БЕЗОПАСНОСТЬ КОММУНИКАЦИЙ В МУЛЬТИАГЕНТНЫХ СИСТЕМАХ

Студент 4 курса группы 5 КБ Добринский И. С.

Научный руководитель – кандидат физико-математических наук, доцент Козлова Е. И.

Белорусский Государственный Университет

Минск, Беларусь

В настоящее время мультиагентные системы (МАС) используются в различных сферах деятельности человека, таких как бизнес, производство, государственное управление, здравоохранение и социальная сфера, и даже при анализе почты на персональном компьютере.

К числу задач, которые могут быть решены с помощью МАС относятся задачи понимания смысла текстов на естественном языке, анализ данных для обнаружения скрытых знаний при принятии решений; обучение компьютерных систем путем выявления предпочтений и построения моделей поведения пользователя, и множество других.

Мультиагентные системы – это децентрализованные системы, в которых результат достигается в процессе распределенного взаимодействия множества агентов – автономных программных или программно-аппаратных объектов, нацеленных на поиск возможно не оптимального, но наилучшего из возможных решений на каждый момент времени. Если найденный агентом лучший вариант уже забронирован другим агентом, агенты оказываются способными выявить конфликт и разрешить его путём переговоров, в ходе которых достигается компромисс, отражающий временное, и, как правило, неустойчивое равновесие (баланс) их интересов.

Обеспечение безопасности МАС при этом представляет сложную задачу из-за наличия большого числа агентов, обеспечивающих сбор и передачу блоков данных, их удаленности и физической незащищенности, а также

возможности внешнего вмешательства в собственно процесс передачи данных.

Несмотря на наличие в большинстве протоколов беспроводной передачи данных средств криптографической защиты и политик безопасности, это не гарантирует неуязвимость отдельных узлов и мультиагентных систем в целом.

Целью данной работы является исследование применения блокчейна в мультиагентных системах и разработка алгоритма безопасной коммуникации агентов, проверка и оценка его работоспособности в симуляции реактивной мультиагентной системы.

Почему как протокол общения между агентами был выбран блокчейн? Блокчейн — это особая структура данных, применяемая для создания децентрализованного регистра. Блокчейн состоит из блоков (block), особым образом соединенных в цепочку (chain). Блок содержит набор транзакций, хеш предыдущего блока, метку времени (время создания блока), сумму отчисления майнеру за блок и т. д. Поскольку каждый блок содержит хеш предыдущего блока, они связаны в цепочку. Также блокчейн считается безопасным по ряду причин: *Децентрализация:* Информация хранится на множестве компьютеров, и каждый узел имеет копию всей или части цепочки блоков. Это делает систему менее уязвимой к атакам, поскольку злоумышленнику нужно изменить данные на многих устройствах одновременно.

Криптография: Блокчейн использует криптографические методы для обеспечения безопасности. Каждый блок содержит хеш (кодовое представление) предыдущего блока, что делает манипуляции данными сложными без изменения всей цепочки блоков.

Неизменяемость: Как только информация записана в блок, изменение этого блока требует согласия большинства участников сети. Это делает изменение данных практически невозможным без обнаружения.

Консенсус: Принятие изменений в блокчейне происходит на основе протоколов консенсуса, таких как Proof of Work (доказательство выполнения

работы) или Proof of Stake (доказательство доли), что требует согласия большинства участников сети.

Прозрачность: Все транзакции видны всем участникам блокчейн сети, что увеличивает прозрачность и делает манипуляции с данными более сложными.

Принцип работы блокчейна заключается в создании цепочки блоков, содержащих данные о транзакциях или других данных, например сообщениях. На рисунке 1 можно увидеть, что принцип (алгоритм) состоит из 5 основных этапов.

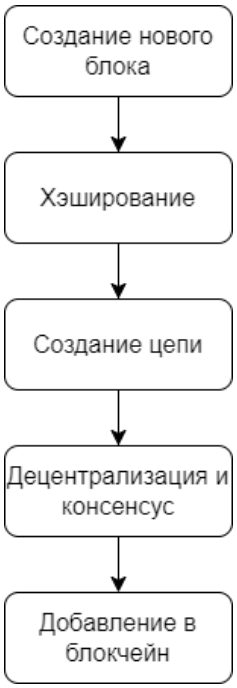

Рисунок 1 – Общий вид алгоритма работы блокчейна

1. Создание нового блока: Новый блок создается, когда определенное количество транзакций готово для добавления в цепь. Новый блок содержит информацию о транзакциях, временные метки и ссылку на предыдущий блок в цепи.

2. Хеширование: Данные в каждом блоке хешируются с использованием криптографических функций. Хеш блока представляет собой уникальную цифровую подпись содержимого блока.

