КОМП'ЮТЕРНИЙ ПРАКТИКУМ КРЕДИТНОГО МОДУЛЯ
"БЛОКЧЕЙН ТА ДЕЦЕНТРАЛІЗОВАНІ СИСТЕМИ"

Лабораторна робота № 2

Виконали:
студенти групи ФІ-31мн
Шевцова Марія та Намчук Олександр

Тема: *Реалізація смарт-контракту або анонімної криптовалюти.*
Мета роботи: *«Отримання навичок роботи із смарт-контрактами або анонімними криптовалютами»*
Для першого типу лабораторних робіт
дослідження методів анонімізації/деанонімізації запропонованої криптовалюти із аналізом складності проведення атак деанонімізації і втрат ефективності анонімних криптовалют у порівнянні із Bitcoin/Litecoin; оцінка та обґрунтування необхідних ресурсів (гасу і ефіру), потрібних для функціонування смарт-контракту.

Вступ

Сучасні блокчейн-технології надають безліч можливостей для створення та використання як смарт-контрактів, так і анонімних криптовалют. Смарт-контракти дозволяють автоматизувати виконання угод, тоді як анонімні криптовалюти забезпечують високий рівень приватності користувачів. Ця лабораторна робота присвячена дослідженню методів анонімізації та деанонімізації криптовалют, а також оцінці необхідних ресурсів для функціонування смарт-контрактів.

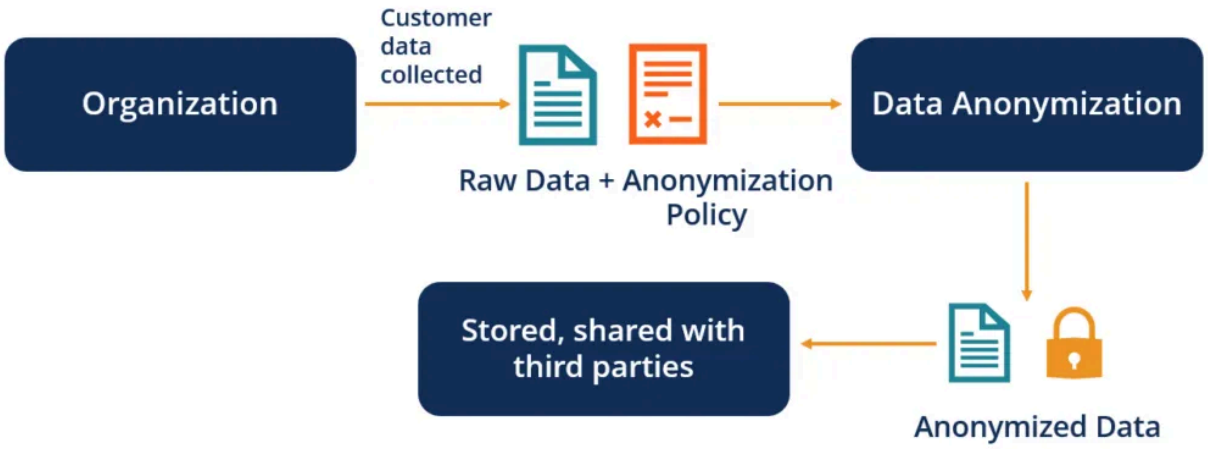
1. Дослідження методів анонімізації криптовалют

