УДК 004.75

УЯЗВИМОСТИ ТЕХНОЛОГИИ БЛОКЧЕЙН: АТАКИ И НЕГАТИВНЫЕ ВОЗДЕЙСТВИЯ

Автор: Д.В. Ямщиков (Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», г. Санкт-Петербург).

Научный руководитель: к.т.н., доцент Н.А. Осипов (Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», г. Санкт-Петербург).

Основные уязвимости технологии Блокчейн целесообразно проанализировать на примере самого известного проекта, построенного на базе рассматриваемой технологии – на примере платежной системы Биткойн. Являясь правительственно нерегулируемой, децентрализованной и не связанной с экономикой какой-либо страны, данная платежная система часто подвергается попыткам осуществления негативного воздействия, проведению атакам со стороны злоумышленников, целью которых является получение дохода или попытка разрушения «непреступной» концепции технологии Блокчейн.

Поскольку система Биткойн не несет и не может нести ответственность за небезопасное хранение криптовалют, ключей доступа и ненадлежащую работу криптобирж, то к одной из основных причин блокчейн-угроз можно отнести невнимательность людей к крипто-безопасности и легкомысленный подход к организации работы с платформой. Для сокращения негативных воздействий мошенников и количества удачных атак на систему, необходимо проанализировать источники воздействия злоумышленников и вектор их направленности.

В докладе подробно рассматриваются негативные влияния, ставящие под угрозу вопросы безопасности технологии Блокчейн. Так, основные из них можно условно сгруппировать следующим образом по объекту их воздействия:

1. Воздействие на уровне сети:
   – DDoS-атака или атака типа «отказ в обслуживании» – путем заражения компьютеров сети и передачи необходимых данных злоумышленникам;
   – «атака Сивиллы» – с целью нарушения работы всей сети путем присваивания одной ноде нескольких идентификаторов;
   – «атака информационного затмения» или Eclipse attack – путем получения конроля над доступом к нодам и изменению поведения их контакта с другими зараженными узлами.
2. Воздействие на уровне пользователя:
   – использование ботнетов – с целью завладения ресурсами компьютера;
   – деанонимизация участников рынка – с целью отслеживания источников осуществления транзакций.
3. Воздействие на уровне майнинга:
   – «Атака 51%» – путем получения контроля над сетью криптовалюты и последующего подтверждения мошеннических транзакций;
   – «Двойная трата» или Double spending – нарушение верификации транзакции с целью двойного использования одних и тех же средств;
   – «Эгоистичный майнинг» или Selfish mining – с целью увеличения доходов путем создания особых условий централизации по причине наличия особых договоренностей.
4. Атаки, не зависящие от блокчейна и успешно применяемые ко многим технологиям:

– фишинг-атаки – путем получения аутентификационных данных посредством поддельных спам-рассылок и сайтов блокчейн-проектов;

– атака Дефейс – с целью подмены адресов для сбора средств на сайтах блокчейн-проектов;

– атаки с использованием методов социальной инженерии.

Стоит отметить, что рассмотренные в докладе атаки и уязвимости являются лишь наиболее известной частью негативного воздействия на блокчейн-индустрию.

Таким образом, проанализировав основные существующие атаки, важно отметить, что они направлены на уязвимости не самой технологии Блокчейн, которая защищена от несанкционированного влияния и взломов, а на воздействие на пользовательском уровне, на недочеты в кибер- и крипто-безопасности. Тем не менее, крайне важным моментом в вопросе предотвращения хакерских атак остается изучение источников и вектора воздействия злоумышленников, которые развиваются с каждым годом.