УДК 004.42

Е. И. Воронцов[1]*

Предотвращение двойного расходования криптовалюты при реорганизации цепи

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: minotavr1712@gmail.com

Аннотация. В статье анализируется угроза двойного расходования на примере криптовалюты Биткоин, которая может возникнуть в результате реорганизации цепи и является одной из основных угроз для безопасности и надежности децентрализованных платежных систем. Злоумышленник, обладающий достаточной вычислительной мощностью, может провести атаку эгоистичного майнинга, приводящую к реорганизации цепи. Благодаря этому становится возможным совершение атаки двойного расходования. С целью решения данной проблемы был разработан и протестирован способ предотвращения эгоистичного майнинга с последующим проведением двойной траты, основанный на модификации структуры хранения не потраченных выходов в базе данных LevelDB. Предлагаемое решение повышает стоимость проведения атаки, благодаря чему вероятность ее проведения уменьшается. Данное решение подходит для криптовалют, которые используют модель не потраченных выходов транзакций.

Ключевые слова: блокчейн, биткоин, криптовалюта, proof-of-work, эгоистичный майнинг, двойное расходование

E. I. Vorontsov[1]*

Preventing double spending of cryptocurrency during chain reorganization

[1] National Research Nuclear University «MEPhI», Moscow, Russian Federation
* e-mail: minotavr1712@gmail.com

Abstract. The article analyzes the threat of double spending on the example of Bitcoin cryptocurrency, which can happen as a result of chain reorganization and this is one of the main threats to the security and reliability of decentralized payment systems. An attacker with sufficient computing power can carry out a selfish mining attack, leading to a chain reorganization. This makes possible a double spending attack. To solve this problem, a method of preventing selfish mining with subsequent double spending was developed and tested. This method based on modifying the structure of storing unspent outputs in the LevelDB database. The proposed solution increases the cost of carrying out an attack, thereby reducing the possibility of its occurrence. This solution is suitable for cryptocurrencies that use the unspent transaction output model.

Keywords: blockchain, bitcoin, cryptocurrency, proof-of-work, selfish mining, double spending

Введение

В связи с развитием сферы информационно-коммуникационных технологий возросли требования к объему хранимой информации, а также к надежности ее хранения. Одним из примеров надежного хранилища является технология «блокчейн». Под данным термином кроется один из видов технологий распределен-

ного реестра. Блокчейн хранится в виде цепочки блоков на узлах, участвующих в сети. Данная цепь образуется за счет того, что все блоки связаны между собой. Благодаря этой связности довольно тяжело подделать информацию, которая однажды попала в блокчейн, поскольку его копия распределена между всеми участвующими узлами в сети. При попытке подмены хранимых в нем данных нарушается структура цепи, и информация восстанавливается за счет хранящейся копии у других участниках сети.

Впервые данная технология была реализована в проекте «Биткоин» в 2009 году. Биткоин является одной из самых распространенных криптовалют. Вся история о транзакциях хранится среди всех участвующих в сети узлов. Однако технология блокчейн имеет более широкое применение и не ограничивается сферой криптовалют. Например, она применяется в сферах кибербезопасности, экономики, здравоохранения, государственного управления, образования и во многих других.

Примерами использования блокчейна в сфере кибербезопасности являются работы научной школы Е. А. Басыни, представители которой в своих работах проводят исследование метода формирования децентрализованного реестра событий информационной инфраструктуры предприятия, а также занимаются его реализацией [1, 2].

Применение блокчейна в сфере здравоохранения описывается в [3]. Авторы работы описывают решение проблемы прогнозирования развития болезни с помощью искусственного интеллекта (англ. AI, Artificial Intelligence), а хранение данных обеспечивается с помощью технологии блокчейн [4].

Для сферы государственного управления предложен метод прозрачного участия в выборах с использованием смарт-контрактов в сети Эфириум (англ. Ethereum) [5].

