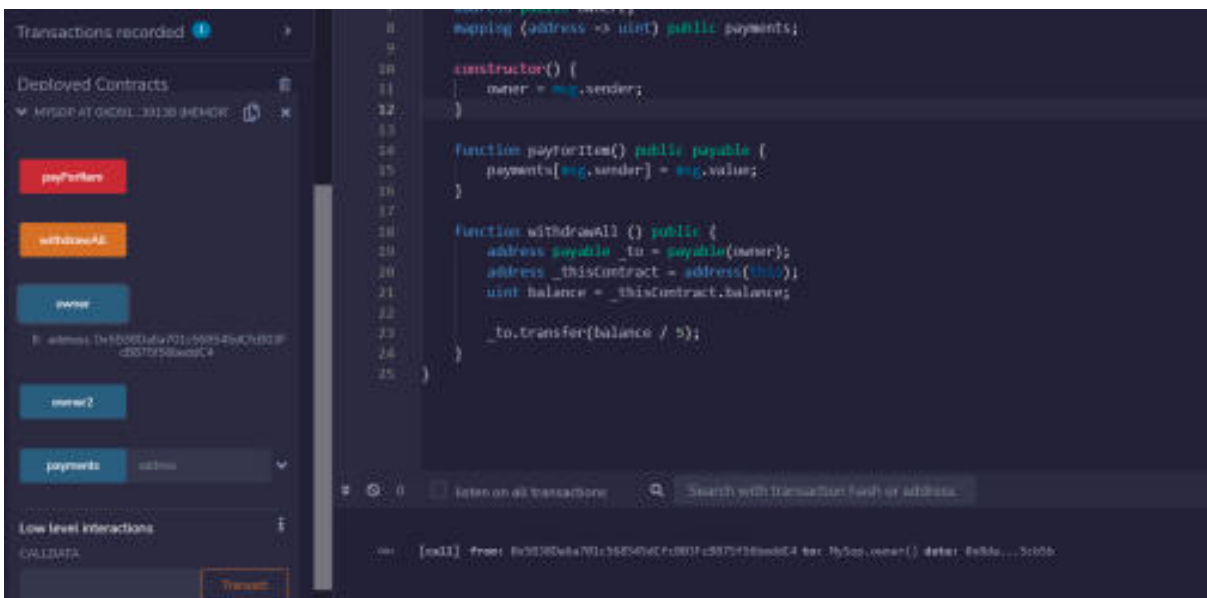
Remix IDE компілювання контракту[26]



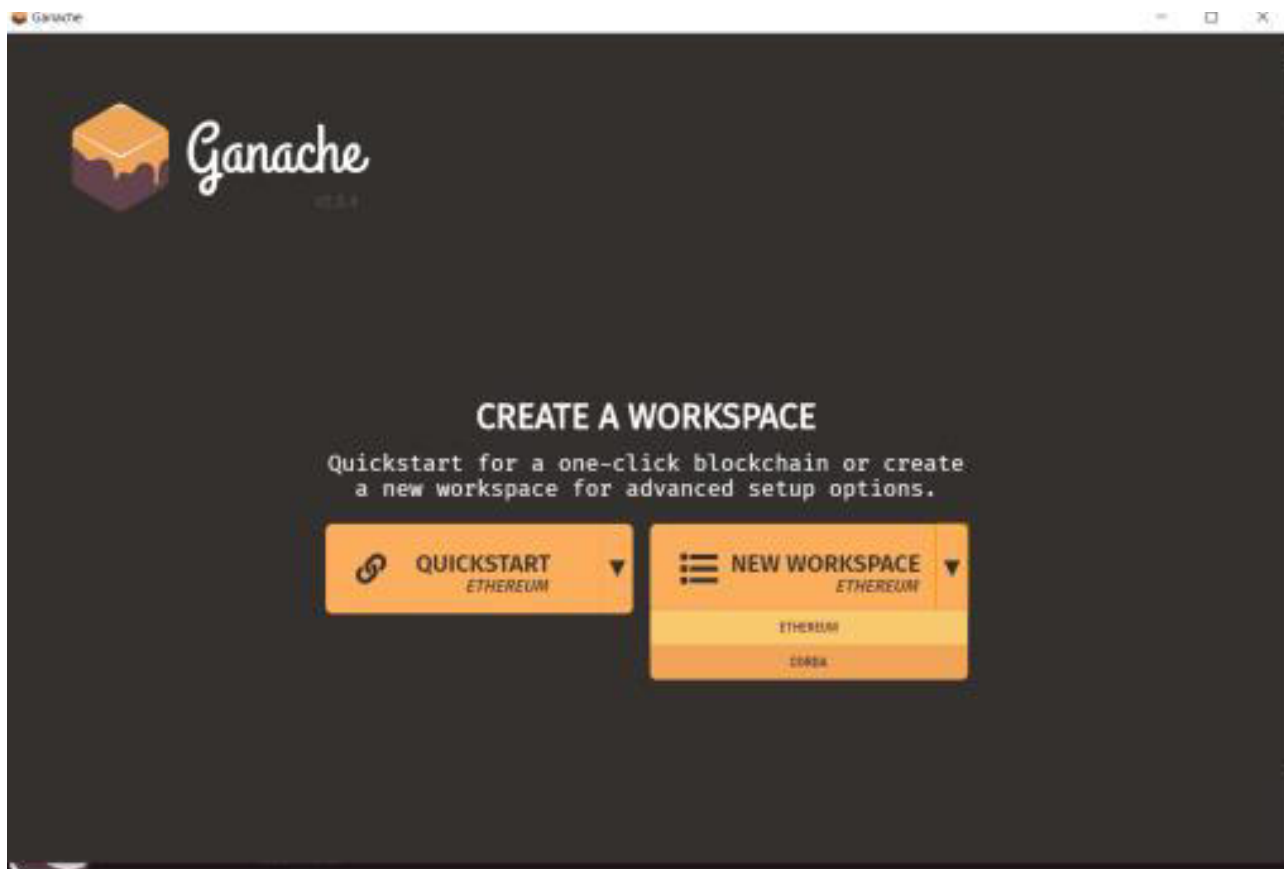
Remix IDE розгортання контракту[26]



