УДК 004.658.114
С. Соленко, Р. Жаровський, канд. техн. наук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МОЖЛИВОСТІ СЕРЕДОВИЩА PLUTUS PLAYGROUND ДЛЯ НАПИСАННЯ ТА ТЕСТУВАННЯ СМАРТ-КОНТРАКТІВ

UDC 004.658.114
S. Solenko, R. Zharovskyi, Ph.D.

PLUTUS PLAYGROUND ENVIRONMENT CAPABILITIES FOR WRITING AND TESTING SMART CONTRACTS

Платформа Plutus – це платформа для написання додатків, які взаємодіють із розподіленим реєстром із можливостями написання сценаріїв, зокрема блокчейном Cardano.

Практичними результатами роботи є розробка smart-контракту та програми Plutus для громадського фінансування (краудфандінг). Програма приймає кошти від учасників кампанії, дає проміжок часу власнику кампанії щоб зібрати кошти і якщо кошти не було зібрано то повертає їх учасникам кампанії.

Розроблятися програма буде в середовищі Plutus Playground. Plutus Playground забезпечує середовище для написання та тестування смарт-контрактів перед їх випуском на блокчейні Cardano. Plutus Core, яка є мовою smart-контрактів, вбудована в реєстр, заснована на формальних принципах програмування Haskell і дозволяє розробникам писати програми з високою надійністю, які взаємодіють з Cardano. Haskell був обраний як основа для платформи Plutus, оскільки він виділяється серед інших мов програмування тим, що пропонує можливість писати більш безпечний код. Використання Haskell для розгортання smart-контрактів гарантує, що контракти запрограмовані на те, що від них очікується, і їх можна перевірити на точність перед впровадженням.

Є два результати кампанії.

1. Власник кампанії збирає кошти від обох учасників. У цьому випадку власник створює одну транзакцію з двома входами, посилаючись на "t_1" і "t_2". Кожен вхід містить скрипт `contributionScript c`, спеціалізований для учасника. Сценарій викупу цієї транзакції містить значення `Collect`, що спонукає сценарій перевірки перевірити гілку на наявність `Collect`.
2. Відшкодування. У цьому випадку кожен вкладник створює транзакцію з одним введенням, вимагаючи повернення своєї частини коштів. Цей випадок охоплює гілка відшкодування "Refund", а його сценарієм викупу є дія відшкодування "Refund".

В обох випадках сценарій перевірки виконується двічі. У першому випадку існує одна транзакція, яка споживає обидва входи. У другому випадку є дві різні транзакції, які можуть відбутися в різний час.

Ouroboros протокол розділяє час на епохи. Кожна епоха Cardano складається з кількох слотів, де кожен слот триває одну секунду.

Наступна послідовність дій (див. рис. 1) призводить до успішної кампанії.

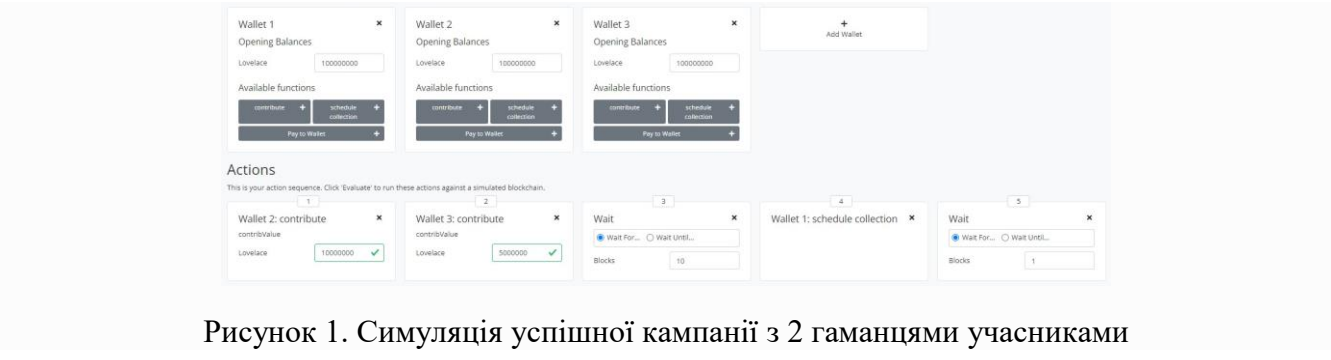

Рисунок 1. Симуляція успішної кампанії з 2 гаманцями учасниками

Гаманець 2 та 3 заносять кошти в кампанію. Після очікування в 10 блоків власник кампанії має право зібрати кошти, що виконуєтся через кнопку «schedule collection». Чекаємо ще 1 блок щоб виконалася транзакція.

Перша транзакція це генезис яка створює початкові кошти на гаманцях (див. рис. 2). Гаманець 2 вносить кошти в розмірі 10,000,000 Lovelace, а гаманець 3 в розмірі 5,000,000 Lovelace (див. рис. 3). Власник кампанії збирає кошти в 11 слоті (див. рис. 4–5).