В сфере образования блокчейну также было найдено применение. Seung J. P., Eung S. K., Jae G. S., Ju W. J. предлагают решение децентрализованного хранения заданий для проведения онлайн-тестирования. Все задания шифруются и хранятся в блокчейне до момента начала теста, после которого обучающийся расшифровывает условие, полученное из блокчейна [6].

Как упоминалось ранее, самым первым применением технологии блокчейн стал проект «Биткоин». Биткоин обеспечивает хранение всех совершенных участниками сети транзакций с использованием данной технологии. Каждый последующий блок хранит хеш от предыдущего блока, и в случае, если блок будет изменен, он быстро восстановится благодаря хранящейся копии блокчейна у соседних узлов.

В связи с существованием различного рода атак, направленных на нарушение корректного функционирования узлов сети или нарушение целостности хранимых в блокчейне данных, необходимо рассмотреть существующие решения, а также предложить новое. Но сперва необходимо провести исследование на тему устройства блокчейна Биткоина, включая детальное изучение основных понятий и деталей его реализации.

Исследование предметной области

В данной главе рассмотрены основные концепции и принципы работы, свойственные блокчейну Биткоина, а также возможные атаки на децентрализованные сети.

Все подключенные узлы образуют одноранговую сеть (англ. P2P, Peer-to-Peer). P2P подразумевает отсутствие центрального сервера, и каждый участник такой сети одновременно является и клиентом, и сервером. Каждый узел в сети Биткоина подключается к восьми таким же узлам, с которыми впоследствии он обменивается информацией. Например, узлы отправляют информацию о новых блоках или о совершенных транзакциях, которые необходимо добавить в блокчейн в дальнейшем.

Для одноранговых сетей свойственно недоверие другим участникам сети, поэтому все узлы должны следовать некоторым правилам. Такие правила называются протоколами консенсуса, благодаря которым все участвующие в сети узлы автоматически приходят к согласию о текущем состоянии блокчейна. Существует большое количество таких протоколов, но самыми распространенными являются доказательство работы (англ. PoW, Proof-of-Work) и доказательство доли (англ. PoS, Proof-of-Stake).

Доказательство работы используется в Биткоине и заключается в создании новых блоков майнерами, которые тратят свои вычислительные ресурсы на подбор подходящего на текущий момент хеша, который определяется установленной сложностью. Сложность представляет из себя набор нулей, которые устанавливают верхнюю границу для хеша нового блока. То есть хеш новых блоков обязательно должен начинаться с заранее определенного количества нулей. Каждый блок в Биткоине в среднем добавляется за 10 минут. В случае, если среднее время добычи блока падает, сложность добычи увеличивается. Основным недостатком данного протокола консенсуса является пустая трата вычислительных ресурсов на подбор хеша блока [7]. Поскольку информация в блоке фиксирована и несет в себе полезную нагрузку, для майнеров отведено специальное поле в блоке, которое включено в заголовок и называется «nonce» (number used once). На каждой итерации майнер изменяет данное поле на новое значение и получает новый хеш блока. В случае, если он удовлетворяет сложности, то блок считается созданным и транслируется в сеть, иначе процесс майнинга продолжается. В каждом блоке есть транзакция, которая называется «Coinbase», в которой майнеру адресована награда за блок, а также собрана комиссия со всех включенных в блок транзакций.

Протокол консенсуса PoS описывает способ, благодаря которому вероятность добавления новых блоков зависит от суммы ставки в виде количества монет. В случае, если блок был скомпрометирован, часть суммы ставки создателя блока блокируется. Такой подход заставляет участников сети действовать по правилам, иначе есть риск потери средств.

Каждый узел в сети Биткоина обладает некоторым функционалом и включает в себя определенные роли, представленные на рис. 1.

