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

УДК 004.62

Ващук
Денис Васильевич

Система осуществления безопасных криптовалютных транзакций

АВТОРЕФЕРАТ

на соискание степени магистра магистра информатики и вычислительной техники по специальности 1-40 81 02 «Технологии виртуализации и облачных вычислений»

Научный руководитель
Самаль Д.И.
кандидат технических наук, доцент

Минск 2017

ВВЕДЕНИЕ

Решения на основе блокчейнов - одно из основных современных направлений разработки для финансовых и государственных учреждений. Старые технологии, используемые в этих учреждениях, уже не соответствуют требованиям современного мира и требуют реорганизации. Децентрализованные и распределенные базы данных с неизменной историей на основе блокчейнов на данный момент являются одними из наиболее популярных решений для организаций. В рамках магистерской работы были исследованы и описаны системы на основе блокчейнов, которые могут послужить основой для создания надежных и защищенных от подделывания финансовых баз данных, реестров документов, систем электронного правительства, реестров логистических сетей, картотек в больницах и поликлиниках.

Впервые блокчейн был применен при разработке криптовалюты Биткоин. Криптовалюты привлекли внимание общественности, потому что старые финансовые и правительственные институты не справляются с возложенными на них обязанностями. На данный момент в мире разработано множество криптовалют со своими достоинствами и недостатками под конкретные нужды отдельных групп пользователей. Некоторые криптовалюты разработаны для использования в глобальных масштабах, некоторые для совершения транзакций между несколькими частными организациями и банками. Криптовалюты обладают следующими достоинствами:

1. Нулевые или очень низкие комиссии.
2. Отличная делимость, простая пересылка и верификация.
3. Мультиподписи. Транзакции могут создаваться с гарантом, когда, например, требуются две из трех подписей для совершения транзакции.
4. Смарт-контракты, позволяющие задавать гораздо более сложные условия для выполнения операций.
5. Избавление от посредников, таких как банки-корреспонденты, что уменьшает время на транзакцию, стоимость транзакции.
6. Децентрализация обработки транзакций.
7. Отсутствие цензуры.
8. Неизменная история транзакций.
9. Предсказуемая инфляция.

В рамках учебного эксперимента с целью повышения мотивации студентов к учебному процессу в рамках кафедры ЭВМ было принято решение разработать и внедрить криптовалюту со следующими свойствами и возможностями:

- осуществление безопасных и необратимых переводов;
- сохранение истории всех переводов, позволяющей проводить финансовый аудит;
- осуществление контроля эмиссии;
- изменение параметров блокчейна (размер комиссий, интервал создания блока);
- масштабирование системы и высокая пропускная способность;
- отсутствие потребности в мощных серверах;
- эксклюзивное создание блока;
- возможность проведения аудита финансовых операций;
- создание пользовательских токенов;
- защита от DoS атак;
- регистрация пользователя только администраторами системы;
- сохранение приватной пользовательской информации отдельно в базе данных.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Целями диссертационной работы являются:

- исследование существующих криптовалют;
- исследование блокчейн-систем, используемых для реализации криптовалют;
- исследование алгоритмов консенсуса в распределенных системах;
- разработка криптовалюты с заданными свойствами.

Для достижения поставленных целей необходимо решить следующие задачи:

- проанализировать существующие криптовалюты;
- проанализировать существующие блокчейн-системы;
- проанализировать алгоритмы консенсуса;
- найти оптимальные параметры криптовалюты и подходящую систему для ее реализации;
- разработать новую криптовалюту на базе существующей блокчейн-системы, удовлетворяющей потребностям кафедры ЭВМ.

Объектом исследования являются криптовалюты и блокчейн-системы.

Предметом исследования являются алгоритмы консенсуса в блокчейн-сетях и оптимальные параметры блокчейнов.

Практическая значимость работы заключается в том, что разработанные криптовалютная система и экосистема для ее использования позволяют группе пользователей осуществлять прозрачное экономическое взаимодействие в пределах отдельной организации. Использование технологии блокчейн позволяет сохранять историю транзакций, проводить аудит, обезопасить данные реплицированием на несколько узлов.

СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, общей характеристики работы, четырех глав, заключения, списка использованных источников.