1.1 Методи анонімізації

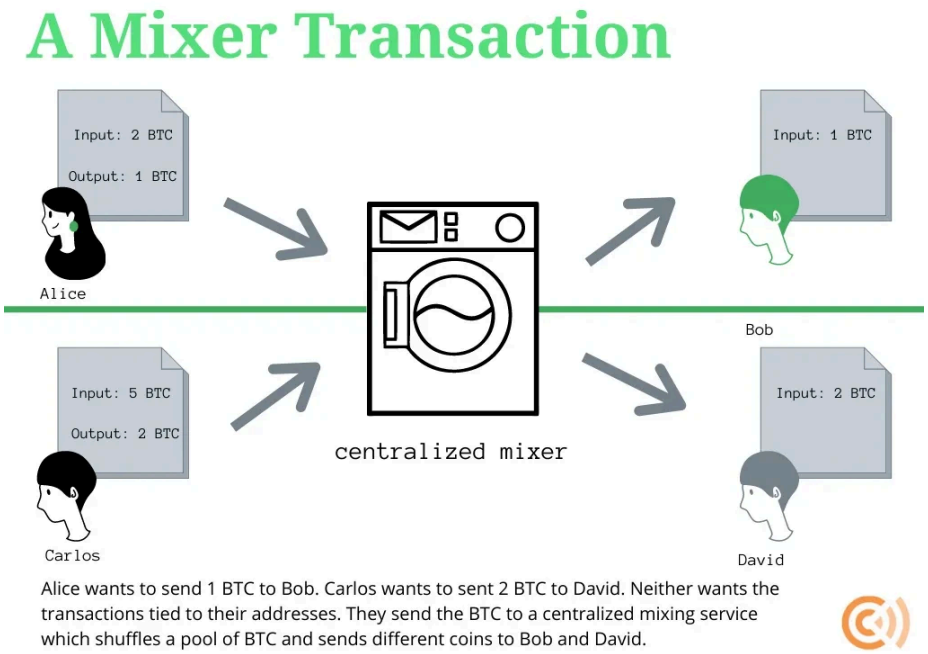
Анонімні криптовалюти використовують різні методи для забезпечення конфіденційності транзакцій. Основні методи включають:

- Змішування монет (Coin Mixing): транзакції об'єднуються з іншими, щоб ускладнити відстеження джерела та одержувача.

- Кільцеві підписи (Ring Signatures): кожна транзакція підписується групою користувачів, що ускладнює ідентифікацію конкретного відправника.
- Stealth-адреси: для кожної транзакції створюється нова адреса, що приховує зв'язок між транзакціями.
- Протокол Zerocoin/Zerocash: забезпечує повну анонімність шляхом створення та знищення монет в окремих транзакціях.

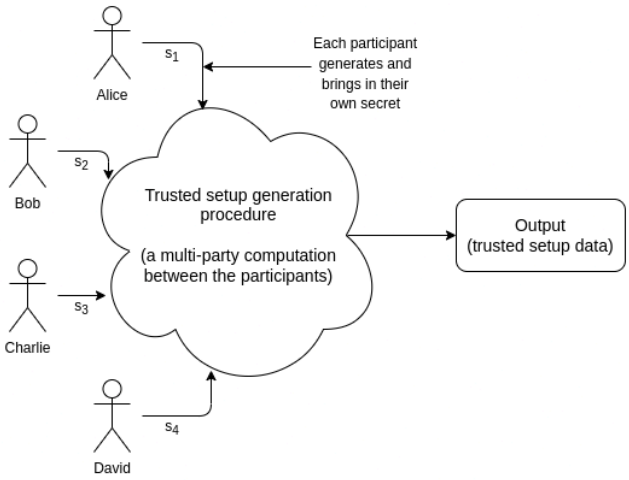


1. Змішування монет (Coin Mixing): Процес змішування монет включає в себе об'єднання декількох транзакцій від різних користувачів у одну або кілька транзакцій, що ускладнює відстеження вихідних і кінцевих адрес. Це досягається за допомогою спеціальних сервісів, які беруть участь у змішуванні монет. Схема цього процесу зображена на рисунку.



Переваги	Недоліки
Захищає користувачів від кіберзлочинців, унеможливлюючи їх відстеження.	Юридичний статус міксерів нестабільний на криптовалютному ринку.
Міксери забезпечують конфіденційність та анонімність транзакцій.	Існує обмеження на кількість токенів, які можуть бути транзакційовані в пулі.
Великі організації можуть забезпечити приватність своїх переказів та угод.	Відсоток комісії може бути невідповідним для малих транзакцій.
Окрім Bitcoin, у процесі змішування монет можуть брати участь й інші криптовалюти.	Загрози кібер-атак все ще існують у цих міксерах.