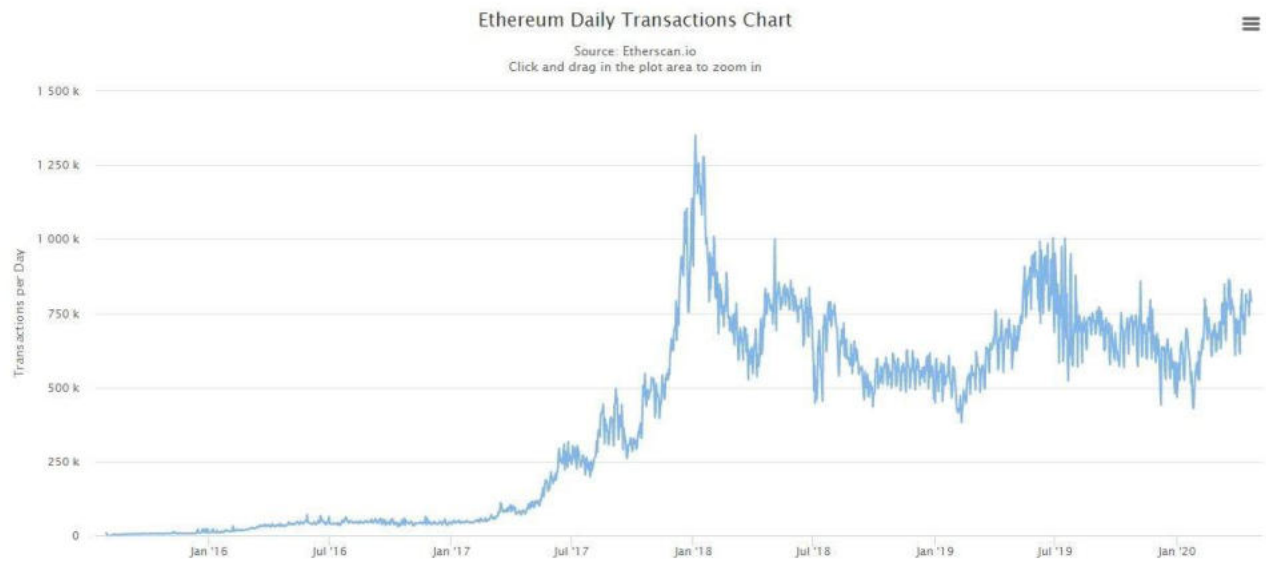
Remix IDE тестування контракту[26]



Ganache початкове вікно[19]



Зниження ціну на Ефіріум[]



Викрадені та повернуті активи[13]