В первой и второй главах представлен анализ предметной области – обзор существующих криптовалют и алгоритмом консенсуса в блокчейн-системах. Рассмотрены алгоритмы Proof-of-Work, Proof-of-Stake и другие. Выявлены основные существующие проблемы в рамках тематики исследования, показаны направления их решения.

Третья глава посвящена обзору существующих открытых систем для разработки приложений с использованием блокчейн-технологии. Рассмотрены системы Биткоин, Graphene, Hyperledger Fabric, Hyperledger Sawtooth Lake, Ethereum, Corda. Целью данной главы было найти систему для реализации криптовалюты.

Четвертая глава посвящена разработке и внедрению собственной криптовалюты на базе Blockchain платформы Graphene. Подробно рассмотрены архитектура системы и аспекты выбора параметров алгоритмов консенсуса.

Общий объем работы составляет 74 страницы, из которых основного текста – 50 страниц, 12 рисунков на 10 страницах, 3 таблиц на 3 страницах и список использованных источников из 72 наименований на 5 страницах.

ЗАКЛЮЧЕНИЕ

Решения на основе блокчейнов образуют безопасный и децентрализованный каркас для обработки транзакций. Основные преимущества блокчейнов по сравнению с другими моделями распределенных баз данных - интеграция обработки данных и безопасности в единый протокол, реализуемый алгоритмически и минимизирующий человеческий фактор.

В ходе исследования были изучены основные принципы построения блокчейн-систем. Блокчейн представляет собой распределенную журналируемую базу данных с сохранением истории всех изменений. База данных представляет собой цепочку блоков, каждый блок содержит транзакции. Каждая транзакция меняет состояние системы. Транзакции криптографически подписываются, используя алгоритмы ECDSA. Таким образом, достигается согласованность состояния системы. К преимуществам такой архитектуры можно отнести сохранение истории операций (журналирование) и гарантирование неизменности этой истории. Неизменность достигается благодаря алгоритмам консенсуса, которые требуют использовать некоторый ресурс (например время работы CPU, или оперативную память валидирующего узла), перед тем, как станет возможным добавить блок с транзакциями в сеть. Чем больше в сети участников, и, как следствие, чем больше «используется» ресурса этими участниками, тем сложнее и экономически не выгодно потреблять этот «ресурс» для перезаписи истории.

Достижения консенсуса - это фундаментальная проблема в отказоустойчивых распределенных системах в контексте репликации данных. Распределенная база данных, которая лежит в основе технологии, состоит из репликаций на всех узлах сети. Цель алгоритмов консенсуса - привести распределенную систему в такое состояние, когда все участники системы согласны с ним. На примере криптовалютных систем, состоянием системы может быть порядок транзакций и текущие балансы пользователей. Типичные алгоритмы консенсуса достигают цели, когда доступно большинство узлов (участников системы).

В рамках магистерской работы была реализована криптовалюта с рабочим названием «Quantcoin», которая позволяет производить внутренний учет потребляемых ресурсов отдельными студентами и сотрудниками университета. Из-за юридических и технических причин, учреждения, в которых задействованы финансовые системы учета или реестры, могут быть заинтересованы в использовании блокчейнов с ограниченным доступом к

обработке транзакций (эксклюзивных), по крайней мере, в краткосрочной перспективе. Поэтому для реализации криптовалюты была выбрана система Graphene из-за используемого алгоритма консенсуса (делегированное подтверждение доли) и большой пропускной способности сети (тысячи транзакций в секунду). Новая система соответствует заданным требованиям и подходит для осуществления экономического взаимодействия в пределах организации:

- управление контролем эмиссии с помощью выпускаемых токенов;
- валидирующие узлы назначаются администратором системы;
- параметры криптовалюты могут быть изменены администратором системы;
- алгоритм консенсуса (DPoS) не требует мощных серверов для поддержания системы в консистентном состоянии;
- доступ к системе осуществляется через WEB и мобильные приложения;
- существует возможность подключить к криптовалютной экосистеме смарт-устройста;
- большая пропускная способность сети (до 100 000 транзакций в секунду), горизонтальное масштабирование.

Список публикаций соискателя

[1-А] Ващук, Д. В. Распределенный анализ криптовалютного Blockchain / Д. В. Ващук // Компьютерные системы и сети : материалы 52-й научной конференции аспирантов, магистрантов и студентов. (Минск, 25 - 30 апреля 2016 года). – Минск : БГУИР, 2016. – С. 21 - 23.