Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056

Набешко
Галина Александровна

РАСПРЕДЕЛЕННАЯ СИСТЕМА ОБРАБОТКИ ИНФОРМАЦИИ НАОСНОВЕ ТЕХНОЛОГИИ РЕЕСТРА БЛОКОВ ТРАНЗАКЦИЙ

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1 - 98 80 01 Информационная безопасность

Научный руководитель

В.А. Захарьев,
кандидат технических наук,
доцент,
доцент каф. СУ БГУИР

Минск 2021

Библиотека БГУИР

ВВЕДЕНИЕ

Вопросы защиты информации имеют большую востребованность в наше время. Актуальность обеспечивается высокой стоимостью данных, которые могут попадать в руки злоумышленников. Одним из основных направлений современного развития криптографии является блокчейн. Блокчейн – это база данных, особенностью которой является неизменяемость данных и высокая степень безопасности. В рамках национального законодательства, а именно Декрета № 8 от 21 декабря 2017 г. "О развитии цифровой экономики" технология блокчейн получила название технологии реестра блоков транзакций.

На базе технологии блокчейн реализовано большое количество различных криптовалют. При этом для, казалось бы, простой операции обмена пользователю необходимо рисковать своими средствами и персональными данными, которые будут переданы на криптовалютную биржу для осуществления обмена. Риск обусловлен частыми случаями компрометации средств и данных с подобных площадок. Одним из решений данной проблемы является технология атомарных свопов, позволяющая произвести обмен одной криптовалюты в другую без участия посредника. Однако стандартная реализация технологии атомарных свопов подходит для узкого круга блокчейнов криптовалют ввиду несовместимости реализаций.

В данной работе будет предложено решение проблемы несовместимости блокчейнов Биткоина и Монеро в виде алгоритма реализации атомарного свопа. Таким образом тема, связанная с разработкой новых алгоритмов атомарного обмена, является актуальной в связи с недостаточным уровнем обеспечения информационной безопасности при организации площадок централизованного обмена.

Цель: сравнительный анализ и модернизация существующих методов, моделей и алгоритмов реализаций технологии реестра блоков транзакций на примере создания алгоритма атомарного обмена между двумя реализациями блокчейна.

Объект исследования: протокол атомарного обмена на основе технологии реестра блоков транзакций, т.е. технологии блокчейн.

Предмет: совершенствование существующих методов защищённого обмена между различными реализациями блокчейн в финансовой сфере (криптовалютами Биткоин и Монеро) по средствам применения атомарных свопов.

Библиотека БГУИР

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность исследования

Одним из основных направлений современного развития криптографии является блокчейн. На базе технологии блокчейн реализовано большое количество различных криптовалют. При этом для, казалось бы, простой операции обмена пользователю необходимо рисковать своими средствами и персональными данными, которые будут переданы на криптовалютную биржу для осуществления обмена. Риск обусловлен частыми случаями компрометации средств и данных с подобных площадок. Одним из решений данной проблемы является технология атомарных свопов, позволяющая произвести обмен одной криптовалюты в другую без участия посредника. Однако стандартная реализация технологии атомарных свопов подходит для узкого круга блокчейнов криптовалют ввиду несовместимости реализаций.

Таким образом тема, связанная с разработкой новых алгоритмов атомарного обмена, является актуальной в связи с недостаточным уровнем обеспечения информационной безопасности при организации площадок централизованного обмена.

Цель исследования

Цель диссертационной работы: сравнительный анализ и модернизация существующих методов, моделей и алгоритмов реализаций технологии реестра блоков транзакций на примере создания алгоритма атомарного обмена между двумя реализациями блокчейна.

Задачи исследования

1. Провести обзор источников по теме диссертационного исследования.
2. Ознакомиться с применением технологии блокчейн в финансовой сфере.
3. Выполнить сравнительный анализ существующих методов, моделей и алгоритмов реализации технологии реестра.
4. Сформулировать и формализовать требования к реализации алгоритма атомарного обмена.
5. Спроектировать и реализовать алгоритм атомарного обмена между выбранными блокчейнами.
6. Проанализировать полученную реализацию на предмет наличия уязвимостей.

