УДК 004.056

Лоборчук А.М.
Баришев Ю.В.

Телеграм-бот для моніторингу подій смарт-контракту

Вінницький національний технічний університет

Анотація

У даній роботі було розглянуто технології Blockchain, смарт-контракт. Розглянуто переваги та недоліки смарт-контрактів та їхні можливі варіанти використання.

Ключові слова: криптовалюта, Blockchain, смарт-контракт.

Abstract

In this paper, Blockchain technology, a smart contract, was considered. The advantages and disadvantages of smart contracts and their possible uses are considered.

Keywords: cryptocurrency, Blockchain, smart contract.

В 2021 році напевно немає таких людей, які б не чули про криптовалюту. Хвиля популярності почалася в 2017 році з криптовалюти Bitcoin, яка і на даний час показує тенденцію росту. Криптовалюти працюють на технології Blockchain, яка вперше була описана в 1991 році Stuart Haber і W. Scott Stornetta в статті "How to Time-Stamp a Digital Document"[1], а для криптовалюти вперше було описано та реалізовано в 2008 та 2009 році Satoshi Nakamoto. З того часу технологія розвивається та надає нові можливості.

Її основою є відкритість даних, та розподіленість їх, тобто всі учасники Blockchain мають однакову інформацію, і вона повністю відкрита. Саме це забезпечує захист від маніпуляцій, оскільки якщо певний учасник змінить щось в себе або декількох учасників то ці зміни просто відкинуться, використовується правило більшості. Тобто буде так як сказала більшість, те що відхиляється від більшості не є істиною, але через це можлива така атака як 50%+, а сама коли зловмисники мають в своїх ресурсах більше 50% учасників. Організувати таку атаку тяжко, або ж навіть не можливо, оскільки учасників буває на стільки багато, що це вимагатиме дуже багато ресурсів.

Словосполучення «смарт-контракт» було придумано Nick Szabo в 1996 році. Він описував його так:

“New institutions, and new ways to formalize the relationships that make up these institutions, are now made possible by the digital revolution. I call these new contracts «smart», because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied. A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises”[2].

Смарт-контракт - це програма про яку знають всі учасники технології, тобто його код видно усім, що звичайно іноді може призвести до проблем, оскільки учасники можуть використати вразливості цього смарт-контракту. Звичайно якщо не допускати помилок при написанні смарт-контракту, то він буде захищений на рівні технології Blockchain. Його мета – укладення й підтримка поетапного виконання контрактів.

Оскільки смарт-контракт - це програма(алгоритм), він як і звичайна програма може виконувати певні функції заложені в нього, зберігати данні.

Якщо пошукати варіанти використання смарт-контрактів в Інтернеті, то можна побачити досить велику їхню кількість, але більша частина не можлива на даний момент, говориться наприклад про використання смарт-контрактів як заміну звичайним контрактам чи договорам. Такі варіанти поки що відкидаються, оскільки смарт-контракти ніяк законодавчо не зазначені, тобто не несуть ніякого значення з точки зору закону. Одним з варіантів є використання смарт-контрактів для того щоб люди могли отримати певну інформацію з нього (занесену раніше), що досить легко. Наприклад, ставки на аукціонах є відкритими, тому таке використання можливе, так усі будуть знати хто скільки, коли поставив, яка ціна товару на даний момент і так далі. Є варіант з використанням смарт-контрактів в іграх. В ігри грають мільйони людей, також часто люди вкладають в них досить великі суми, тому

їхні ігрові аккаунти несуть велику цінність. Використовуючи смарт-контракти заносяться дані в Blockchain, які вже не зміниш, і не очистиш.

Переваги та недоліки смарт-контрактів є досить багато. Недоліки:

−слабке регулювання. Немає певної системи, яка могла б дозволити смарт-контрактам стати повноцінним інструментом. Це не юридичний документ, він не має сили. Держава не визнає смарт-контракт як повноцінний договір (немає законодавчого регулювання).

−помилки, вразливості, баги. Якщо контракт був написаний неправильно, змінити його не можливо, доведеться створювати новий. Також знадобиться проводити тестування, для забезпечення надійності.

−повільна робота. Дані обробляються досить довго.

Переваги:

−Надійність та відкритість інформації. Як було сказано вище, смарт-контракти працюють в технології Blockchain, це публічність, яка потрібна багатьом фінансовим сферам, а також дані зберігаються на безлічі комп'ютерів відразу, тому знищити їх просто неможливо(тяжко, багато затратно).

−економія грошей і часу. Немає посередників, що економить кошти, комісія що сплачується в системі досить низька.

−точність. При написанні контрактів практично виключається людський фактор. Можлива помилка програміста, але його роботу можливо проконтролювати в тестовій версії.

На даний час смарт-контракти мають як мінуси так і плюси. Не виключено, що в майбутньому смарт-контракти досягнуто точки, де вони дійсно замінять звичайні нам речі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. How to Time-Stamp a Digital Document / Stuart Haber, W. Scott Stornetta, Springer-Verlag Berlin Heidelberg, 1991. 455 p. URL: https://link.springer.com/content/pdf/10.1007%2F3-540-38424-3_32.pdf.

2. Smart Contracts: Building Blocks for Digital Markets // fon.hum.uva : веб-сайт. URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

3. Blockchain Tree as Solution for Distributed Storage of Personal ID Data and Document Access Control // DOI: веб-сайт. URL: https://doi.org/10.3390/s20133621 (дата звернення: 01.03.2021).

4. АНАЛІЗ СТІЙКОСТІ ТЕХНОЛОГІЇ БЛОКЧЕЙН НА ПРИКЛАДІ РЕАЛІЗАЦІЙ BITCOIN ТА ETHEREUM / Ю. В. Баришев. URL: http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/20535/4351.pdf?sequence=3 (дата звернення: 01.03.2021).

Лоборчук Андрій Михайлович — *факультет інформаційних технологій та комп'ютерної інженері, Вінницький національний технічний університет, Вінниця, e-mail: loborchuka@gmail.com*

Баришев Юрій Володимирович — канд. техн. наук, *доцент кафедра захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: yuriy.baryshev@vntu.edu.ua*

Loborchuk Andriy Mykhailovych - *Faculty of Information Technologies and Computer Engineer, Vinnytsia National Technical University, Vinnytsia, e-mail: loborchuka@gmail.com*

Baryshev Yurii Volodymyrovych - *Cand. Sc., Associate Professor, Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: yuriy.baryshev@vntu.edu.ua*