УДК 004.056

Лаврик В.Ю.

ВИКОРИСТАННЯ СМАРТ-КОНТРАКТІВ

Анотація

Робота присвячена використанню смарт контрактів в повсякденному житті людей. Проведено аналіз смарт-контрактів, його створення та плюси і мінуси його впровадження в повсякденне життя людини.

Ключові слова: *смарт-контракт, блокчейн, Біткоін, Ethereum, Solidity.*

Annotation

The work is devoted to the use of smart contracts in people's daily lives. An analysis of smart contracts, its creation and the pros and cons of its implementation in everyday life.

Keywords: *smart contract, blockchain, Bitcoin, Ethereum, Solidity.*

Вступ

З розвитком системи блокчейн, все більше компаній зацікавлені в можливостях, які надає нова технологія. Одним з найбільш перспективних вважається використання смарт-контрактів - алгоритмів, які забезпечують автоматичне виконання умов комерційних угод. Смарт-контракт - це комп'ютерний аналог звичайних договорів[1], спеціальна програма (алгоритм), яка виконує якісь дії при виконанні сторонами угоди певних умов, наприклад, відправляє гроші продавцю при поставці товару покупцеві належної якості. Smart-contracts надають можливість безпечно обмінюватися криптовалютами, грошима, цінними паперами, ресурсами в іграх, а також іншими товарами і послугами безпосередньо між учасниками угоди, без участі посередників. Для покращення роботи смарт-контрактів в данний час пропонується використовувати сайти для перевірки контракту на цілістність, або ж штучних інтелектів, які зменшують вплив людини.

Результати досліджень

Смарт-контракти були вперше запропоновані на початку 1990-х років Ніком Сабо, який і ввів цей термін[1]. Відомий криптограф використовував його для позначення «набору обіцянок, зазначених у цифровій формі, включаючи протоколи, в яких сторони виконують ці обіцянки». Пізніше, у 1998 році цей термін був використаний для опису об’єктів на рівні служби управління правами системи The Stanford Infobus[2], яка була частиною Стенфордського проекту цифрової бібліотеки.

У 2014 році Віталік Бутерін, співзасновник платформи Ethereum, запропонував власну ідею щодо вдосконалення мережі Bitcoin. І вже за рік був запущений сам Ethereum, який є платформою для впровадження цих самих удосконалень і дозволяє створювати автономні смарт-контракти.

Існує помилкове переконання, що технологія смарт контрактів існують тільки в Ethereum. Це не правда. У Bitcoin з самого початку в 2009 році була досить велика смарт-контрактна мова під назвою Script[3]. Фактично, смарт-договори існували до Bitcoin. Різниця між мовою контракту Bitcoin і Ethereum полягає в тому, що Ethereum використовує Turing-повноту. Тобто, Solidity (мова розумних контрактів ETH) дозволяє складати більш складні угоди за рахунок пригнічення їх аналізу.

Елементами «розумного» контракту є:

▪ Сторони угоди, що мають цифровий підпис, які погоджуються або відмовляються від відповідності товару або послуги висунутим раніше вимогам

▪ Предмет договору - товар або послуги, які будуть відправлені в обмін на грошові кошти

▪ Умови, при дотриманні яких буде проведений автоматичний обмін благами, наприклад, відповідність поставленого товару стандартам якості. Повинні мати повний математичний опис

▪ Децентралізована платформа, в якій написаний алгоритм (програмний код) самого смарт-контракту

Як у будь-якої технології, у смарт-контрактів є як переваги, так і недоліки.

Переваги:

▪ Економія часу і ресурсів

▪ Більш низькі витрати, так як немає потреби в послугах посередників

▪ Додаткова безпека від використання блокчейна

▪ Більш швидка перевірка умов виконання контракту

Недоліки:

▪ Чи можуть бути помилки і вразливі місця в програмному коді смарт-контракту. Так, внаслідок хакерської атаки на проект «The DAO» в липні 2016 року зловмисникам вдалося вивести з системи 64 млн. доларів[4].

▪ Складність в побудові алгоритму коду, так як потрібно передбачити всі можливі варіанти розвитку подій

▪ Є ймовірність втрати ключів доступу або паролів до смарт-контракту сторонами угоди

▪ Система сприймає умови контракту з точністю, без урахування форс-мажорів

▪ Нема законодавчої бази використання смарт-контрактів

Але всі ці недоліки не такі суттєві. Адже ймовірність втрати ключів чи форс-мажорні ситуації є більше людським фактором. І для усунення таких помилок пропонується використовувавти більше блокових тестів для контрактів, або перевірки на якихось веб-ресурсах. Тому, можна впевнено говорити що переваг у смарт-контрактів більше і їх поширення варто прогнозувати в майбутньому.

Висновок

Із отриманих результатів дослідження, можна зробити висновки, що використання смарт-контрактів є великим кроком вперед для розвитку людства. Використання контрактів, в майбутньому, буде невід'ємною складовою для будь-якого процесу, починаючи від юридичних фірм завершуючи іграми на телефон чи комп'ютер. Це полегшить роботу в багатьох напрямках і прискорить використання блокчейну урядами країн та компаніями.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Nick Szabo. Smart Contracts. 1994. URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (accessed 19.05.2022)

2. Martin Röscheisen, Michelle Baldonado, Kevin Chang, Luis Gravano, Steven Ketchpel, Andreas Paepcke The Stanford InfoBus and Its Service Layers. Stanford, August 8, 1997. 28 p. URL: http://ilpubs.stanford.edu:8090/318/1/1998-25.pdf (accessed 19.05.2022)

3.Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. 9 p. URL: https://bitcoin.org/bitcoin.pdf (accessed 19.05.2022)

4. Cryptopedia Staff. What Was The DAO? March 16, 2022. URL: https://www.gemini.com/cryptopedia/the-dao-hack-makerdao#section-the-dao-hack-remedy-forks-ethereum (accessed 19.05.2022)

Лаврик Владислав Юрійович – студент групи 1БС-18б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: lavrikvlad0107@gmail.com

Баришев Юрій Володимирович – к.т.н., доцент кафедри захисту інформації факультету інформаційних технологій та комп'ютерної інженерії. Вінницький національний технічний університет.

Vladyslav Lavryk *- student of group 1BS-18b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: lavrikvlad0107@gmail.com*

Yurii Baryshev *— PhD (Eng), Associated Professor of the Department of Information Protection, Faculty of Information Technologies and Computer Engineering. Vinnytsia National Technical University.*