УДК 681.3.06

А.А. Гаврилова, Р.М. Королев

alla.gavrylova@hneu.net, korolevrv01@ukr.net

Харьковский национальный экономический университет имени Семена Кузнеца, Харьков

АНАЛИЗ УЯЗВИМОСТЕЙ ТЕХНОЛОГИИ БЛОКЧЕЙН ПРИ РАБОТЕ С КРИПТОВАЛЮТАМИ

На сегодня использование блокчейн технологии имеет двойственный характер являясь одновременно перспективным многообещающим направлением и таящим в себе опасности как уже известные, так неизвестные. Самым популярным приложением данной технологии является работа с криптовалютой, что предполагает необходимость повышенного внимания к вопросам безопасности проходящих транзакций. Поэтому в работе рассмотрены возможные угрозы и риски, которые могут влиять на проведение процессов майнинга биткоина.

Во время майнинга биткоина решается огромное количество математических задач, которые приводят к зарабатыванию криптовалюты. При этом все прошлые совершенные операции сохраняются в общем доступе. Добытчики биткоина подбирают нужный хеш из различных комбинаций, который дает доступ к секретным ключам и к новым операциям. Весь этот сложный математический процесс требует наличия мощного специального устройства, которое поможет в минимальные сроки подобрать нужный хеш. Этим обосновывается положительная тенденция хешрейта [1] биткоина, которая наблюдалась с 2018 года и на конец 2019 года показал рост на 140% [2], свидетельствует также о достаточно высокой степени защищенности блокчейна от взлома [3]. Существует мнение, что транзакции криптовалют защищены, а схемы шифрования с открытым ключом почти невозможно взломать, но есть ряд уязвимостей, методы решения для которых приведены в табл. 1.

Таблица 1

Уязвимости и методы их решения

№ п/п	Уязвимость	Решения
1	хранения ключей	Использовать решения на основе Public Key Infrastructure (PKI): доверенный платформенный мо дуль (TPM); физически неклони руемые функции (PUF)
2	хищения ключей при помощи ме-тодов социа-льной инженерии	Совершенствовать процедуры конт роля, развитие критичности мыш ления, психологической устойчи вости, проницательности [4]
3	среды разработки	Использовать средства стати-ческого тестирования защищен-ности приложений (SAST)
4	в IT-архитектуре системы	Избавляться от неактуального программного обеспечения; Регуля рно устанавливать обновления на ПО; контролировать ИТ-инфрастру ктуру на предмет открытых портов, наличия мер защиты, регулярно менять пароли, контролировать полномочия пользователей
5	появления квантовых компьютеров	Использование математической модели, основанной на схеме Мак-Элиса гибридных модифицирован-ных эллиптических ко-дах (MEC) для кодирования и декодирования информации с использованием модифицированного алгоритма UMAC при передаче и получении открытого сообщения по каналам связи [5]
6	опасной “атаки-51”	Повышение хеш мощности биткоина

Отдельного внимания заслуживает уязвимость, связанная с применением полномасштабных квантовых компьютеров. В связи с этим в будущем будет возрастать возможность взлома используемых ныне относительно криптостойких алгоритмов SHA-класса (SHA-1, SHA-2, SHA-3) а также алгоритма RIPEMD, который используется в биткоинах и других криптовалютах на основе биткоинов. В процессе реализации предлагаемой модели предусмотрена двойная верификация, которая позволяет обеспечить высокий уровень целостности и достоверности передаваемого сообщения, а также высокий уровень быстродействия и криптостойкости хеш-кода в условиях пост-квантовой криптографии.

Список литературы

[1] Blockchain. Com [Online]. Available: https://www. Bloc kchain.com/ru/charts/hash-rate. Accessed on: Febr. 29, 2020.

[2] Лола Степанова, Вычислительная мощность сети биткоина достигла исторического максимума 74,5 млн. терра-хеш/сек. [Электронный ресурс]. Доступно: https:// hashtelegraph.com /vychislitelnaja-moshhnost-seti-bitkoina-dostiglastoricheskogo -maksimuma-745-mln-teraheshsek/. Дата обращения: Febr. 29, 2020.

[3] Биткоин: сетевая активность опережает рост цены [Электронный ресурс]. Доступно: https://altstake.io/news/ bitkoinsetevaya-aktivnostyopereghaet-rost-ceny. Дата обраще ния: Mar. 01, 2020.

[4] Константин Ценцура, Три убийственных проблемы блокчейна. [Электронный ресурс]. Доступно: https: //nv.ua/ techno/techno blogstri-ubiystvennyh-problemy-blokchejna-246 5554.html Дата обращения: Apr. 21, 2018.

[5] Alla A. Havrylova, Olha H. Korol, Stanyslav V. Milevskyi, and Lala R. Bakirova, "Mathematical model of authentication of a transmitted message based on a McEliece scheme on shorted and extended modified elliptic codes using UMAC modified algorithm", Кібербезпека: освіта, наука, техніка, No 1(5), p. 40 – 51, 2019.