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

УДК 004:[336.76+336.743]

Моисеенко
Георгий Сергеевич

Электронная биржа по торговле токенами

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

Научный руководитель

Ганжа Виктор Александрович

к.ф.-м.н., доцент

Минск 2020

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи исследования

Объектом исследования является распределенная система хранения данных, которая используется для хранения транзакций биржи.

Предметом исследования выступают алгоритмы, решающие задачу построения блоков транзакций в системе блокчейн и их подтверждения.

Цель работы состоит в исследовании технологии блокчейн и механизмов достижения консенсуса при построении блоков, а также разработке распределенной системы хранения данных по технологии блокчейн.

В соответствии с поставленной целью, можно выделить следующие **задачи**:

– обзор существующих распределенных систем хранения данных;

– теоретическое обоснование выбора технологии блокчейн в качестве распределенной системы хранения данных;

– разработка защищенной распределенной системы хранения данных для транзакций биржи;

Апробация диссертации

Результаты исследований по теме диссертации были представлены в виде доклада «Технология блокчейн для электронной биржи по торговле токенами» на 56-ой научной конференции аспирантов, магистрантов и студентов БГУИР в 2020 году в Минске.

Публикация результатов исследований

Результаты исследований опубликованы в виде тезисов доклада на 56-ой научно-технической конференции аспирантов, магистрантов и студентов БГУИР, которая проходила в апреле 2020 в Минске. Тема тезисов: «Технология блокчейн для электронной биржи по торговле токенами».

ВВЕДЕНИЕ

Современному человеку тяжело представить мир без привычных ему вещей, будь то смартфон, электрочайник или иной другой предмет быта или досуга. Человечество всегда стремилось совершенствовать окружающее его пространство, а также делать свою жизнь проще. Каждый день изобретаются новые технические устройства, строятся новые корабли и открываются новые горизонты в различных сферах человеческой жизни. Все это было бы невозможно без объединения людей в группы единомышленников, стремящихся воплотить свою мечту в реальность. В то же время перед многими изобретателями встает вопрос о целесообразности и финансировании проекта. В связи с чем остро встает вопрос о получении финансовой поддержки со стороны общества.

Как правило компании получают финансирование от узкого круга лиц в ограниченном объеме. Некоторые компании, в виде акционерных обществ, стремятся получить большую финансовую поддержку распространяя активы компании через биржу. Однако эта возможность доступна только крупным компаниям, а покупка акций – только состоятельным инвесторам и людям, вращающимся в специальных кругах.

В связи с этим в рамках магистерской работы определена следующая цель – разработать программное средство, реализующее возможность выпуска и продажи активов любых компаний для любых лиц и предоставляющее удобный интерфейс пользователя.

Важно, чтобы система была защищена от возможных сбоев аппаратуры или попыток подделки данных, а также являлась надежным источником хранения данных. Для удовлетворения этих условий сегодня существует множество технологий и решений как централизованных, так и децентрализованных. В последнее время популярность снискали именно децентрализованные хранилища ввиду своей доступности и повышенной надежности. Однако данные технологии в массе своей не лишены проблем, связанных с защитой информации и возможностью ее компрометирования.

Особое место среди децентрализованных систем занимает технология блокчейн, которая обладает всеми необходимыми характеристиками как распределенность данных, их неизменность, а также практически полная невозможность подделки или уничтожения данных путем атаки злоумышленника.

Идея технологии блокчейн была описана еще в 1991 году, когда ученые-исследователи Стюарт Хабер и У. Скотт Шторнетта внедрили вычислительно-практическое решение для цифровых документов с штампом времени, чтобы они не могли быть оформлены задним числом или подделаться [1].

Система использовала криптографически-закрепленную цепочку блоков, для хранения документов с отметкой времени, а в 1992 году деревья Меркла были включены в разработку, что сделало ее более эффективной, позволив собирать несколько документов в один блок. Однако эта технология не использовалась, и патент был упущен в 2004 году, за четыре года до создания Биткойна.