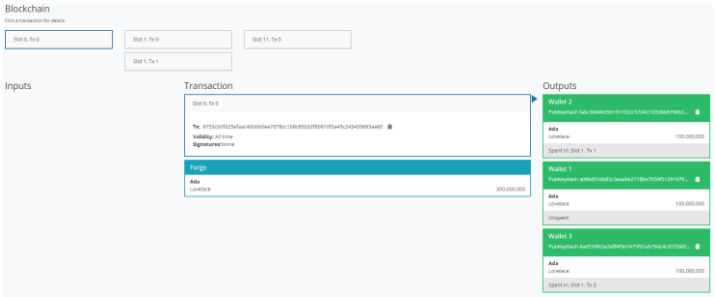

Рисунок 2. Слот 0 генезис

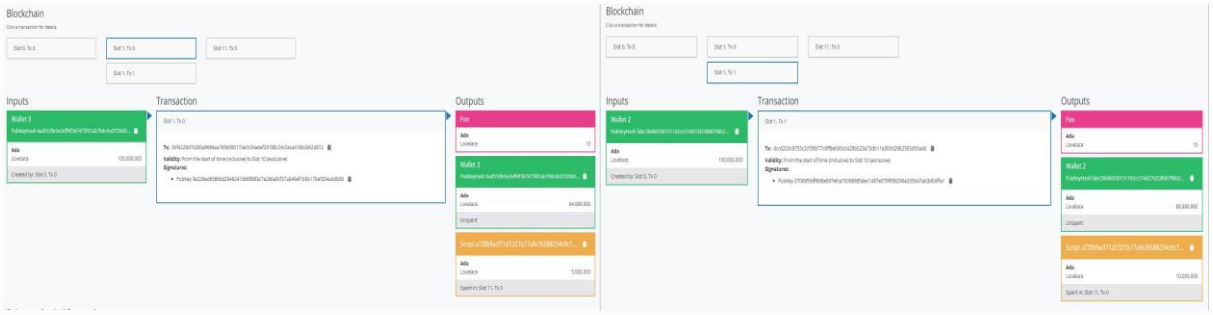

Рисунок 3. Слот 1 внесення коштів 2 та 3 гаманцем

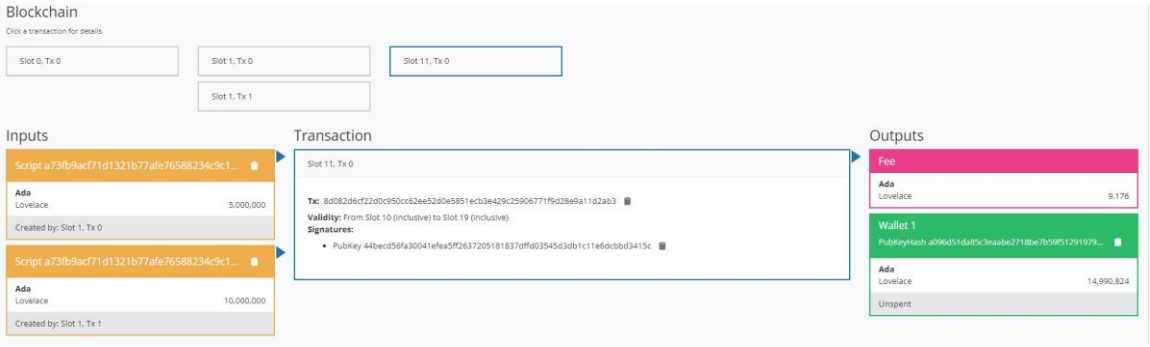

Рисунок 4. Слот 11 збір коштів власником кампанії

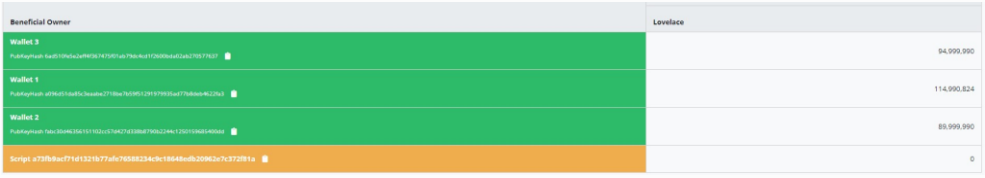

Рисунок 5. Слот 11 остаточний баланс

Як бачимо кампанія пройшла успішно і 15,000,000 Lovelace з вирахуванням комісії за транзакції поступили на гаманець власника кампанії.

Smart-контракти це сучасна і прогресивна технологія яка може допомогти вирішити велику кількість завдань в комерційній галузі. Вважаю, що написання smart-контрактів на базі блокчейна Cardano є технологічно і економічно хорошим рішенням для використання в електронній комерції. В роботі буде проведено аналіз архітектури та технології блокчейну Cardano і розглянуті методи та засоби реалізації smart-контрактів на базі даного блокчейну.