УДК 004.75

РЕАЛИЗАЦИЯ КРИПТОВАЛЮТЫ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ С ФЕДЕРАТИВНЫМИ КВОРУМАМИ

Королева А.С., Университет ИТМО, Санкт-Петербург
Научный руководитель – PhD, Кузнецов П.В., Университет ИТМО, Санкт-Петербург

В рамках работы были изучены существующие подходы реализации криптовалюты с использованием федеративной системой кворумов. Была изучена реализация криптовалюты с отсутствием консенсуса. Была предложена реализация криптовалюты без консенсуса в федеративной системе кворумов, и исследована проблема двойного расходования в таких настройках.

Введение. В последнее время тема криптовалют набирает все большую популярность. Криптовалюта является разновидностью цифровой валюты, и ее реализация подразумевает, что обработка состояния системы происходит автоматически и распределенно. Основным элементом существующих реализаций является консенсус, то есть алгоритм, позволяющий достичь согласия между всеми участниками процесса. Алгоритм консенсуса может быть реализован с использованием систем кворумов. Интуитивно, система кворумов определяет, каким множествам процессов можно доверять при возможных вариантах исполнения. Недавно предложенные модели рассматривают ситуации, в которых нет центральной системы кворумов, и каждый процесс решает самостоятельно, кому он будет доверять. Этот подход получил название "федеративных систем кворумов". Все предложенные модели криптовалют рассматривают консенсус как основной блок построения алгоритма. Относительно недавно было показано, что для реализации криптовалюты консенсус не обязателен, что облегчает требования к системе. В рамках работы мы изучаем проблему внедрения криптовалюты в установке федеративных кворумов без использования консенсуса.

Основная часть. В современных реализациях криптовалюты алгоритм консенсуса используется для упорядочивания и подтверждения транзакций участниками. Это необходимо для того, чтобы предотвратить проблему двойного расходования, то есть ситуацию, когда одну и ту же единицу валюты тратят дважды. Проблема реализации алгоритма консенсуса с использованием фиксированной системы кворумов заключается в том, что участники системы должны быть известны в начале процесса. Для криптовалюты же важна открытость, то есть новые участники должны иметь возможность присоединяться к процессу в любой момент времени. Были предложены разные подходы, одним из них является использование федеративных систем кворумов, реализованный в криптовалютах Ripple XRP и Stellar.
Однако, как недавно было показано Гирауи и др. (Guerraoui et al., PODC 2019) , для реализации криптовалюты глобальное упорядочивание транзакций необязательно. Участники формируют свое локальное видение глобальной истории, и на основе этого самостоятельно принимают решение об одобрении новой транзакции. Тем не менее решение подразумевает использование фиксированной системы кворумов. Подходом, позволяющим решить эту проблему, является применение федеративных настроек системы.
Основным строительным блоком реализации криптовалюты без консенсуса является надежная широковещательная отправка сообщений, использующая систему кворумов. В существующих статьях было показано, что в федеративных настройках возможна реализация ослабленной версии широковещательной отправки сообщений. Степень ослабленности зависит от важного свойства – пересекается ли каждые два кворума по корректному участнику системы. Кашан и Такман (Cachin and Tackman, OPODIS 2019) показали, что если это свойство в системе есть, то проблема двойного расходования отсутствует. При этом участники, доверяющие злонамеренным, потенциально могут видеть историю лишь частично, или же их аккаунты могут заблокироваться. Существует множество участников, которые видят полную историю транзакций, и их транзакции не блокируются. Если такое свойство отсутствует, то в

системе есть возможность двойного расходования (как и в существующих реализациях криптовалют, использующих федеративные системы кворумов). Была найдена верхняя граница на двойное расходование, зависящая от конфигурации системы.
Важной проблемой реализации криптовалюты без консенсуса, приведенной в статье, является бесконечно растущее внутреннее состояние участников системы. Предложенная реализация в федеративных настройках не избавляется от этой проблемы.

Выводы. После разрешения проблемы бесконечно растущего состояния участников системы предложенный подход может быть использован в реализациях криптовалют, что позволит упростить и ускорить процесс обработки транзакций.