Рис. 1. Основные роли

Роль «Кошелек» отвечает за возможность создания транзакций. Роль «Майнер» заключается в предоставлении возможности создания новых блоков. «Блокчейн» позволяет локально хранить полную копию истории (также существуют узлы, которые хранят облегченную версию блокчейна, то есть только заголовки блоков). Каждый блок содержит заголовок (время создания, хеш предыдущего блока и так далее) и набор транзакций. «Сетевой функционал» позволяет узлу быть частью сети и взаимодействовать с другими участниками. Следует отметить, что каждому узлу необходимо обладать сетевым функционалом, иначе он не сможет получать актуальную информацию, а также делиться своей.

Помимо описанного ранее типа существуют и другие, обладающие ограниченным функционалом, изображенные на рис. 2.

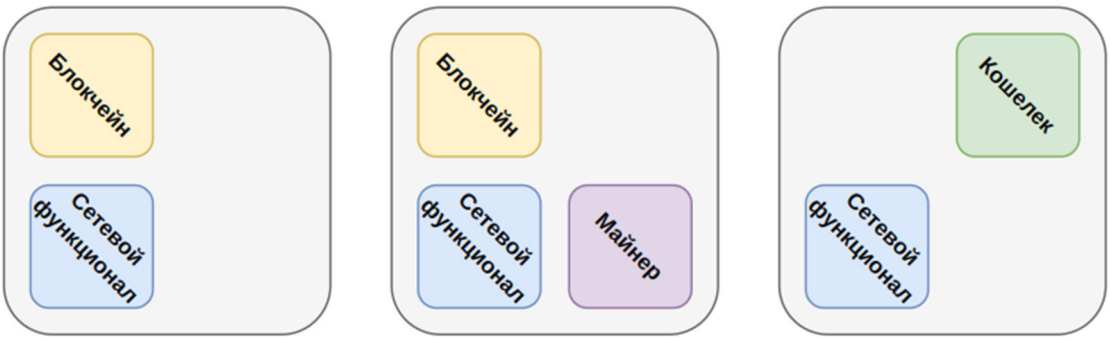

Рис. 2. Другие типы узлов

Следует заметить, что в Биткоине отсутствует модель аккаунтов, которая предполагает наличие у каждого некоторого баланса. Биткоин использует модель, основанную на непотраченных выходах (англ. UTXO, Unspent transaction output). Каждая транзакция представляет из себя набор входов и выходов, где каждый вход ссылается на какой-то выход транзакции, в которой средства были получены, а выходы отражают количество полученных монет [8]. Благодаря такому подходу становится возможным отследить историю передачи средств вплоть до самой первой транзакции, в которой монеты были получены майнером в качестве награды за найденный блок.

При создании новой транзакции она транслируются в сеть, узлы которой добавляют ее в свой мемпул (временное хранилище созданных, но еще не подтвержденных транзакций). Когда происходит майнинг нового блока, майнер добавляет в блок часть транзакций, находящихся в мемпуле.

Следует отметить, что существуют различного рода атаки, которые направлены на нарушение целостности хранимых в блокчейне данных. Примерами таких атак могут являться «Атака 51%», «Finney attack», «Race attack» или эгоистичный майнинг в комбинации с двойным расходованием и другие. Одним из примеров атаки нарушения корректности функционирования узла или совокупности узлов являются атаки, направленные на отказ в обслуживании (англ. DoS, Denial of Service)

Ситуация, при которой злоумышленник овладевает большей частью вычислительной мощности, называется «Атака 51%». При таких условиях злоумышленник может решать какие блоки добавлять в сеть, отклонять новые транзакции, а также изменять уже существующий блокчейн [9]. Эта атака является довольно опасной, поскольку она позволяет контролировать сеть, а также может проводиться в комбинации с другими атаками, в результате которых может нарушиться целостность хранимых данных.