Данная технология может использоваться и уже имеет практическое применение в таких сферах как банковский сектор, земельный реестр, удостоверение личности и др.

Разрабатываемое программное средство может стать удобным и востребованным сервисом для молодых быстрорастущих компаний и людей, желающих заняться инвестированием.

Стоит отметить, что данная работа имеет практическую связь с такими направлениями, как распределенные системы и криптографические алгоритмы, ввиду чего является актуальной.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В **общей характеристике работы** сформулированы цель и задачи исследования, даны сведения об объекте и предмете исследования, приведены апробации и публикации результатов.

Во **введении** дается обоснование актуальности работы, описываются прикладные задачи, в которых может быть использована разработанная система, приводится краткий перечень требований к ней.

В **первой главе** производится подробный обзор основных характеристик систем хранения данных, проблем, порождаемых выставляемыми требованиями, а также их решения. Также рассматривается множество существующих технологий, представленных на рынке, их преимущества и недостатки. Выполняется формализация задачи исследования, а также формируется основная идея электронной биржи для торговли токенами.

Во **второй главе** производится теоретическое обоснование технологии блокчейн для построения децентрализованного распределенного хранилища данных, описываются основные аспекты построения цепочки блоков, а также механизмы достижения согласованности узлов сети. Дается подробное описание структуры блоков и алгоритмов подтверждения подлинности транзакций.

В **третьей главе** приводится подробное описание разработанного приложения. В разделе описываются основные шаги разработки подобных систем, а также приводятся промежуточные результаты испытаний различных механизмов, разработанных в системе.

В **заключении** производится краткий обзор результатов исследования, приводится обоснование выбранных методов и инструментов, дается критический анализ разработанной системы и приводятся описание проблем, которые могут более успешно решены в будущих исследованиях.

ЗАКЛЮЧЕНИЕ

В ходе исследования был произведен обширный обзор предметной области. Был проведен тщательный анализ основных решений распределенных систем хранения данных, представленных на рынке на данный момент. Каждая из рассмотренных технологий обладает своим преимуществами и недостатками, поэтому по результатам исследования было решено использовать технологию блокчейн как систему, наиболее удовлетворяющую выставляемым требованиям.

Для более полного понимания объекта исследования был проведен глубокий анализ как самой структуры построения цепочки блоков, так и алгоритмов, обеспечивающих согласованность и безопасность системы. Полученные знания нашли отражение в выбранном алгоритме достижения консенсуса. Для проведения испытаний и дальнейшего анализа результатов было решено использовать один из наиболее популярных алгоритмов – доказательство работы.

При выборе инструментов для создания блокчейна было исследовано множество существующих библиотек и фреймворков, существующих на рынке. Однако, для наиболее полного понимания всех аспектов технологии и одновременной демонстрации простоты реализации столь высокоустойчивой системы было решено реализовать ее с нуля, ограничившись лишь несколькими библиотеками для реализации общения узлов сети посредством HTTP запросов, а также шифрования информации.

Использование одной из методик для согласования узлов, позволило реализовать высокопроизводительную систему, а также оценить ее преимущества и недостатки. На примере реализации транзакций биржи была продемонстрирована варьиативность использования технологии блокчейн, а также возможность ее использования в реальном мире.

Данная система будет использована в качестве основы для будущих исследований. В дальнейших работах планируется добавить возможность использования более продвинутых алгоритмов достижения консенсуса для более эффективного противодействия централизации системы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Список публикаций соискателя

[1 – А.] *Моисеенко, Г. С.* Использование технологии блокчейн для электронной биржи по торговле токенами / Г.С. Моисеенко // Компьютерные системы и сети: 56-ая научная конференция аспирантов, магистрантов и студентов, Минск, 21-22 апреля 2020 г. — Минск : Белорусский государственный университет информатики и радиоэлектроники, 2020. — С. 47.