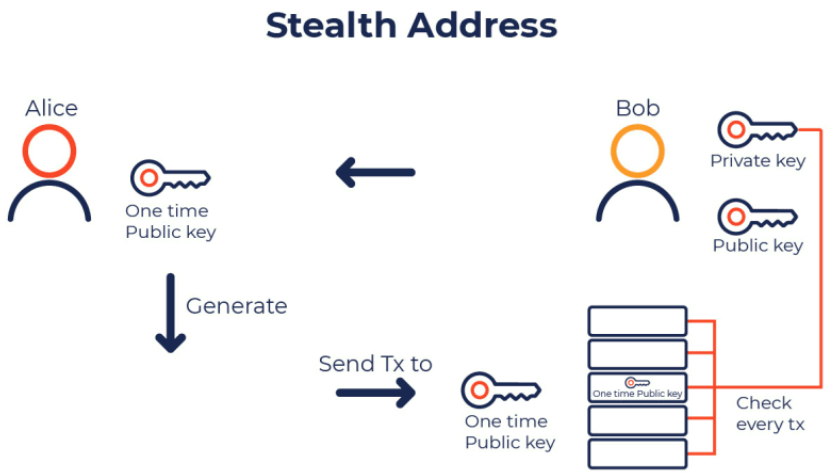
2. Кільцеві підписи (Ring Signatures): Кільцеві підписи використовуються для приховування особи відправника, оскільки підпис надається групою користувачів. Це означає, що для кожної транзакції створюється кільце підписів, ідентифікувати реального відправника стає неможливо. Більш наглядна схема кільцевих підписів представлена на рисунку.



Переваги	Недоліки
Анонімність: Дозволяють підписанту приховати свою особу серед групи користувачів.	**Складність реалізації**: Впровадження кільцевих підписів є складним та ресурсоємким.
Безпека: Забезпечують високий рівень криптографічного захисту для транзакцій.	**Розмір транзакцій**: Збільшують розмір транзакцій, що може впливати на швидкість мережі.
Відсутність потреби у довірі: Не вимагають довіри до інших учасників кільця.	**Витрати**: Підвищують вартість транзакцій через додаткові обчислювальні витрати.
Гнучкість: Можуть використовуватись у різних типах криптовалют та блокчейнів.	**Складність деанонімізації**: Може бути важко провести аудит або розслідування транзакцій.

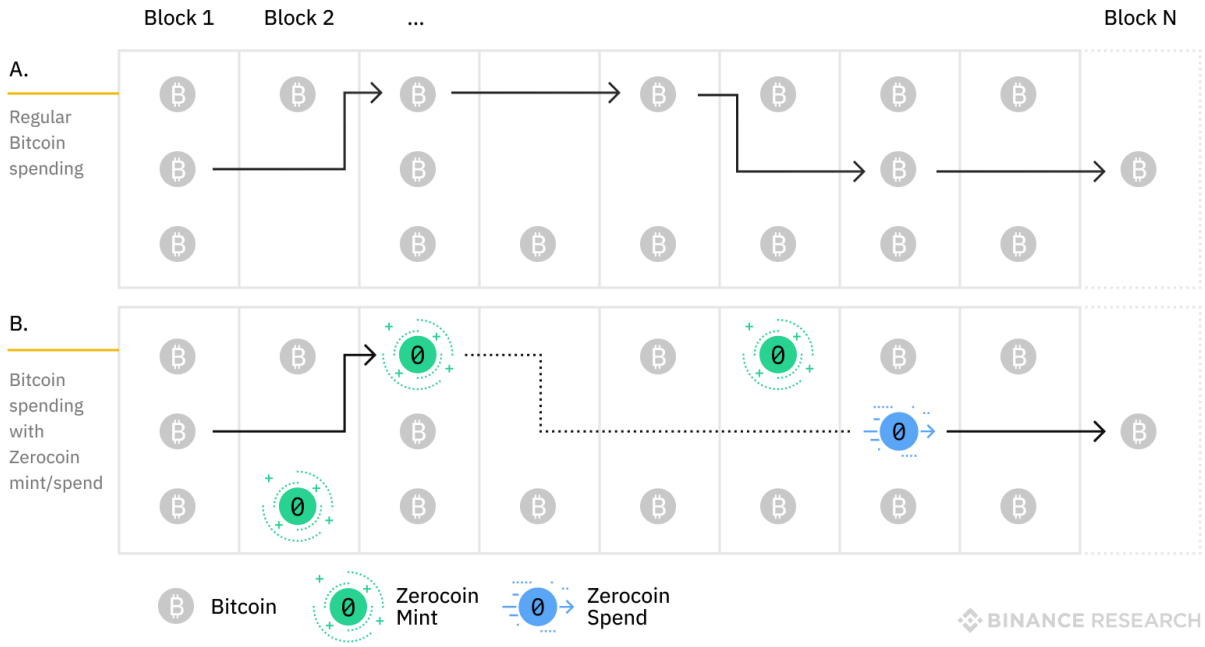
3. Stealth-адреси: Stealth-адреси дозволяють одержувачу створювати одноразові адреси для кожної транзакції, що приховує зв'язок між транзакціями. Цей метод широко використовується в

криптовалютах, таких як Monero. Схема роботи stealth-адрес зображена на рисунку.