DoS-атаки направлены на заполнение сети фиктивным трафиком, чтобы нарушить работу служб и участвующих компонентов, подключенных к сети Биткоин. Примером DoS-атаки может быть атака на майнинг-пул. Майнинг-пул представляет из себя совокупность майнеров, которые объединили свои вычислительные мощности для увеличения вероятности нахождения блока. Атаки на отказ в обслуживании могут привести к исключению пула из числа конкурентов, что увеличивает вероятность нахождения блоков другими майнерами [10].

Атака двойного расходования заключается в трате одного и того же актива дважды [10]. От обычного двойного расходования Биткоин защищен путем хранения информации о всех существующих еще не потраченных выходах в базе данных (БД) LevelDB. LevelDB является не реляционной базой данных, в которой хранится информация в формате ключ-значение. В Биткоине она используется для хранения информации о всех текущих UTXO всех участников сети. Когда происходит трата UTXO, то он удаляется из БД. В случае, если транзакция тратит несуществующий в базе данных выход, то она считается недействительной и не добавляется в блокчейн.

Существуют разновидности данного вида атаки:

– «0-confirmations race attack»;
– «Finney attack»;
– двойное расходование в комбинации с эгоистичным майнингом.

«0-confirmations race attack» – атака, при которой одновременно создаются транзакции с тратой одного и того же UTXO себе и продавцу. При переводе монет себе злоумышленник оставляет майнеру большую комиссию, а при переводе средств продавцу – маленькую. За счет того, что майнерам выгоднее включать те транзакции, в которых комиссия более крупная, из двух полученных транзакций он выберет ту, в которой комиссия больше [11].

«Finney attack» заключается в том, что злоумышленник заранее тратит определенный выход и отправляет его самому себе, а также создает блок с этой транзакцией, но не публикует его в сеть. После создания обычной транзакции за оплату какого-то товара продавцу злоумышленник публикует этот блок в сеть, а транзакция продавцу отклоняется, поскольку данный выход уже потрачен [11].

Двойное расходование в комбинации с эгоистичным майнингом заключается в изменении истории блокчейна, благодаря которому злоумышленник может провести двойную трату. Эгоистичный майнинг предполагает производство блоков, которое происходит временно без их трансляции в сеть. В случае если блокчейн злоумышленника обогнал текущий, то он публикует свой вариант, который принимается сетью по правилу более длинного блокчейна, и случается реорганизация. Реорганизация цепи – это процесс, при котором узлы сети заменяют одну версию блокчейна на другую, более длинную и актуальную. Это может произойти, когда два или более узлов создают блоки одновременно и в одном и том же месте, что приводит к разветвлению цепи. Благодаря реорганизации, вызванной эгоистичным майнингом, нечестный участник сети переписывает историю последних блоков блокчейна, а также забирает награду за найденные блоки, лишая ее честных узлов. Если рассматривать данную атаку в комбинации с двойным расходованием, то злоумышленник транслирует в сеть транзакцию продавцу с тратой определенного UTXO. В свой блокчейн, над которым он работает локально, он включает транзакцию с тратой данного выхода самому себе. Когда блокчейн атакующего обгоняет текущий, то он принимается сетью, а транзакция продавцу отменяется, так как записи о данном UTXO в БД уже нет, поскольку он уже потрачен.

Существуют некоторые решения, которые позволяют участнику не быть обманутым. Одним из таких решений является ожидание некоторого количества подтверждающих блоков. Подтверждающие блоки – это блоки, которые добавляются к блокчейну после блока, содержащего определенную транзакцию. Количество подтверждающих блоков показывает, насколько надежно включена транзакция в блокчейн и насколько маловероятно, что она будет отменена или изменена. Например, для Биткоина считается, что наличие шести подтверждающих блоков достаточно, чтобы злоумышленник не смог провести атаку 51%, которая может привести к двойному расходованию. Другим примером решения атаки является мониторинг состояния блокчейна у других узлов. Благодаря этому продавец может удостовериться, что на текущий момент отсутствуют соревнующиеся ветки блокчейна. Следует отметить, что описанные решения позволяют избежать атаки двойного расходования на уровне отдельного участника, но не предотвращать проблему на уровне всей сети в целом.

