УДК 004.056

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ СТЕГАНОГРАФИИ В ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ РЕШЕНИЯ ЗАДАЧ ЗАЩИТЫ ИНФОРМАЦИИ

Федосенко М.Ю. (Университет ИТМО)
Научный руководитель – профессор, доктор технических наук, Беззатеев С.В.
(Университет ИТМО)

Введение. В настоящее время технология блокчейн активно развивается. Производственная сфера осуществляет разработки блокчейн для решения оптимизационных задачи и обеспечения дополнительной защитой. Научная сфера активно исследует отрасль с целью найти новые сферы применения блокчейн и расширить возможности имеющихся. Одним из направлений научного поиска является совместное использования блокчейн и стеганографии, имеющей схожести с криптографией, однако отличающейся от неё принципиальным подходом. В данной работе будут рассмотрены возможные способы использования стеганографии в технологии блокчейн а также применения блокчейн в качестве стеганографического метода, выдвинуты новые идеи для реализации совместного использования данных технологий.

Основная часть. Стеганография отличается от криптографии тем, что скрывает сам факт наличия защищаемой информации. В то время, алгоритмы хеширования, являющиеся разновидностью криптографических алгоритмов, имеют особенность, заключающуюся в одностороннем преобразовании защищаемой информации. Получаемая в итоге хэш-сумма позволяет проводить различные манипуляции с информацией, такие как сравнение, удостоверение её подлинности и целостности без самого раскрытия сути этой информацией. Ключевым условием для получения хэш-значения и последующего его использования, помимо необратимости преобразования, является невозможность однозначно установить зависимость оригинальных данных о хэша, а также выявить закономерность изменения хэш-суммы от изменения информации. Всё это активно применяется в технологии блокчейн для защиты блоков данных и идентификации их оригинальности, сокращает количество возможных успешных атак на данную систему.

Однако, блокчейн имеет свои уязвимости, которые как зависят от особенностей ресурсов, на которых развёрнут реестр (отказоустойчивость серверов, уязвимости программного кода), так и от самой технологии (атака 51%, атаки на коллизию хэша). Это не делает распределённые реестры абсолютно защищёнными и устойчивыми. В тоже время, стеганография также используется для решения задач защиты информации, позволяет удостоверять подлинность и целостность данных за счёт цифровых водяных знаков (ЦВЗ), осуществлять защищённый обмен информации в каналах связи. Отсюда, идеей данной работы является поиск возможностей совместного использования блокчейн и стеганографии в целях защиты информации. Работы над вопросом стыка данных областей начались сравнительно недавно. Однако, уже имеются идеи, концепты, реализации в научных сообществах.

Учёные из БГТУ [1] в своей работе предложили использование хэш-значений, передаваемых в протоколах блокчейн в качестве стеганоконтейнера. В другой работе Мохсин и др. [2] предложили произвести незначительные изменения в алгоритме оптимизации роя частиц (PSO) для защиты и безопасной передачи данных о COVID-19 через технологию блокчейн. Basuki и Rosiyadi [3] в своём исследовании успешно разработали защищенную систему передачи данных с использованием метода стеганографии транзакций и стеганографии изображений. Еще один исследователь рассматриваемой проблемы Партала [4] предложил концепт системы, использующей наименьший значащий бит (LSB) в блокчейн. Интересный в рамках данной работы концепт предложили Хорнг и др. [5]. Они зашифровали покрывающие изображения используя перестановку блоков в системе блокчейн.

Выводы. Таким образом, на сегодняшний день, в научном сообществе уже активно ведутся исследования возможностей практического совмещений понятий «блокчейн» и «стеганография». Имеются как выдвинутые теории по совместному использованию, так и реализованные концепты, основные из которых являются следующие идеи:

1. Использование блокчейн технологии в качестве стеганографического алгоритма
2. Использование блокчейн технологии в качестве среды обмена стеганографическими вложениями
3. Использование стеганографии для дополнительной защиты информации в блокчейн системе
4. Комбинированное использования подходов.

Произведённый в работе научный поиск доказал актуальность проведения исследований в данной области как с целью выявления новых подходов в защите информации, так и для развитие распределённых технологий. В дальнейшем, на основе данного литературного обзора будет осуществляться поиск ответов на вопросы каким образом реализовать стеганографическую систему на блокчейн, как защитить информацию в блоках при помощи ЦВЗ, использование каких технологий, их особенностей, конкретных алгоритмов и значений необходимо для успешной практической реализации данной системы.

Список использованных источников:

1. Информационные технологии : материалы 84-й науч.-техн. конференции профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 3-15 февраля 2020 года [Электронный ресурс] / отв. за издание И.В. Войтов; УО БГТУ. – Минск : БГТУ, 2020. – 285
2. Mohsin, A.H.; Zaidan, A.A.; Zaidan, B.B.; Mohammed, K.I.; Albahri, O.S.; Albahri, A.S.; Alsalem, M.A. PSO–Blockchain-Based Image Steganography: Towards a New Method to Secure Updating and Sharing COVID-19 Data in Decentralised Hospitals Intelligence Architecture. Multimed. Tools Appl. 2021, 80, 14137–14161.
3. Basuki, A.I.; Rosiyadi, D. Joint Transaction-Image Steganography for High Capacity Covert Communication. In Proceedings of the 2019 International Conference on Computer, Control, Informatics and its Applications (IC3INA), Tangerang, Indonesia, 23–24 October 2019; pp. 41–46.
4. Partala, J. Provably Secure Covert Communication on Blockchain. Cryptography 2018, 2, 18.
5. Horng, J.H.; Chang, C.C.; Li, G.L.; Lee,W.K.; Hwang, S.O. Blockchain-Based Reversible Data Hiding for Securing Medical Images. J. Healthc. Eng. 2021, 2021.

Федосенко М.Ю. (автор) Подпись

Беззатеев С.В. (научный руководитель) Подпись