информации, персональных данных или больших суммах денег.

Но в реальности очень большой процент ошибок вызван человеческим фактором и уязвимый код является причиной многочисленных рисков. Одна из причин, провоцирующих уязвимости, заключается в сложности проектирования, разработки и тестирования смарт-контрактов. И если для простых смарт-контрактов вероятность ошибки относительно мала, то в сложных смарт-контрактах ошибки встречаются часто. А последствием может быть хищение средств, их заморозка или даже уничтожение смарт-контракта.

Распространенные уязвимости вызваны давно известными чисто программными ошибками.

1. Рекурсивный вызов: смарт-контракт совершает вызов к другому внешнему контракту до того, как изменения были зафиксированы. После этого внешний контракт может рекурсивно взаимодействовать с исходным смарт-контрактом недопустимым способом, так как его баланс еще не обновлен.

2. Целочисленное переполнение: смарт-контракт выполняет арифметическую операцию, но значение превышает емкость хранилища (обычно 18 знаков после запятой). Это может привести к неправильному расчету сумм.

3. Опережение: плохо структурированный код содержит данные о будущих транзакциях, которые могут быть использованы третьими лицами в своих интересах.

Эффективность смарт-контрактов

Оптимизация производительности смарт-контрактов является показателем мастерства разработчика. Некоторые контракты для выполнения своей функции производят сложные серии транзакций, и комиссия за производимые операции становится высокой. Эффективные контракты могут значительно сократить комиссию за транзакции.

Вопрос комиссии за вычисления в смарт-контрактах тесно связан с безопасностью, ведь ситуация, когда средства навсегда застряли в контракте, с практической точки зрения мало отличается от ситуации, когда их украли.

Виртуальная машина Ethereum

EVM (Ethereum Virtual Machine) – это единый глобальный 256-битный "компьютер", в котором все транзакции хранятся локально на каждом узле сети и исполняются с относительной синхронностью.

EVM может выполнять произвольные команды, и в этом кроется его уязвимость: можно подобрать программный код, который приведет к непредвиденным последствиям. Понятно, что уязвимости в EVM могут привести к сбою в работе смарт-контрактов.

Еще одна проблема заключается в том, что можно практическим либо техническим способом подобрать код смарт-контракта, операции которого нагрузят виртуальную машину и замедлят ее непропорционально той комиссии, которая была оплачена за выполнение этих операций. Исследователи борются с такого рода злоупотреблениями, но проблема по-прежнему остается актуальной.

Аудит защищенности смарт-контрактов

В качестве ответной меры на возможные риски довольно распространенной услугой стал аудит смарт-контрактов.

Аудит безопасности предоставляет подробный анализ смарт-контрактов проекта для защиты вложенных средств. Так как все транзакции в блокчейне являются конечными, вернуть средства в случае кражи невозможно. Единого подхода к аудиту нет, и каждая аудиторская компания выполняет его по своему усмотрению.

Детерминизм исполнения кода смарт-контракта позволяет тестам работать везде, быть крайне простыми в поддержке и делает расследование инцидентов надежным и неоспоримым.

Аудиторы изучают код смарт-контрактов, составляют отчет и предоставляют его команде проекта. Затем выпускается окончательный отчет с подробным описанием всех оставшихся ошибок и работы, проделанной для решения проблем с производительностью и безопасностью. Помимо общих выводов, отчет обычно содержит рекомендации, примеры избыточного кода и полный анализ ошибок кодирования.

Команде проекта дается время, чтобы исправить ошибки, прежде чем будет выпущен окончательный отчет.

Большая часть аудита включает проверку контрактов на наличие уязвимостей в системе безопасности. Хотя некоторые проблемы лежат на поверхности, многие ошибки могут быть устранены только с помощью сложных инструментов и стратегий. Например, слабый смарт-контракт может подвергнуться атаке в сочетании с рыночными манипуляциями. Чтобы обнаружить эти проблемы, аудиторы проводят пентесты.

Аудит безопасности смарт-контрактов широко распространен в экосистеме децентрализованных финансов (DeFi). Решение инвестировать в блокчейн-проект может быть частично основано на результатах проверки кода смарт-контракта.

Заключение

Несомненно, смарт-контракты оказали большое влияние на мир криптовалют и, безусловно, произвели революцию в области блокчейн-технологий. Совместный потенциал смарт-контрактов и блокчейна может оказать значительное влияние практически на все сферы жизни общества. Но только время покажет, смогут ли эти инновационные технологии преодолеть барьеры на пути к широкомасштабному внедрению.

Поскольку транзакции блокчейна необратимы, очень важно убедиться в безопасности кода смарт-контрактов. Особенности технологии "блокчейн" затрудняют возврат средств и решение проблем постфактум, поэтому лучше заранее определить потенциальные уязвимости проектов.

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

Вопрос комиссии за вычисления в смарт-контрактах тесно связан с безопасностью, ведь ситуация, когда средства навсегда застряли в контракте, с практической точки зрения мало отличается от ситуации, когда их украли.

В качестве ответной меры на возможные риски довольно распространенной услугой стал аудит смарт-контрактов.