В ходе исследования предметной области было установлено, что проблема двойного расходования криптовалют при реорганизации цепи является актуальной, так как существующие решения не гарантируют полной защиты от атак злоумышленников.

Постановка задачи

Целью настоящей работы является создание алгоритма по предотвращению двойного расходования при реорганизации цепи.

В ходе решения данной проблемы выделены следующие задачи:

– исследование предметной области;
– изучение устройства блокчейна Биткоина;
– программная реализация блокчейна;
– программная реализация алгоритма, предотвращающего атаку двойной траты;
– создание стенда для тестирования разработанного решения.

Предлагаемое решение

Предлагаемое решение основано на модификации структуры хранения информации о всех UTXO в LevelDB. В роли ключа в БД выступает хеш транзакции, а также номер выхода для этой транзакции. Значением является следующая информация:

– является ли транзакция «Coinbase» или нет;
– индекс блока, в который включена транзакция;
– количество монет;
– данные, позволяющие потратить выход только владельцу.

Данные, которые позволяют тратить выход только владельцу, называются также блокирующим скриптом. Благодаря такому механизму средства могут быть потрачены только после того, как участник сети предоставляет цифровую подпись для транзакции, в которой он тратит этот выход.

С целью предотвращения двойного расходования предлагается добавить два дополнительных поля в уже существующую структуру хранения UTXO в БД. Первым предлагаемым полем является индикатор, указывающий на то, что UTXO уже потрачен или нет. Второе поле указывает на хеш транзакции, в которой данный выход был потрачен.

Биткоин удаляет существующую запись о UTXO из БД, как только тот был потрачен в новой подтвержденной транзакции. В предлагаемом решении данная запись о выходе после траты UTXO должна удаляться из LevelDB только спустя какое-то время. Данный временной интервал измеряется в количестве блоков и должен выбираться, основываясь на общей вычислительной мощности сети и частоте совершения транзакций. Чем меньше вычислительная мощность сети, тем больше должно быть это число. Чем чаще совершаются транзакции, тем меньше этот интервал, поскольку данное решение имеет один недостаток – невозможно создать новую транзакцию с уже существующим в БД хэшем транзакции пока уже существующая запись не будет удалена.

Благодаря такому решению в случае получения нового блока от соседних узлов необходимо проводить проверку корректности транзакций согласно блок-схеме, изображенной на рис. 3.

