УДК 004.75

UC-БЕЗОПАСНОСТЬ МНОГОМЕРНОГО БЛОКЧЕЙНА

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

Несмотря на постепенно спадающий интерес к криптовалютам и лежащему в их основе блокчейну, актуальность развития распределенных и децентрализованных систем не вызывает сомнений в научной среде и в бизнесе. Крупные организации стремятся адаптировать блокчейн для построения устойчивой информационной инфраструктуры. Одной из проблем данной технологии является слабая масштабируемость и отсутствие механизмов для сокращения затрат памяти вычислительных узлов. Кроме того, не решена проблема безопасного обмена информацией между системами, основанными на блокчейне. Одним из способов решения данной проблемы является применение многомерного блокчейна.

Целью работы является доказательство безопасности многомерного блокчейна как средства реализации устойчивого распределенного реестра с использованием фреймворка универсальной композиции. Данный фреймворк в последние годы приобрел популярность при исследовании децентрализованных систем и криптографических протоколов с нулевым разглашением. На его основе было построено доказательство некоторых систем на основе блокчейна – например, Hawk. Каждая система в UC-фреймворке представляется в виде набора взаимодействующих интерактивных машин Тьюринга.

В работе рассматриваются существующие UC-модели одномерных блокчейнов – Bitcoin и различных модификаций механизма достижения консенсуса Ouroboros. С использованием данных моделей производится построение модели многомерного блокчейна в терминах UC-фреймворка, исследуются накладываемые на нее ограничения. Построение модели предполагает написание программ для интерактивных машин Тьюринга, что позволяет выявить недостатки модели на этапе ее проектирования.

На основе специального математического аппарата и методов теории вычислений доказывается реализация многомерным блокчейном устойчивого реестра с определенной вероятностью, а также безопасность проведения внешних транзакций, т.е. транзакций между отдельными блокчейнами.

В результате работы многомерный блокчейн формализуется с использованием нотации фреймворка универсальной композиции. Тем самым закладывается основа для дальнейшей его реализации. Доказываются важные теоремы о безопасности решения и его отдельных компонентов. Наконец, открываются новые пути исследования некоторых компонентов многомерного блокчейна, в частности, протокола обмена информацией о транзакциях между реестрами. Построение безопасного многомерого блокчейна позволит масштабировать распределенные реестры, а также объединять их в единую систему без ущерба для безопасности.