Захватывающая история The DAO: работа над ошибками

ОБЗОРЫ 17.06.2017

17 июня 2016 года произошла, пожалуй, самая масштабная атака за всю историю криптоиндустрии — из-за ошибки в коде перспективный и очень популярный в то время проект The DAO лишился более 60 миллионов долларов.

Журнал ForkLog решил вспомнить эту дату и попытаться проанализировать, к чему привело это событие.

Немного предыстории

На заре ICO, то есть всего-то около года назад — 28 мая 2016, закончилась распродажа токенов проекта по децентрализованному управлению инвестициями The DAO, который основала команда стартапа Slock.it.

До поры до времени у The DAO дела шли очень хорошо: и сообщество проект полюбило, и Виталик Бутерин стоял за него горой, и краудсейл прошел, мягко говоря, успешно — собрали более 12 миллионов ETH, что на тот момент составляло около 165 миллионов долларов (сегодня — более 4,3 миллиарда долларов!).

13 июня 2016 года, за несколько дней до взлома, журнал Forklog писал:

> ***«за последние сутки The DAO вырос в стоимости почти на 16% по отношению к доллару ($ 0,158) и более чем на 5% по отношению к ETH (0.000228)».*** *(Для справки: биткоин тогда стоил 695 долларов).*

Что-то пошло не так…

Однако буквально за неделю до краха The DAO редакция нашего журнала опубликовала несколько занимательных материалов, которые напрямую рассказывали о возможных уязвимостях проекта. Это «Атаки Влада: обзор основных уязвимостей The DAO»и интервью со Стефаном Туалем, сооснователем и операционным директором стартапа Slock.it, который как раз занимался созданием инвестиционного фонда The DAO.

В разговоре с Туалем годичной давности ForkLog интересовался тем, насколько оправданы опасения сообщества насчет возможных атак на проект. Оценивая содержание этого текста сейчас, можно сказать, что команда Slock.it отнеслась несерьезно и к возможным уязвимостям, и даже к честному разговору о них.

> ***«Я спокоен по поводу будущего The DAO. Все произошедшие события сделали его самым большим проектом в истории, финансируемым за счет краудфандинга, и по сути самым крупным венчурным проектом. The DAO позволит появиться компаниям, которые в ином случае никогда бы не существовали», —*** *заявил 10 июля 2016 года Стефан Туаль.*

В это же время пользователи GitHub и участники проекта забили тревогу по поводу «ужасной атаки на контракты кошельков». К решению этой проблемы подключился и сам Стефан Туаль, который уже на следующий день опубликовал ссылку на фикс и анонсировал серию апгрейдов ПО. Эту уязвимость Туаль назвал «рекурсивным вызовом» — именно она и привела проект The DAO к краху.

Рекурсивный вызов и крах The DAO

Именно столько в пятницу 17 июня в 9 часов утра стоил ETH:

А примерно в полдень стало известно, в чем причина резкого падения цены токена: The DAO атакована, украдено $50 миллионов.

На рынке началась паника. Под горячую руку попали и основатели The DAO, и Виталик Бутерин, и Ethereum. Многие криптоэксперты и члены сообщества хоронили эти проекты прямо в одной могиле. Кульминацией обширной дискуссии вокруг произошедшего стало эпичное появление непосредственно атаковавшего The DAO.

Представим, что после ограбления банка во время разбирательств между полицией и плачущими вкладчиками внезапно появляется человек в маске и говорит: «Спокойно, ребята! Это моих рук дело, но все законно». Вот примерно это и произошло, правда, в онлайн-пространстве: атаковавший написал открытое письмо, в котором не то что не признавал вины, но и грозил судом в случае, если его лишат «награбленного».

> ***«Я внимательно изучил код the DAO и решил поучаствовать после того, как нашел функцию, при запуске которой разделение вознаграждается дополнительными эфирами. Я задействовал данную функцию и законно получил 3 641 694 эфира. Хочу поблагодарить the DAO за эту награду. (…) Я оставляю за собой право принять любые и все возможные легальные действия против любых соучастников незаконных краж, заморозок или изъятия моих законно полученных токенов ETH, и я продолжаю активно работать с моей юридической фирмой. Все эти соучастники в ближайшее время получат соответствующие уведомления на свои почтовые адреса. Я надеюсь, что это событие станет ценным опытом для сообщества Ethereum, которому я желаю всего наилучшего»,*** *— говорилось в письме.*

Однако позже эксперты признали это письмо, достойное того, чтобы войти в историю криптовалют, подделкой. И тем не менее точка в этом вопросе пока не поставлена. Возможно, в будущем мы узнаем удивительные и никому не известные подробности произошедшего 17 июня 2016 года.

