УДК 004.75

РАЗРАБОТКА АЛГОРИТМА КОНСЕНСУСА С КОНСТАНТНЫМ ВРЕМЕНЕМ ВАЛИДАЦИИ ТРАНЗАКЦИЙ В ДЕЦЕНТРАЛИЗОВАННЫХ IOT СЕТЯХ

Курако А.Е. (Университет ИТМО, Санкт-Петербург)
Научный руководитель - доцент, Быковский С.В.
(Университет ИТМО, Санкт-Петербург)

В работе рассматривается создание алгоритма консенсуса для валидации транзакций за константное время в децентрализованных IoT сетях. Рассмотрены существующие протоколы и механизмы обеспечения консенсуса в блокчейн системах. Спроектирован устойчивый алгоритм консенсуса для децентрализованных сетей, который может быть реализован на устройствах с малыми вычислительными ресурсами.

Введение. В настоящее время актуальной задачей является обеспечение надежного и безопасного взаимодействия устройств друг с другом. Это позволит реализовать возможность осуществления финансовых сделок между устройствами посредством обмена транзакциями на базе децентрализованной сети взаимодействия. Поддержка такой возможности будет являться следующим шагом развития индустрии IoT устройств. В данной работе предложен алгоритм консенсуса, позволяющий обеспечить безопасный обмен транзакциями с константным временем валидации для устройств с малыми вычислительными ресурсами.

Основная часть. Несмотря на большое количество протоколов и механизмов консенсуса в блокчейн системах, все они не предусмотрены для использования в IoT системах, так как не учитывают специфику устройств данных систем. Устройства в IoT системах не обладают большим количеством вычислительным ресурсов и имеют, зачастую, процессоры с не высокими показателями производительности и малый объем памяти. Это особенность исходит из необходимости удовлетворения требования к низкому энергопотреблению и возможности непрерывной работы от батарейки.

Разработка алгоритма консенсуса с константным временем валидации позволит строить крупные децентрализованные системы для IoT устройств.

В данной работе проведен анализ блокчейн-системы IOTA, его подходов в организации топологии сети, валидации транзакций нодами и векторы атак. Данная система использует подход валидации транзакций по средствам константного времени для всех участников сети. Рассмотрены подходы разработчиков, которые позволяют исключить атаку Сивиллы на блокчейн систему.

Проведен анализ механизма консенсуса Avalanch, который позволяет обеспечить свойства высокой доступности и финализации транзакций.

На базе преимуществ рассмотренных механизмов консенсуса предложен собственный алгоритм, оптимизированный для использования в децентрализованных IoT сетях.

Выводы. Реализация алгоритма консенсуса с константным временем валидации транзакций сделает возможной организацию сложных децентрализованных систем с обменом транзакций для IoT устройств. Это впоследствии позволит реализовывать финансовые отношения между такими устройствами. Были проанализированы и исследованы существующие блокчейн системы для IoT устройств, выделены их слабые и сильные стороны. Было установлено, что существующие решения обладают существенными недостатками, но проанализированные ошибки в их проектировании позволили спроектировать собственный алгоритм консенсуса. В дальнейшем планируется реализация прототипа децентрализованной системы с использованием такого алгоритма и сравнение с существующими аналогами.

Курако А. Е. (автор)

Быковский С.В. (научный руководитель)