УДК 004.75

АБСТРАКЦИИ УЧЕТНЫХ ЗАПИСЕЙ В УПРАВЛЕНИИ УСТРОЙСТВАМИ ИНТЕРНЕТА ВЕЩЕЙ

Гаврилов С.О. (ИТМО)
Научный руководитель - к.ф.-м.н., доцент практики Ромакина О. М. (ИТМО)

Введение. Применение технологии блокчейн помогает посмотреть на решение привычных задач под другим углом. Она может применяться в распределенных реестрах (сфера управления данными, анализ данных и тестирование), идентификации и подтверждении прав доступа, для криптографической защиты децентрализованных платформ, построения анонимных и прозрачных платформ (для голосования), хранение идентификационных данных физических предметов для разработки киберфизических систем, в том числе, программного обеспечения для интернет вещей. В данной работе мы рассмотрим проблему сохранности средств в проекте по повышению эффективности и безопасности цепочек поставок с применением концепции интеграции устройств интернета вещей с технологией блокчейн.

Основная часть. Концепция проекта направлена на предоставление IoT-устройствам возможности автономно подписывать транзакции в блокчейне, используя аутентифицированные приватные ключи IoT-устройств закрытых ключей, устраняя необходимость во внешних кошельках. Для обеспечения целостности передаваемой информации, устройство интернета вещей должно единолично распоряжаться приватным ключом для подписания отправляемых транзакций [1]. В то же время, устройству интернета вещей необходимы средства для оплаты комиссии сети за отправляемые транзакции. Указанные средства предоставляет менеджер устройства. Однако, в случае поломки или потери устройства, неизрасходованные средства безвозвратно утрачиваются. В данной работе исследуется инструмент абстракции учетных записей для предотвращения потерь средств в указанных случаях.

Рассмотрим несколько путей решения поставленной задачи. Используя логику работы смарт-контракта, мы можем прописать условие: если устройство не подписывало транзакций в течении установленного времени или если у устройства был отозван сертификат, то монеты автоматически возвращаются на кошелек, с которого они были получены. Но вышедшее из строя устройство не сможет подписать данную транзакцию.

Альтернативным вариантом является хранение большей части монет на смарт контракте. Устройство будет брать монеты с него небольшими частями, но таким образом задачу мы полностью не решим, потому что баланс всё же должен быть не нулевым, и в случае внезапного прекращения физического существования устройства мы всё равно потеряем монеты.

Рассмотрим стандарт ERC-4337, описанную в нём парадигму account abstraction и то как её можно использовать, для ухода от оплаты комиссии самим устройством.

Стандарт ERC-4337 — это стандарт токенов абстракции учетной записи, который раскрывает возможности криптокошельков со смарт-контрактами в блокчейне Ethereum [2].

Предложение по абстракции учетной записи исключает необходимость изменения протокола уровня консенсуса. Вместо добавления новых функций протокола и изменения типа транзакции нижнего уровня в этом предложении вводится объект псевдотранзакции более высокого уровня, называемый UserOperation. Пользователи отправляют UserOperation объекты в отдельную комнату ожидания (mempool). Специальный класс, называемый bundle, упаковывает набор этих объектов в транзакцию, вызывающую handleOps специальный контракт, и эта транзакция затем включается в блок [3].

Одним из наиболее привлекательных и инновационных аспектов ERC-4337 для дальнейшего исследования и применения, является опциональный элемент именуемый, Paymaster, а именно возможность хранить на его счету монеты и оплачивать комиссии вместо самих устройств. В контексте проекта, описанного выше, Paymaster представляет собой решение для обработки транзакций и обеспечения устойчивости в среде интернета вещей (IoT).

Выводы. Исследование показало, что Paymaster, как сущность ERC-4337, может эффективно управлять хранением монет и осуществлять оплату комиссий за транзакции, связанные с внесением данных в блокчейн. Это предоставляет устройствам IoT надежный механизм для оплаты за транзакции, что может решить существующую проблему потери средств при выходе устройства из строя.

Список использованных источников:

1. Yash Madhwal, Yury Yanovich, S. Balachander, K. Harshini Poojaa, R. Saranya, B. Subashini. Enhancing Supply Chain Efficiency and Security: A Proof of Concept for IoT Device Integration With Blockchain // IEEE Access. - 2023. - №Digital Object Identifier 10.1109/ACCESS.2023.3328569. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10299623.

2. AcademyBinance. (4337). https://academy.binance.com/ru/articles/what-is-erc-4337-or-account-abstraction-for-ethereum.

3. ERC-4337: Account Abstraction Using Alt Mempool. https://eips.ethereum.org/EIPS/eip-4337#abstract.