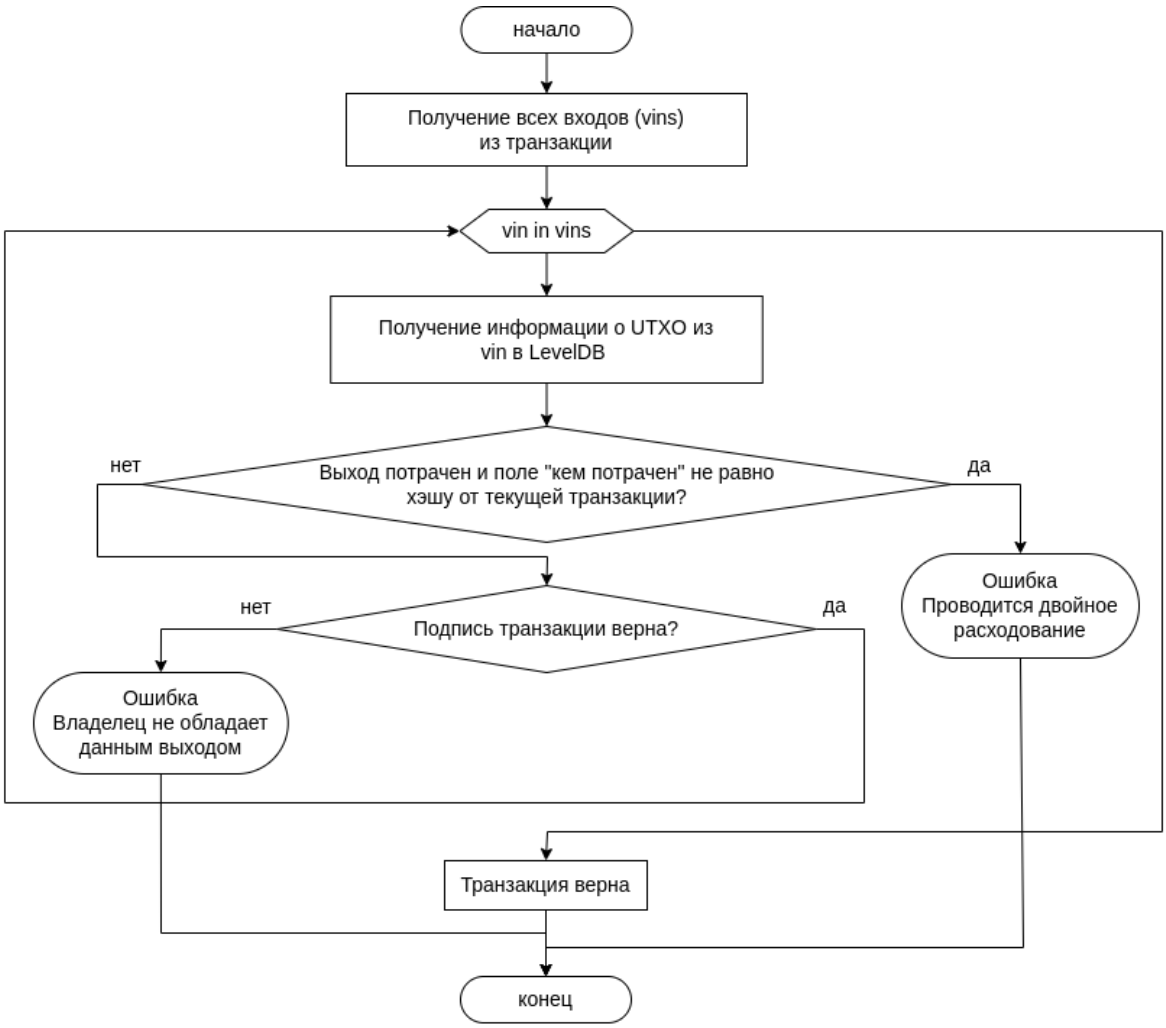

Рис. 3. Блок-схема алгоритма проверки транзакций полученного блока на проведение двойного расходования

Из каждой транзакции нового блока извлекается информация о входах, которые проверяются на их достоверность. Проверяется, не проводится ли двойное расходование, а также корректность подписи, которую создал инициатор транзакции. Двойное расходование можно обнаружить согласно предложенному методу: поскольку запись о трате UTXO еще не была удалена из БД, то проверяется, был ли потрачен выход. Если выход был потрачен, то необходимо удостовериться в том, что данный выход был потрачен в той же самой транзакции. Вторая проверка необходима на случай, если произошла реорганизация цепи, но одна и та же транзакция попала в оба варианта блокчейна. Если проверка была пройдена успешно, то транзакция является корректной. При невыполнении одного из условий данный блок нельзя добавлять в блокчейн, поскольку он содержит некорректную транзакцию.

Следует отметить, что несмотря на наличие у злоумышленника вычислительной мощности в 51% и более ему не удастся провести атаку двойного расходования, пока запись о конкретном UTXO хранится в базе данных остальных

участников сети. Благодаря предлагаемому решению стоимость атаки 51% для совершения двойного расходования возрастает, поскольку злоумышленнику необходимо поддерживать такую вычислительную мощность на соответствующем уровне до момента, пока нужная ему запись не будет удалена из БД. Данные выводы были сделаны в ходе проведения экспериментального исследования.

