ВИДЫ АТАК НА БЛОКЧЕЙН И УМНЫЕ КОНТРАКТЫ

Г. Г. Трубач

Белорусский государственный университет, г. Минск
trubach1996@mail.ru;
науч. рук. – А. Н. Курбацкий, д-р техн. наук, проф.

Для решения проблемы доверия существует технология блокчейн. Блокчейн имеет большую популярность на данный момент и используется в системах разного назначения таких как криптовалюты и системы контроля поставок. Блокчейн обеспечивает децентрализованное, защищенное и в то же время открытое хранение данных. Для автоматизации выполнения договоренностей в системах, использующих блокчейн, применятся умные контракты. В данной работе приводится описание блокчейна и умных контрактов. Целью работы является обзор основных атак на блокчейн и умные контракты, а также способов их предотвращения. Приведенный материал следует учитывать при выборе или разработке блокчейна для обеспечения большей безопасности в приложениях, использующих его.

***Ключевые слова*:** атаки на блокчейн; атаки на умные контракты; криптовалюта; майнинг; proof-of-work.

ОПИСАНИЕ БЛОКЧЕЙНА

Блокчейн – это журнал всех подтвержденных транзакций. Все транзакции собираются в блоки, которые генерируются случайным процессом – майнингом.

Майнеры – участники процесса майнинга, – проверяют транзакции и собирают их в блоки (рис. 1). Каждый блок в блокчейне имеет хеш, который является результатом применения хеш-функции для всех данных блока, включая транзакции в нем. Для формирования данного хеша используется алгоритм proof-of-work, который требует достаточных вычислительных мощностей для вычисления хеша, но проверяется достаточно просто. Каждый последующий блок содержит в заголовке хеш предыдущего блока, что усложняет несанкционированное изменение данных в нем [1, с. 4-5].

Также заголовок блока содержит такие параметры, как временную метку создания и Nonce – параметр, определяющий сложность алгоритма proof-of-work.

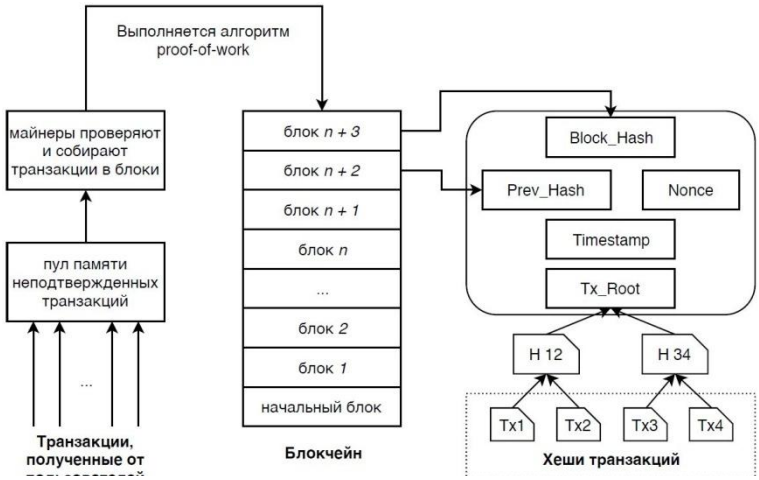

Рис. 1. Создание блоков

Так как блоки формируются одновременно несколькими майнерами, то возможно ветвление цепочек блоков – несколько блоков указывают на один и тот же блок в качестве предыдущего (рис. 2). В данном случае будет выбрана та ветвь, которая имеет большую сложность хеша и большую длину. Остальные будут отвергаться, и транзакции в них будут отклоняться [1, с. 5].

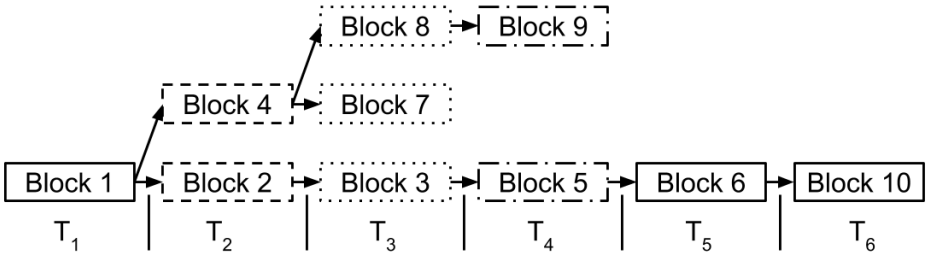

Рис. 2. Ветвление цепочки блоков [1, с. 5]

АТАКИ НА БЛОКЧЕЙН

Блокчейн, использующий алгоритм proof-of-work, может быть подвержен атакам, основанным на атаке «двойного расходования» – повторной трате средств. Данная атака может быть успешной, если в сети блокчейна используется малое число подтверждений блоков или, если у злоумышленника находится большее число вычислительной мощности, чем у всех остальных майнеров. В качестве общей защиты от атаки «двойного расходования» предлагается использовать такие методы, как мониторинг сети блокчейна, использование «черных списков» и ожидание множественных подтверждений транзакций для подтверждения совершения операций [1, с. 10].