Возвращаясь к атаке, нужно напомнить, что кража была совершена как раз из-за уязвимости под названием «рекурсивный вызов» — она позволяла бесконечно снимать средства The DAO и переводить их в дочернее DAO посредством многократного разделения DAO, повторно собирая ETH в рамках одной транзакции.

Однако окно для создания дочернего DAO составляло ровно 27 дней, и средства с кошелька все это время нельзя было вывести. Сообщество начало искать пути «восстановления справедливости» и в конце концов остановилось на во всех смыслах жестком предложении Виталика Бутерина.

Утешительные итоги

Год спустя можно с уверенностью сказать, что атака на The DAO не погубила ничего, кроме непосредственно The DAO, и подарила сообществу Ethereum Classic, вокруг которого собралось пусть и небольшое, но влиятельное сообщество. Взлом The DAO наоборот показал, что криптовалютный мир весьма устойчив к подобным потрясениям, даже в том зачаточном состоянии, которое было год назад.

Хотелось бы отметить, что в самом начале огромного бума ICO, начавшегося после провала The DAO, на Forklog вышел материал под названием «Уроки DAO: куда приводят мечты». Сейчас эти уроки можно назвать основами успешного выбора ICO в качестве инвестиций. Они не потеряли своей актуальности и сейчас, поэтому их можно процитировать целиком.

1. **Внимательно анализируйте ICO.** Важно понимать, что вы покупаете и с какой целью. Жадность и погоня за быстрой наживой рано или поздно приводят к финансовым потерям. Безусловно, даже самые провальные в своей сути криптовалютные проекты в среднесрочной перспективе могут иметь колоссальный спекулятивный потенциал. И если как инвестор вы рассчитываете именно на это, не стоит вкладывать больше денег, чем вы готовы потерять.
2. **Отложенный релиз лучше небезопасного кода.** Разработчики The DAO, по всей видимости, не ожидали такого финансового успеха, и это сделало проект привлекательным не только для инвесторов, но и для злоумышленников. Тем не менее, ничто не мешало на некоторое время заморозить проект, ограничив возможность работы с основным контрактом. И только после проведения тщательного тестирования при поддержке сообщества и специалистов по блокчейну и безопасности — запускать основной функционал проекта. То, с чем мы столкнулись в реальности, — непозволительная халатность программистов. В результате репутация отдельных разработчиков пострадала если не окончательно, то очень сильно.
3. **Здесь львы.** Идеализм и благие намерения, которыми переполнено криптовалютное сообщество, опьяняют и отвлекают от реального положения дел. В то время как количество новых криптовалют и проектов растет почти экспоненциально, пора обратиться к истории фондовых рынков, чтобы не повторять ошибок прошлого.
4. **Эмоции и паника никогда не приводят к конструктивному решению проблемы.**

О том, что произошло после атаки на The DAO, читайте в материале ForkLog, который будет опубликован 20 июля — в день годовщины хардфорка Ethereum.

Tanya Otter

И не забывайте следить за нашими новостями в Twitter, тем более что он теперь стал, как говорят, такой красивый!

Подписаться на новости Forklog

Подписаться

E-mail *

Похожие материалы

- Мнение: Ethereum покидает категорию альткоинов
- Началось публичное бета-тестирование мобильного приложения MetaMask
- Взломанная биржа Bitpoint обнаружила пропажу криптовалют еще на $2,3 млн
- Работа децентрализованной биржи 0x оказалась прервана из-за обнаруженной уязвимости
- Binance снизит число подтверждений для зачисления средств в биткоине и Ethereum
- Пришли в движение украденные с Binance биткоины на сумму более $8 млн
- «Случайный гений» реализовал идею Бутерина о сервисе микширования для Ethereum
- SEC ищет подрядчика для сбора данных из блокчейнов биткоина и Ethereum

Метки #Ethereum, #Slock, #The DAO, #жизнь - боль, #уязвимости, #хакеры

О ПРОЕКТЕ

Журнал ForkLog - информационный ресурс о криптовалютах, блокчейне и децентрализованных технологиях. Мы работаем для вас с 2014 года.

КОНТАКТЫ

ПОДДЕРЖАТЬ ПРОЕКТ