Смарт-контракты и вопросы безопасности

Александр Подобных, *CISA, эксперт по кибербезопасности инфраструктуры блокчейнов и противодействию мошенничеству в сфере оборота криптовалют, член АРСИБ*

Смарт-контракт — это приложение, использующее блокчейн и выступающее в качестве цифрового соглашения, подкрепляемого набором правил. Смарт-контракты не являются договорами в юридическом смысле в большинстве юрисдикций, включая российскую. Это всего лишь приложение, удовлетворяющее формальным требованиям и запущенное в распределенной системе блокчейна. Смарт-контракты делают транзакции отслеживаемыми, прозрачными и необратимыми. Результатом выполнения контракта может быть обмен активами между сторонами[1].

Смарт-контракты позволяют создавать протоколы коммуникации, не требующие априорного доверия между сторонами.

Одна из причин, провоцирующих уязвимости, заключается в сложности проектирования, разработки и тестирования смарт-контрактов.

Смарт-контракты имеют обширную область применения не только в финансовом секторе, но и в иных отраслях экономики, и мировой тренд на цифровизацию является одним из основополагающих драйверов развития этого инструмента[2].

Смарт-контракты позволяют создавать протоколы коммуникации, не требующие априорного доверия между сторонами. Участники процесса могут быть уверены, что контракт будет выполнен только при соблюдении всех условий, в нем предусмотренных. Кроме того, использование смарт-контрактов избавляет от необходимости в посредниках, значительно снижая расходы на проведение операций.

Каждый блокчейн может использовать собственный способ реализации смарт-контрактов. Например, в сети Ethereum для написания смарт-контрактов используется язык Solidity. С точки зрения разработчика, Solidity легко читается практически любым программистом и на первых шагах обманчиво кажется простым.

Кроме кода, смарт-контракты содержат два публичных ключа, один из которых предоставлен создателем контракта, а другой является цифровым идентификатором, уникальным для каждого смарт-контракта.

Неизменность смарт-контрактов

Поскольку смарт-контракты работают в рамках неизменяемой децентрализованной блокчейн-сети, их результаты нельзя подделать ради неправомерного извлечения выгоды. Но неизменность является не только достоинством, но и недостатком. Например, в 2016 г. хакеры взломали децентрализованную автономную организацию The DAO и украли эфиры (валюта сети Ethereum) на миллионы долларов, воспользовавшись уязвимостями в коде смарт-контракта. Поскольку смарт-контракт The DAO был неизменным, разработчики не смогли исправить код.

В результате сеть Ethereum приняла решение откатить ситуацию до момента взлома, вернуть средства законным владельцам, и этот форк является частью текущего блокчейна Ethereum. В то время как оригинальная цепочка, получившая название Ethereum Classic, никак не отреагировала на взлом, руководствуясь тем, что события в блокчейне никогда не должны изменяться.

Высокая зависимость от уровня программистов и подверженность багам

Считается, что взлом злоумышленниками качественно написанных смарт-контрактов практически невозможен, а популярные смарт-контракты в индустрии децентрализованных финансов на сегодняшний день являются самым надежным способом хранения документов в цифровом мире.

Но код пишется программистами, а из-за того, что смарт-контракт виден всем пользователям блокчейна, в рамках которого он функционирует, его возможные уязвимости будут видны всей сети, притом что устранить их не всегда возможно из-за неизменности.

В идеальном мире разработка смарт-контрактов должна осуществляться только опытными программистами, особенно когда речь идет о конфиденциальной

Рис 1. Торговое финансирование на основе смарт-контрактов

[1] *При написании статьи использовались материалы https://academy.binance.com/ru/articles/what-is-a-smart-contract-security-audit*
[2] *https://cbr.ru/Content/Document/File/47862/SmartKontrakt_18-10.pdf*