Экспериментальное исследование

Тестирование работоспособности предлагаемого решения проводилось в сети, изображенной на рис. 4. Данная сеть состоит из одной физической машины и четырех виртуальных.

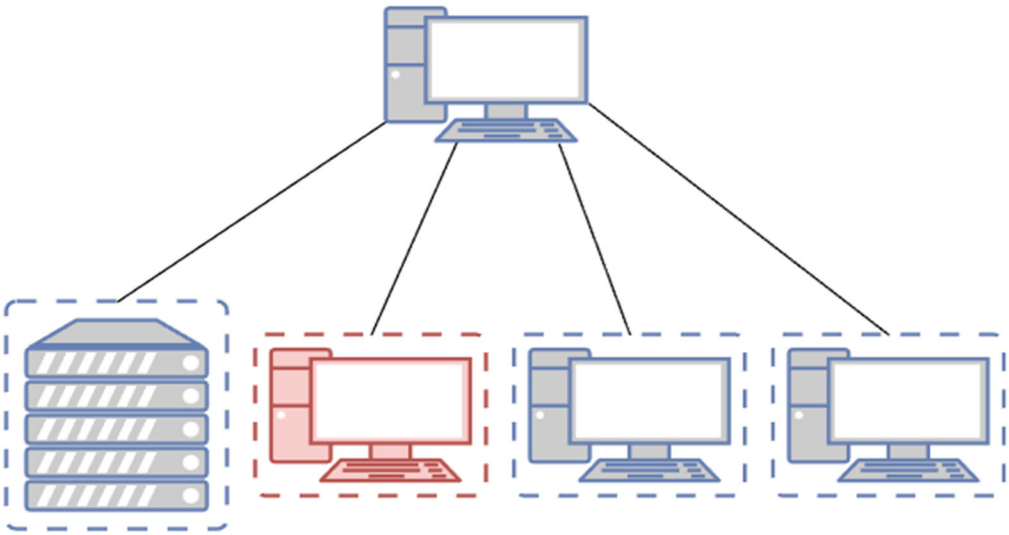

Рис. 4. Сеть тестирования решения

Один из изображенных узлов является сервером, на котором хранится вся информация об активных участниках сети. К данному серверу происходит самое первое подключение любого узла для получения актуальной информации о сети. Остальные машины обладают функционалом полного узла.

Тестирование предлагаемого решения проходило в сети, где один из узлов играл роль злоумышленника и пытался провести эгоистичный майнинг с последующим двойным расходованием. Сперва злоумышленник тратит свой UTXO в транзакции для оплаты какого-то товара, которая транслируется в сеть. Затем он отключается от сети, удаляет ранее совершенную транзакцию из своего мемпула и создает новую с тратой того же самого UTXO, в которой средства отправляет на свой адрес. В это время честные узлы создают один блок, в который включается ранее полученная транзакция злоумышленника с отправкой монет на адрес продавца. Злоумышленник в этот момент создает два новых блока, подключается к сети и транслирует свой блокчейн, поскольку ему удалось обогнать цепь честных узлов. Благодаря алгоритму проверки корректности транзакций блокчейн злоумышленника не принимается, поскольку в нем содержится транзакция, в которой совершается двойное рас-

ходование. Таким образом, злоумышленник должен дождаться момента, когда остальные участники сети удалят интересующую его запись из LevelDB, и только тогда он сможет провести атаку с двойным расходованием при реорганизации цепи. Но необходимо заметить, что все это время атакующий должен поддерживать на том же уровне свою вычислительную мощность, чтобы к моменту удаления UTXO с передачей средств продавцу из базы данных других узлов его блокчейн обгонял блокчейн остальных участников сети. Это условие проведения атаки делает ее достаточно дорогой.