Переваги	Недоліки
Високий рівень конфіденційності: Кожна транзакція використовує унікальну адресу, що ускладнює відстеження транзакцій.	**Складність управління**: Користувачам може бути важко управляти великою кількістю одноразових адрес.
Покращена анонімність: Захищають особу одержувача, оскільки адреси не повторюються.	**Обмежена підтримка**: Не всі криптовалюти та гаманці підтримують **stealth**-адреси.
Безпека: Знижують ризик відстеження транзакцій третіми сторонами.	**Вищі витрати**: Використання **stealth**-адрес може вимагати додаткових обчислювальних ресурсів.
Гнучкість: Можуть бути інтегровані в різні проекти для підвищення конфіденційності.	**Складність реалізації**: Впровадження та використання **stealth**-адрес може бути складним для розробників.

4. Протокол Zerocoin/Zerocash: Цей протокол забезпечує повну анонімність, дозволяючи користувачам знищувати монети і створювати нові. Таким чином, неможливо відстежити транзакції, оскільки всі сліди видаляються під час процесу. Схема протоколу Zerocoin/Zerocash представлена на рисунку.

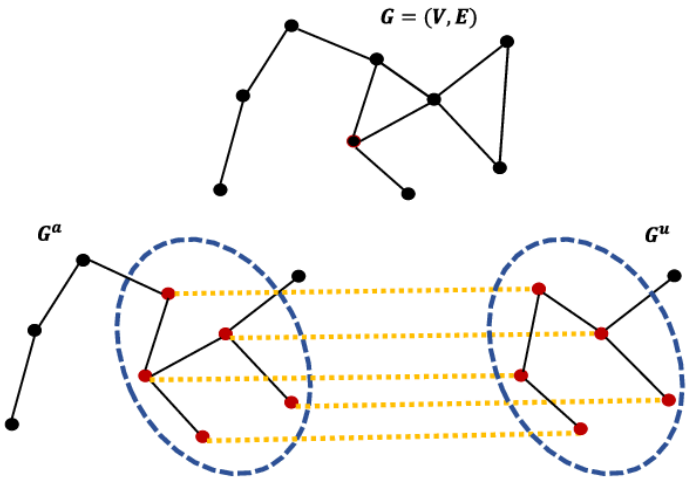


Переваги	Недоліки
Повна анонімність: Забезпечує повну анонімність транзакцій, приховуючи відправника, одержувача та суму транзакції.	**Висока складність:** Впровадження протоколу є складним завданням для розробників і потребує значних ресурсів.
Стійкість до аналізу: Надійно захищає від аналізу графів транзакцій та інших методів деанонімізації.	**Високі обчислювальні витрати:** Вимоги до обчислювальних ресурсів значно вищі, ніж у традиційних криптовалютах.
Масштабованість: Підтримує високий рівень анонімності навіть у великих мережах з великою кількістю користувачів.	**Збільшений розмір транзакцій:** Транзакції можуть бути значно більшими, що впливає на швидкість мережі.
Гнучкість: Може бути використаний для різних криптовалют, підвищуючи їх конфіденційність.	**Складність аудиту:** Ускладнює аудит та розслідування транзакцій, що може бути проблемою для регуляторів.
Прозорість: Усі транзакції є прозорими, але анонімними, що забезпечує додатковий рівень безпеки.	**Потреба в спеціалізованому програмному забезпеченні:** Для використання протоколу потрібне спеціалізоване ПЗ.

