

УДК 004.75

О.С. Тхір

Тернопільський національний технічний університет імені Івана Пулюя, Україна

РЕАЛІЗАЦІЯ SMART-КОНТРАКТІВ ДЛЯ СТРАХОВОЇ КОМПАНІЇ НА ПЛАТФОРМІ ETHEREUM

O.S. Tkhir

IMPLEMENTATION OF SMART CONTRACTS ON THE ETHEREUM PLATFORM FOR INSURANCE COMPANY

Ринок страхових послуг є другим за рівнем капіталізації серед інших небанківських фінансових ринків. Страховий ринок з'явився внаслідок людської необхідності захистити себе та свою власність від несподіваних ризиків. Ця сфера динамічно розвивається. Страховий ринок в Україні один з найбільш перспективних: доходи населення поступово зростають, кількість прибуткових підприємств збільшується. Ці фактори вимагають страхового забезпечення, яке, в свою чергу, буває добровільним і обов'язковим. Обов'язковими видами страхування є страхування предметів іпотеки від ризиків випадкового знищення; страхування тварин на випадок епідемії, вимушеного забою або загибелі; страхування відповідальності власників собак; страхування цивільної відповідальності осіб, які мають зброю; нещасні випадки на транспорті. До необов'язкових видів страхування належать страхування життя, страхування від нещасних випадків, страхування майна, страхування кредитів, неперервне страхування здоров'я та інші. Технологію Blockchain можна використовувати для:

- зменшення експлуатаційних витрат та покращення рівня обслуговування клієнтів;
- введення даних/перевірки особистих даних;
- преміального обчислення;
- оцінки ризиків, попередження шахрайства;
- плата за користування, мікрострахування;
- однорангового страхування.

Блокчейн в страхуванні може використовуватися для вирішення наступних завдань, зокрема зменшення частки паперового документообігу, створення унікальної системи для забезпечення оперативного підтвердження та обробки страхових вимог, зведення до мінімуму випадків шахрайства, підвищення довіри до страхової компанії, підвищити швидкість та ефективність страхового процесу.

Блокчейн-платформи умовно платформи умовно поділяються на глобальні та приватні. Глобальні платформи надають користувачам і розробникам додатків можливість використовувати блокчейн мережу, доступну для всіх бажаючих. У такій мережі на smart-контракти, їх коректність та безпеку лягає вся відповідальність постачальника послуг перед клієнтами. Приватні використовуються коли компанія має бажання впровадити блокчейн і smart-контракти на внутрішніх рівнях своєї системи і не давати користувачам можливості підключатися до них безпосередньо. Компанія отримує такі переваги блокчейну, як підвищення безпеки, бездоганне збереження транзакцій, при цьому користувачі системи будуть користуватися звичними послугами, якість яких не викликатиме у них сумнівів. Smart-контракти розміщуються на спеціальних платформах, таких як Ethereum, EOS, Waves, Cardano, Stellar, NEO, Hyperledger Fabric, Aeternity, Emotiq, Bitcoin, Side Chains, NXT та інші. Компанія має можливість вибрати зручну для себе платформу, оцінивши умови, переваги та недоліки кожної із них.[1]

Для класифікації smart-контрактів можна задавати різні групи критеріїв. За середовищем виконання є децентралізовані та централізовані. Перевагою децентралі-

зованого середовища є більша відмовостійкість та незалежність під час виконання. По процесу завдання і виконання умов поділяють на довільно програмовані, обмежені або попередньо записані, тобто суворо типізовані. Коли на платформі smart-контрактів існують певні шаблони та параметри до них можна задавати довільним чином. Це пришвидшує час роботи, оскільки потрібно вибрати із списку контракт та задати потрібні параметри. Повний по Тюрінгу smart-контракт дозволяє задавати практично будь-які алгоритми в якості умов виконання контракту: прописувати цикли, функції розрахунку ймовірностей, власні алгоритми електронного підпису, тощо. Довільні smart-контракти не є повними по Тюрінгу. До такого типу можна віднести Bitcoin і Litecoin із своїм скриптом. Тобто, в довільному порядку можна використовувати лише певні операції, але не можна написати власні алгоритми та цикли.

Розроблюваний проект буде розміщений на платформі Ethereum.[2] На платформі існує два типи аккаунтів: користувача та контракту. Управління аккаунтом користувача здійснюється за допомогою особистого ключа електронного підпису. За допомогою алгоритму ECDSA (Elliptic Curve Digital) власник облікового запису здійснює генерацію пари ключів для електронного підпису. Змінювати стан цього аккаунта можуть тільки підписані цим ключем транзакції. Аккаунт smart-контракту управляється за допомогою попередньо заданого програмного коду. За допомогою нього визначається поведінка smart-контракту, наприклад як розпоряджатися своїми монетами при настанні певних умов, з ініціативи якого користувача, за яких додаткових умов монети будуть поширюватися. Можуть виникнути проблеми, якщо розробники в коді не передбачили цих умов, або не всі умови прописали. Наприклад, можуть відбутися певні обставини, при яких контракт не приймає ініціювання подальшого виконання від жодного з користувачів. В такому випадку монети не можна буде використовувати, якщо в контракті не передбачено виходу контракту із цього стану. Отже, Blockchain є сучасною прогресивною технологією яка може допомогти вирішити велику кількість завдань в страховій галузі. Її використання зможе допомогти усунути посередників, знизивши кількість ресурсів необхідних для оплати їх послуг. Скоротити кількість друкованих документів, зменшити витрати потрібні для обслуговування клієнтів, покращити рівень їх обслуговування, попередити можливі випадки шахрайства, використовувати для однорангового страхування.

У доповіді буде розглянуто типи аккаунтів в Ethereum, класифікацію smart-контрактів, представлено добірку блокчейн-платформ для розміщення smart-контрактів, описано їх переваги та недоліки, розглянуто мови програмування, які вони підтримують. Також буде здійснено огляд завдань, для яких можна використати технологію, структуру smart-контракту в Solidity, детально представлено процес створення smart-контракту на Ethereum в середовищі Remix. Буде представлено приклад практичної реалізації smart-контракту, який підходить для будь-якої страхової компанії. З його допомогою можна буде зберігати дані страхового контракту та страхових ризиків. Також, буде представлено роботу smart-контракту на прикладі оплати відшкодування за застрахований автомобіль по програмі страхування КАСКО. При потребі smart-контракт може бути адаптований під інші види страхування, залежно від потреб компанії.

Література

1. Введение в смарт-контракты [Електронний ресурс] // habr. – 406. – Режим доступу до ресурсу: <https://habr.com/company/distributedlab/blog/413231/>.
2. Ethereum [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: <https://www.ethereum.org/>.