Библиотека БГУИР

Новизна полученных результатов

Научная новизна заключается в создании безопасного алгоритма обмена для реализаций блокчейн Биткойн и Монеро на основе технологии атомарного свопа. Все этапы алгоритма таких, как генерация ключей, обмен ключами и подписание транзакций описаны подробно, так же рассмотрены все возможные случаи отклонения от основного сценария, что отражает глубину анализа и обеспечивает безопасность обмена, и является главным показателем качества реализованного алгоритма.

Личный вклад соискателя

Соискателем выполнены все изложенные в работе разработки и исследования. Постановка задач и обсуждение результатов проводились совместно с научным руководителем. Соавторы опубликованных работ принимали участие в обсуждении промежуточных и конечных результатов. Обработка, интерпретация данных, а также выводы сделаны автором самостоятельно.

Апробация результатов диссертации

Основные положения диссертационной работы докладывались на следующих научных конференциях:

– The International Conference on Information Technologies and Systems ITS 2020 (Минск 2020).

Библиотека БГУИР

СОДЕРЖАНИЕ РАБОТЫ

Реестр блоков транзакций (блокчейн) – выстроенная на основе заданных алгоритмов в распределенной децентрализованной информационной системе, использующей криптографические методы защиты информации, последовательность блоков с информацией о совершенных в такой системе операциях.

Атомарный своп, как операция по обмену одной криптовалюты на другую, может быть реализован мгновенно без необходимости полагаться на требующую доверия третью сторону (посредника) в лице биржи или обменной платформы. В результате контроль над сделкой осуществляют исключительно участвующие в ней стороны.

Ключевые особенности технологии таковы:

- с ее помощью можно решить проблему масштабируемости сети и интероперабельности;
- полный контроль пользователями над их средствами;
- высочайший уровень безопасности совершения сделок;
- одной из важнейших особенностей является удаление промежуточных токенов;
- возможность открытия огромного количества децентрализованных торговых площадок, которые не будут брать с пользователей комиссию за совершение сделок.

Для реализации базового протокола есть два главных требования:

1. Поддержка смарт контрактов, которые позволяют реализовать временные блокировки и определить условия обмена.
2. Использование одного и того же криптографического алгоритма для возможности обмена ключами.

Основное препятствие для реализации атомарных свопов в Monero- необходимость предусмотреть транзакцию возврата в случае отмены атомарного обмена. Из-за технологии обеспечения приватности Monero под названием «кольцевые подписи» отправитель транзакции всегда неизвестен. Поэтому протокол не сможет произвести транзакцию возврата, потому что ему даже неизвестно, кто был источником транзакции.

Используя схему подписей Шнорра и временные блокировки, становится возможным реализовать протокол атомарного обмена между реализациями блокчейн Биткойн и Монеро. Протокол будет состоять из следующего набора транзакций:

XMR_1 – транзакция блокировки средств в блокчейне Монеро.

XMR_r – транзакция выкупа средств в блокчейне Монеро.

XMR_c – транзакция отмены атомарного свопа, возвращает средства владельцу.

Библиотека БГУИР

BTC_1 – транзакция блокировки средств в блокчейне Биткойн.

BTC_r – транзакция выкупа средств в блокчейне Биткойн.

BTC_c – транзакция отмены атомарного свопа, возвращает средства владельцу.

BTC_t – транзакция снятия средств, отправляет средства новому владельцу.

BTC_e – транзакция экстренной отмены атомарного свопа, которая возвращает средства владельцу.

Транзакции основного сценария: XMR_1 → BTC_1 → BTC_r→ XMR_r → BTC_t.

Транзакции альтернативного сценария:

Боб не выходит на связь: XMR1→ XMRc.

Алиса прекращает взаимодействие: XMR1 → BTC1 → BTCc.

Алиса пытается забрать оба актива: XMR1 → BTC1 → BTCr→ XMRc →BTCe.

В первом разделе диссертации проанализирована технология блокчейн с точки зрения наличия преимуществ и недостатков, приведены классификации технологии и рассмотрены примеры применения технологии блокчейн в финансовой сфере.

Во втором разделе рассмотрены методы и модели формирования реестра блоков транзакций и протоколы выработки консенсуса. Выделены преимущества и недостатки протоколов выработки консенсуса Проанализированы проблемы несовместимости реализаций блокчейн, которые не позволяют реализовать стандартный протокол атомарного обмена, алгоритм которого так же приведен.