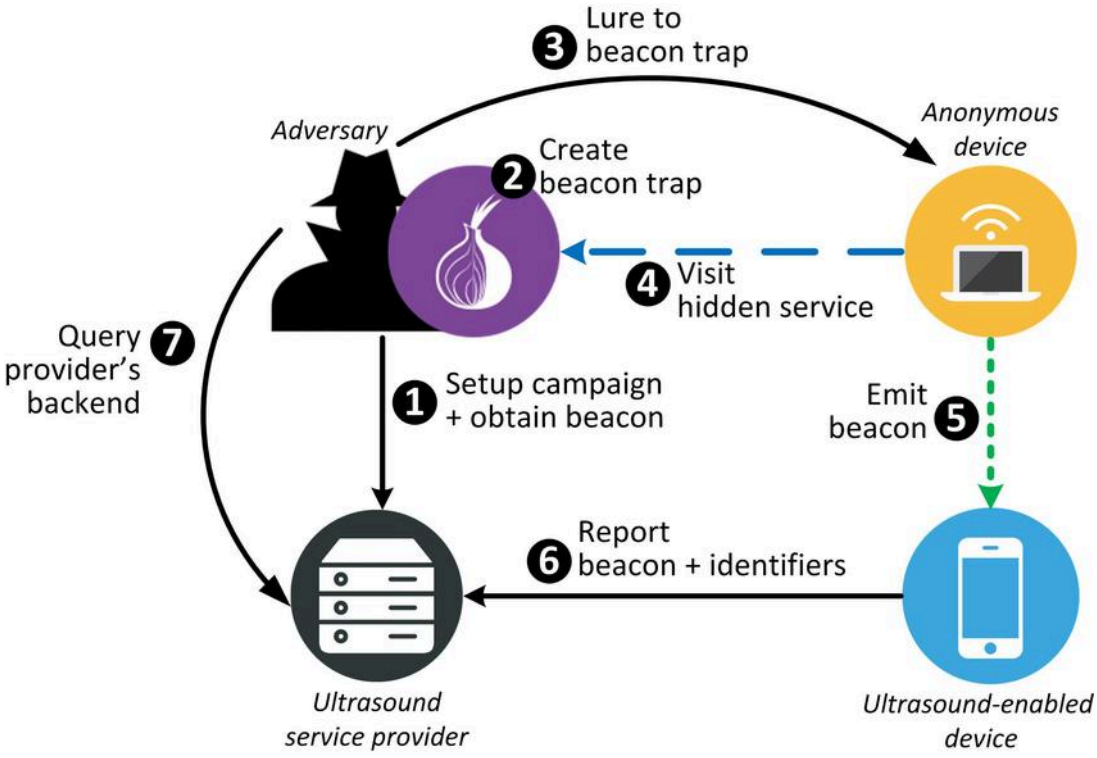
1.2 Аналіз складності проведення атак деанонімізації

Атаки деанонімізації спрямовані на виявлення особи, що стоїть за певною транзакцією. Відомі методи атак включають:

- Аналіз графів транзакцій: Відстеження шляхів транзакцій у блокчейні для ідентифікації користувачів. Зазвичай використовуються алгоритми аналізу графів, які дозволяють виявити певні закономірності та встановити зв'язки між адресами. Спростовна схема аналізу графів.



- Змішування зі сторонніми даними: Використання зовнішніх даних для ідентифікації учасників транзакцій. Наприклад, якщо користувач публічно повідомляє свою адресу, це може бути використано для деанонімізації його транзакцій.
- Атаки на вузли мережі: Перехоплення інформації від вузлів, що обробляють транзакції. Це може включати моніторинг мережевого трафіку та аналіз даних, що передаються між вузлами. Схема атаки на вузли мережі зображена на рисунку.



Складність проведення атак залежить від використовуваних методів анонімізації. Протоколи, такі як Zerocoin/Zerocash, значно ускладнюють деанонімізацію завдяки високому рівню криптографічного захисту. Проте, методи аналізу графів транзакцій та атаки на вузли можуть залишатись ефективними для інших криптовалют, які використовують менш складні методи анонімізації.

1.3 Втрати ефективності анонімних криптовалют у порівнянні з Bitcoin/Litecoin

Анонімні криптовалюти зазвичай мають деякі втрати ефективності у порівнянні з традиційними криптовалютами, такими як Bitcoin або Litecoin. Ці втрати можуть включати:

- Збільшені розміри транзакцій: Використання додаткових даних для анонімізації призводить до збільшення розмірів транзакцій. Наприклад, у Monero кожна транзакція включає кільцеві підписи та одноразові адреси, що збільшує її розмір у порівнянні з транзакціями в Bitcoin.
- Зниження швидкості підтвердження транзакцій: Додаткові етапи обробки анонімних транзакцій можуть уповільнювати підтвердження. Це пов'язано з тим, що обробка складних криптографічних алгоритмів вимагає більше часу та обчислювальних ресурсів. С
- Збільшені вимоги до обчислювальних ресурсів: Алгоритми анонімізації вимагають більшої обчислювальної потужності для обробки транзакцій. Наприклад, у Monero використовується складний алгоритм CryptoNote, що вимагає значних ресурсів для виконання операцій.