В ходе экспериментального тестирования решение отработало успешно, были выявлены попытки проведения двойного расходования при совершении злоумышленником эгоистичного майнинга.

Заключение

В рамках данной работы было предложено решение атаки двойного расходования при реорганизации цепи на примере блокчейна Биткоина, которое было реализовано программно и работало успешно. Необходимо добавить, что данное решение подходит только для криптовалют, использующих модель UTXO.

Практическая значимость работы состоит в повышении безопасности при совершении сделок, поскольку благодаря модернизации структуры не потраченных выходов, хранимых в LevelDB, а также разработанному алгоритму проверки транзакции вероятность успешного проведения атаки двойного расходования уменьшается.

Новизна работы заключается в решении атаки двойного расходования при реорганизации цепи. Данная атака сильно увеличивается в стоимости ее реализации, и в некоторых случаях предложенное решение может предотвратить атаку 51%. Также следует заметить, что помимо Биткоина существуют и другие криптовалюты, которые обладают меньшей мощностью, а значит больше подвержены атаке 51%.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Leila B. Blockchain Technology: Practical P2P Computing (Tutorial) / Leila B., Sarunas G. // 2019 IEEE 4th International Workshops on Foundations and Applications of Self* Systems (FAS*W). - 16-20 June 2019. - P. 249 - 250.

2. Басыня Е. А. Децентрализованный подход к сбору и обработке данных информационной инфраструктуры предприятия = Decentralized approach for collecting and processing data of the enterprise information infrastructure / Е. А. Басыня, А. В. Сафронов // Вестник УрФО. Безопасность в информационной сфере = Journal of the Ural Federal District Information security. - 2019. - № 3 (33). - С. 43–54. - DOI: 10.14529/secur190305.

3. Басыня Е. А. Метод формирования децентрализованного реестра событий информационной инфраструктуры предприятия = Method for forming a decentralized registry of the enterprise information infrastructure events / Е. А. Басыня, А. В. Сафронов // Вестник УрФО. Безопасность в информационной сфере = Journal of the Ural Federal District Information security. - 2019. - № 4 (34). - С. 35-44.

4. Sabyasachi C. A Secure Healthcare System Design Framework using Blockchain Technology / Sabyasachi C., Satyabrata A., Hee-Cheol K. // 2019 21st International Conference on Advanced Communication Technology (ICACT). - 17-20 February 2019. - P. 260-264.

5. Kriti P. Decentralized E-Voting Portal Using Blockchain / Kriti P., Swapnil J. // 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). - 06-08 July 2019. - P. 1-4.

6. Seung J. P. Online test and management system using blockchain network / Seung J. P., Eung S. K., Jae G. S., Ju W. J. // 2019 21st International Conference on Advanced Communication Technology (ICACT). - 17-20 February 2019. - P. 269-272.

7. P. Rajitha N. Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain / P. Rajitha N., D. Ramya D. // 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV). - 04-06 February 2021. - P. 279 - 283.

8. Yan W. Forensic Analysis of Bitcoin Transactions / Yan W., Anthony L., Dianxiang X. // 2019 IEEE International Conference on Intelligence and Security Informatics (ISI). - 2019. - P. 167 - 169.

9. Fredy A. A. The 51% Attack on Blockchains: A Mining Behavior Study / Fredy A. A., Ana L. S. O., Ricardo V., Pedro W. // IEEE Access. - 11 October 2021. - Vol. 9. - P. 140549 - 140564.

10. Ehab Z. Bitcoin and Blockchain: Security and Privacy / Ehab Z., Tongtong L., Matt W. M., Jian R. // IEEE Internet of Things Journal. - 2020. - Vol. 7. - P 10288 - 10313.

11. Mubashar I. Exploring Sybil and Double-Spending Risks in Blockchain Systems / Mubashar I., Raimundas M. // IEEE Access. - 19 May 2021. - Vol. 9. - P. 76153 - 76177.