В третьей главе формализованы требования к реализуемому алгоритму атомарного обмена между блокчейнами валют Bitcoin и Monero. Предложен вариант реализации протокола атомарного обмена, как решение проблемы несовместимости, который использует подписи адаптера для блокчейна Биткойн. Проблема данного алгоритма заключалась в двух вещах.

Если после публикации первой транзакции Алиса прекращает взаимодействие Бобу необходимо возвращать средства назад публикацией второй транзакции, за которую ему необходимо заплатить майнинговую комиссию. Таким образом Боб тратит 2 комиссии сети биткоин, которая знаменита самыми высокими комиссиями. И этот пользователь рискует потерять все свои средства на оплату майнинговой комиссии в случае нескольких неудачных обменов.

Библиотека БГУИР

Обмен ключами во время протокола вызывает ещё один дополнительный альтернативный сценарий. Поэтому было принято решение о модификации алгоритма.

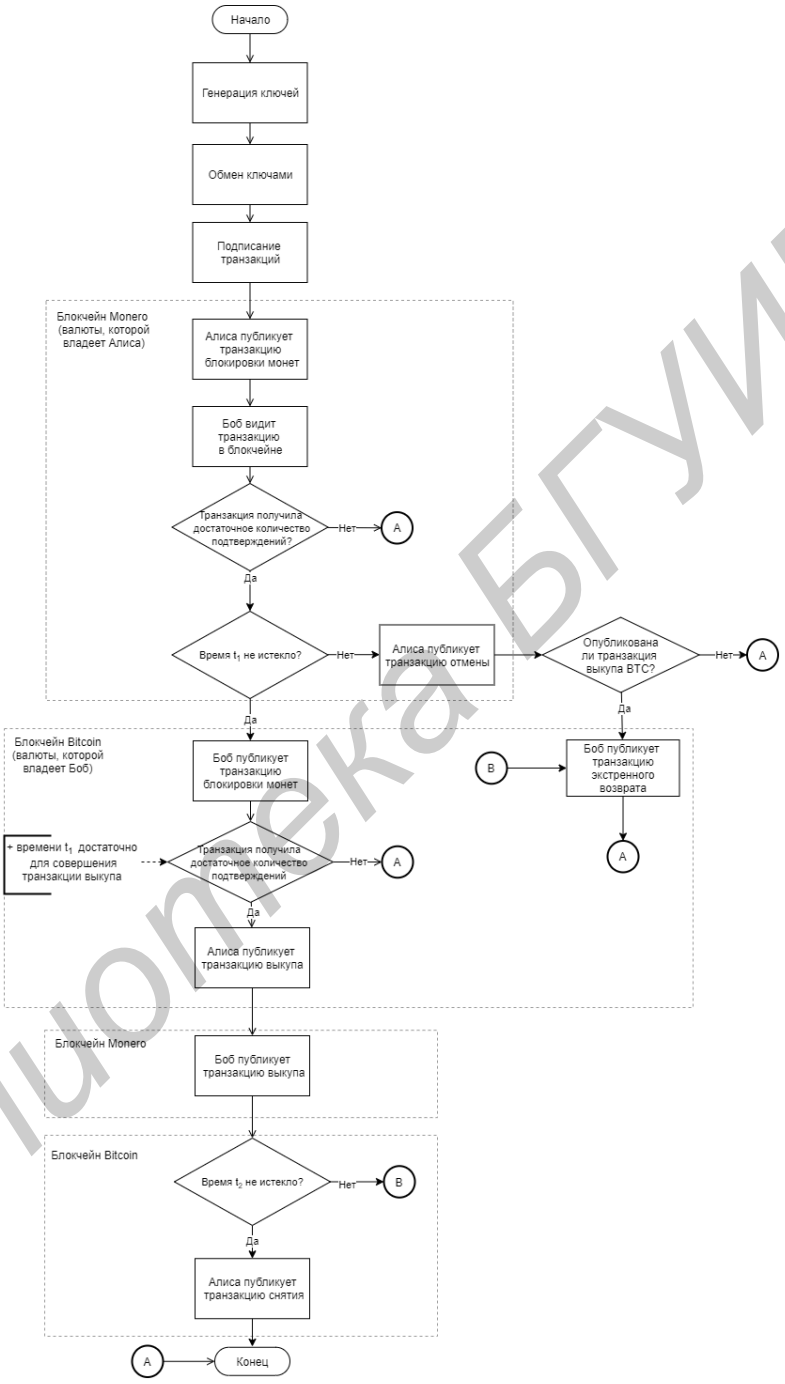

Рисунок 1 – Алгоритм атомарного обмена

В четвертой главе произведена модификация защищенного протокола обмена на основе атомарных свопов в виду наличия уязвимости у первого варианта реализации. Алгоритм атомарного обмена между реализациями блокчейн Монеро и Биткоин приведен на рисунке 1.

Библиотека БГУИР

ЗАКЛЮЧЕНИЕ

В диссертации проанализирована технология блокчейн с точки зрения наличия преимуществ и недостатков, приведены классификации технологии по доступности реестра данных и поколениям. Рассмотрены вопросы применения технологии блокчейн в финансовой сфере, которые показали, что основными предпосылками внедрения технологии блокчейн являются слабые или «узкие» места современной финансовой системы. Произведен обзор существующих систем и решений построенных на основе технологии блокчейн.

Проведен сравнительный анализ протоколов выработки консенсуса, выделены преимущества и недостатки конкретных методов. Изучены методы и модели формирования блоков транзакций. Выявлена проблема несовместимости текущих реализаций блокчейнов, которая не позволяет реализовать стандартный протокол атомарных свопов. Рассмотрены частые случаи компрометация пользовательский данных и средств на площадках, предоставляющих функционал обменов, что ярко подчеркивает актуальность и востребованность технологии атомарных свопов. Так же приведен пример работы стандартного протокола атомарного свопа.