2. Оцінка та обґрунтування необхідних ресурсів для функціонування смарт-контракту

2.1 Розрахунок витрат на газ та ефір

Смарт-контракти на платформі Etherium вимагають певну кількість газу (Gas) для виконання операцій. Газ — це одиниця виміру обчислювальних зусиль, необхідних для виконання операцій. Ціна газу визначається в ефірі (ETH). Основні етапи включають:

- Розрахунок газу для операцій: Кожна операція в смарт-контракті має визначену вартість у газі. Наприклад, операція зберігання даних у блокчейні коштує більше газу, ніж операція читання даних. Таблиця вартості операцій у газі зображена нижче.

Operation	Gas cost	Price(Ether)	Price ($USD)
Factory deployment	2,344,498	0.2907178	489.28
Auction creation	1,760,105	0.218253	367.32
First bid of contract	237,518	0.0294522	49,57
First bid of user	207,829	0.0257708	43,37
Modify existing bid	94,747	0.0117486	19,77
Adjudication	198,295	0.0245886	41.38
Total (scenario)	**3,180,058**	**0.3943272**	**663.65**

- Оцінка загальних витрат: Множення кількості газу на поточну ціну газу в ефірі. Наприклад, якщо ціна газу становить 80 Gwei, а смарт-контракт вимагає 42,300 газу для виконання, загальні витрати складатимуть 0.00338 ETH.

Схема оцінки вартості смарт-контракту

2.2 Приклад оцінки вартості смарт-контракту

Розглянемо простий смарт-контракт для зберігання та передачі токенів:
solidity

```
pragma solidity ^0.8.0;

contract SimpleToken {
 mapping(address => uint256) public balances;

 function transfer(address to, uint256 amount) public {
 require(balances[msg.sender] >= amount, "Insufficient balance");
 balances[msg.sender] -= amount;
 balances[to] += amount;
 }
}
```

Для оцінки вартості виконання функції transfer потрібно врахувати витрати на газ для:

- Читання та запис даних до мапінгу balances.
- Виконання умов та логіки контракту.

Схема оцінки вартості смарт-контракту

1. Читання даних з мапінгу balances:
    - Операція: balances[msg.sender]
    - Вартість: 2100 газу
2. Перевірка умов:
    - Операція: require(balances[msg.sender] >= amount, "Insufficient balance");

- Вартість: 700 газу

3. Запис даних у мапінг balances:
    - Операція: balances[msg.sender] -= amount
    - Вартість: 5000 газу
4. Запис даних у мапінг balances:
    - Операція: balances[to] += amount
    - Вартість: 5000 газу
5. Виконання логіки контракту:
    - Інші операції: передача керування, виклик функцій і т.д.
    - Вартість: 2100 газу

Загальна вартість:

- Сумарна вартість газу: 2100 + 700 + 5000 + 5000 + 2100 = 14900 газу

Приклад розрахунку:

- Ціна газу: 20 Gwei
- Загальні витрати: 14900 газу * 20 Gwei = 298000 Gwei = 0.000298 ETH

Схема:

```
[SimpleToken Contract]
|
+--> Читання balances[msg.sender] (2100 газу)
|
+--> Перевірка require (700 газу)
|
+--> Запис balances[msg.sender] -= amount (5000 газу)
|
+--> Запис balances[to] += amount (5000 газу)
|
+--> Виконання логіки контракту (2100 газу)
|
+--> Загальна вартість: 14900 газу
```

Висновок

Дослідження методів анонімізації та деанонімізації криптовалют показує, що анонімні криптовалюти мають свої переваги та недоліки. Високий рівень приватності досягається за рахунок збільшених розмірів

транзакцій та зниження швидкості їх обробки. Оцінка витрат на функціонування смарт-контрактів показує, що ефективність та вартість виконання операцій значною мірою залежать від складності контракту та поточних цін на газ та ефір.