УДК 004.75

БЕЗОПАСНОСТЬ ВНЕШНИХ ТРАНЗАКЦИЙ В УСТОЙЧИВЫХ РАСПРЕДЕЛЕННЫХ РЕЕСТРАХ НА ОСНОВЕ МНОГОМЕРНОГО БЛОКЧЕЙНА

Шилов И.М.
(Санкт-Петербург, Университет ИТМО)
Научный руководитель – к.т.н., доцент, декан факультета БИТ, Заколдаев Д.А.
(Санкт-Петербург, Университет ИТМО)

Аннотация. Доказательство безопасности протокола поиска и верификации занимает существенное место в процессе доказательства безопасности многомерного блокчейна. В исследовании использован гибридный симуляционный подход, основанный на фреймворке универсальной композиции, для формального доказательства безопасности распределенных реестров на основе многомерного блокчейна. При доказательстве применяется усовершенствованная GUC-модель многомерного блокчейна.

Введение. Устойчивые распределенные реестры все чаще применяются в различных сферах научной и практической деятельности для решения проблемы безопасного обмена информацией в условиях ненадежности среды передачи данных и при наличии атакующих. Автором был предложен подход для построения устойчивых распределенных реестров – многомерный блокчейн – который является обобщением понятия одномерного блокчейна и решает некоторые характерные для него проблемы. Была математически доказана безопасность механизмов достижения консенсуса в рамках многомерного блокчейна, а также (с использованием UC-фреймворка) безопасность самого многомерного блокчейна. Однако доказательство было основано на существенном предположении – о наличии безопасного протокола поиска и верификации информации в пределах многомерного блокчейна. Целью данной работы является доказательство безопасности без использования данного предположения.

Основная часть. Для доказательства безопасности и устойчивости распределенных реестров на основе многомерного блокчейна используется UC-фреймворк. Построенная ранее модель была модифицирована для целей доказательства безопасности протокола поиска и верификации. Доказательство произведено с использованием гибридных моделей. При этом осуществляется последовательный переход между различными представлениями многомерного блокчейна, когда отдельные компоненты протокола заменяются на так называемые идеальные функционалы. Для всех представлений последовательно доказывается эквивалентность. Путем подобного перехода возможно доказать безопасность всей технологии, т.е. эквивалентность распределенного реестра на основе многомерного блокчейна и идеального функционала, реализующего устойчивый распределенный реестр (реестр, обладающий свойствами стойкости и живости). В работе представлено формальное описание всех используемых гибридных моделей, а также формализован переход между этими моделями.

Выводы. В работе доказана безопасность внешних транзакций и протокола поиска и верификации в многомерном блокчейне. Полученные результаты могут быть использованы для построения устойчивых распределенных реестров на основе многомерного блокчейна. Доказательство безопасности может быть усовершенствовано при введении в модель новых алгоритмов выбора источников информации при внешнем взаимодействии и при использовании кэширования.