Так же формализованы требования к реализуемому алгоритму атомарного обмена между блокчейнами валют Биткоин и Монеро. Описаны процессы взаимодействия пользователей до начала обмена, т.е. подготовительные действия перед совершением первой транзакции. Приведены схемы протокола на этапах подписания и генерации ключей. Описан основной сценарий, проанализированы альтернативные сценарий на предмет наличия уязвимостей. Так же построены и приведены схема транзакций и диаграмма последовательности, отображающая взаимодействие пользователей в блокчейнах валют, между которыми производится атомарный обмен.

В процессе диссертации произведена модификация защищенного протокола обмена на основе атомарных свопов в виду наличия уязвимости. Приведена схема транзакций в блокчейнах валют, отображен полный алгоритм модифицированного протокола. Проведен анализ алгоритма на предмет наличия уязвимостей и незакрытых сценариев и на соответствие требованиям. Модифицированный алгоритм полностью удовлетворяет требованиям, предъявляемым в начале работы над алгоритмом.

Таким образом предложено решение проблемы несовместимости текущих реализаций блокчейн в виде алгоритма атомарного свопа между блокчейнами валют Биткоин и Монеро. Технология атомарных свопов является достаточно новой в мире криптовалют и предполагает под собой разработку алгоритмов между различными реализациями блокчейн, что

Библиотека БГУИР

накладывает определенную сложность в имплементации, но однозначно затраты на эту разработку будут оправданы ввиду того, что альтернативный обмен с помощью централизованных бирж небезопасен и ущерб от компрометации средств, и персональных данных пользователей с одной площадки обмена оценивается в 1 млрд долларов.

В будущем технология атомарных свопов может предложить решение для обмена криптовалюты на фиатную валюту (BYN, USD, EUR и др.). Технически существует возможность совершать атомарные свопы с фиатом, для этого достаточно добавить в платежную систему транзакции с секретом. Пользователь переводит свои средства абоненту, выставляя секрет, и абонент может забрать эти средства в течение какого-то времени, только предъявив этот секрет. Добавление одной маленькой функциональности в любую платежную систему, где есть возможность совершать внутренние транзакции в фиате, позволяет сделать атомарные свопы между криптовалютой и фиатом реальностью.

Библиотека БГУИР

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Набешко, Г. А. Стандарты токенов сети Ethereum и их особенности в реализации работы смарт-контрактов / Г. А. Набешко, В. А. Захарьев// Материалы международной научной конференции, ITS-2020, Минск, 18 ноября 2020 г. / – с. 43-44

Библиотека БГУИР