3. Создание цепи: Каждый блок включает в себя хеш предыдущего блока, формируя цепь блоков. Это обеспечивает целостность и устойчивость блокчейна, поскольку изменение данных в одном блоке потребует изменения всех последующих блоков.

4. Децентрализация и консенсус: Новый блок передается по сети узлам, которые подтверждают его достоверность и валидность. Этот процесс обеспечивает консенсус в сети и подтверждает действительность нового блока.

5. Добавление в блокчейн: После подтверждения новый блок добавляется в цепь и становится частью общедоступной и неизменяемой базы данных.

Этот процесс повторяется для каждого нового блока, что создает постоянно растущую цепь блоков с уникальными хешами, обеспечивая прозрачность, целостность и безопасность данных.

Следующий этап проектирования алгоритма заключается в создании мультиагентной системы, за основу которой будет взята peer-to-peer (p2p) сеть. Данная сеть лучшим образом описывает мультиагентную систему, так как каждый участник сети равноправен и способен обмениваться информацией с любым участником данной сети напрямую, без участия центрального сервера.

Изучив теоретическую часть работы можно приступить к разработке мультиагентной система и алгоритма блокчейна. В результате выполненной работы была создана простая реализация алгоритма блокчейна, включающая в себя три основных класса: Message, Block и Blockchain. Дополнительно были разработаны классы для сетевой инфраструктуры: Agent и P2Pnetwork. После проведения тестирования этих классов можно ожидать демонстрации их работоспособности и потенциала применения алгоритма блокчейна в мультиагентных системах в перспективе.

На рисунке 2 приведена блок-схема алгоритма тестирования приложения [1].

Заключение

В работе рассмотрена проблема обеспечения безопасности в мультиагентных системах (МАС), исследован и разработан алгоритм блокчейна, рассмотрены его основные этапы и P2P сеть для обеспечения безопасной коммуникации между агентами. Блокчейн был выбран в качестве протокола обмена данными, благодаря своей децентрализации, криптографической защите, неизменяемости данных и механизмам консенсуса. Разработанный алгоритм блокчейна и P2P сеть успешно подтвердили свою работоспособность, обеспечивая целостность, прозрачность и безопасность обмена информацией в среде с множеством агентов.

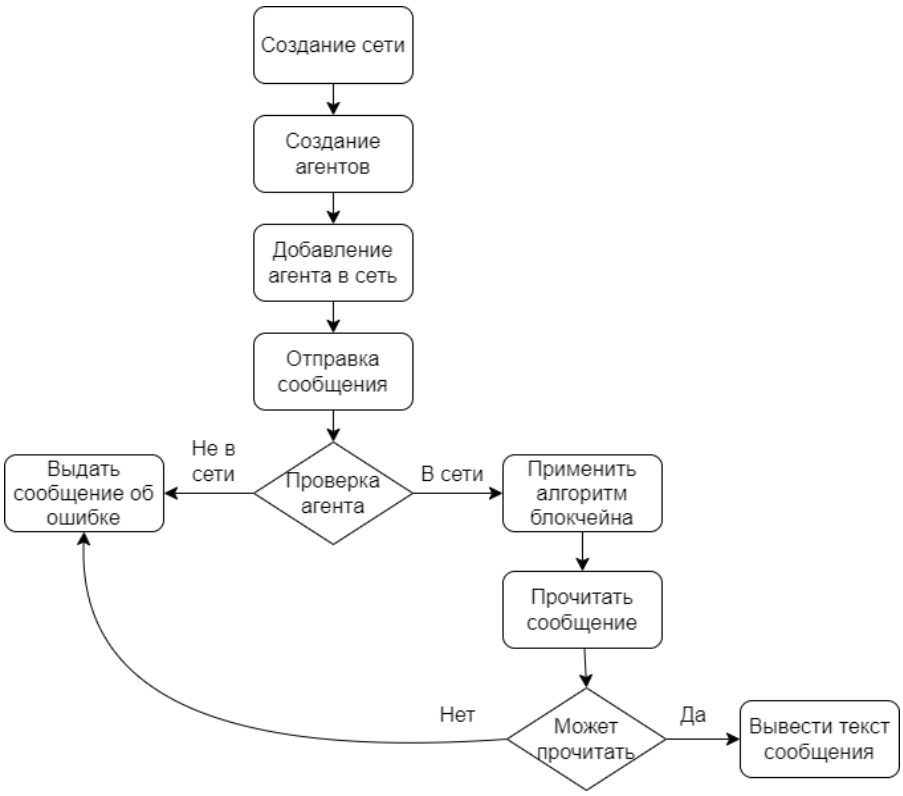

Рисунок 2. Алгоритм тестирования

Литература

1. Добринский Илья: Курсовая работа “Безопасность коммуникаций в мультиагентных системах”. – БГУ, Минск. – 2023.