Атака Финни

Атака Финни является вариацией атаки «двойного расходования», когда для совершения сделки ожидается не более одного подтверждения транзакции. Атакующий готовит транзакцию с оплатой товара и вместе с ней готовит блок, содержащий транзакцию на перевод этих средств на другой свой счет, но не публикует этот блок в сети. Как только транзакция с оплатой подтверждается одним из майнеров и злоумышленник получает товар, он незамедлительно публикует заранее подготовленный блок в сеть. В этом случае в сети оказывается две цепочки блоков одинаковой длины (рис. 2). И если остальные майнеры будут развивать вторую цепочку, содержащую транзакцию на перевод денег на счет атакующего, то транзакция перевода денег продавцу будет отклонена, и, следовательно, продавец потеряет деньги, так как товар уже был отправлен.

Защитой в данном случае является ожидание продавцом некоторого достаточного числа подтверждений транзакций, что уменьшает вероятность данной атаки, но не устраняет ее полностью [1, с. 11].

Если атакующий имеет контроль над n узлами сети, а продавец ожидает меньшее число подтверждений транзакций, то используя атаку Финни атакующий может создать более длинную цепочку с транзакцией, переводящий средства на контролируемый им счет. После публикации цепочки в сеть, майнеры продолжать работать над более длинной цепочкой, содержащей блок с необходимой атакующему транзакцией. Данная атака называется атакой грубой силы. Для защиты необходимо проводить мониторинг сети блокчейна.

Атака 51%

Данная атака предполагает, что у злоумышленника сосредоточено более 50% вычислительной мощности сети блокчейна. В данном случае атакующий, обладая большинством голосов, может отклонять или подтверждать необходимые ему транзакции быстрее создавая новые блоки, чем остальные майнеры. Защититься от такой атаки невозможно. Ее можно только предотвратить путем мониторинга сети. В закрытых блокчейнах, необходимо удостовериться, что узлы сети находятся в доверенных местах.

Другие атаки

Кроме атак «двойного расходования» существуют другие типы атак. Они включают атаки на сеть, атаки на пулы майнеров – объединение вычислительной мощности для работы над одними и теми же блоками и атаки на пользователей.

Атаки на сеть в блокчейне не имеют такой силы как в случае централизованных сетей, так как в распределенной сети можно атаковать лишь отдельные узлы или пулы.

Атаки на пулы майнеров направлены на повышение вычислительной мощности злоумышленника, что повысит его шансы на успешное проведения атаки «двойного расходования».

Атаки на пользователей направлены на попытку украсть их закрытые ключи для получения контроля над их кошельками.

ОПИСАНИЕ УМНЫХ КОНТРАКТОВ

Умный контракт – это компьютерный алгоритм, предназначенный для заключения и поддержания коммерческих контрактов в технологии блокчейн. Они предназначены для автоматизации и достоверности исполнения договорных отношений [2, с. 1].

АТАКИ НА УМНЫЕ КОНТРАКТЫ

Так как умные контракты – это алгоритм, то возможные атаки зависят от их конкретной реализации. Основной возможной атакой на умные контракты является использование ошибок при написании кода. Так как умный контракт описывается на определенном формальном языке, то могут допускаться ошибки в его описании.

Примером успешной атаки, является атака DAO, в ходе которой было украдено несколько десятков млн. долларов. Злоумышленник воспользовался ошибкой в реализации функции умного контракта Ethereum, в результате которой он смог рекурсивно получить вознаграждения за транзакцию.

Библиографические ссылки

1. *Conti M., Kumar S., Lal C., Ruj S.* A Survey on Security and Privacy Issues of Bitcoin // arXiv:1706.00916v3 [cs.CR]. 2017. URL: https://arxiv.org/pdf/1706.00916.pdf (дата обращения: 25.05.2018).
2. *Szabo N*. Smart Contracts: Building Blocks for Digital Markets // Phonetic Sciences. 1996. URL: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (дата обращения: 25.05.2018).