УДК 004.4'242

Использование методов синтеза конечных автоматов для автоматической генерации моделей смарт-контрактов

Суворов Д. М., Университет ИТМО, Санкт-Петербург
Научный руководитель – Ульянцев В. И., к.т.н., доцент факультета ИТиП

Введение

В последнее время приобретают популярность блокчейн-системы. Это объясняется тем, что они позволяют поддерживать полностью распределенную базу данных без участия доверенного лица, гарантируя при этом надежность и целостность системы. Современные блокчейн-системы поддерживают создание смарт-контрактов – программного кода, хранящегося в системе и обеспечивающего соблюдение некоторой договоренности [1]. Таким образом предоставляется платформа для разработки распределенных приложений, корректное исполнение которых достигается за счет принципов безопасности этой платформы.

Однако, гарантируется лишь корректное исполнение смарт-контрактов, а не то, что написанный программный код корректен. Более того, смарт-контракты оперируют значительными объемами криптовалют, что делает их привлекательной мишенью атак, а дизайн блокчейн-систем не позволяет обновить смарт-контракты и отменить совершенные транзакции [2]. Поэтому актуальна проблема проектирования корректных (удовлетворяющих спецификации, заданной пользователем) смарт-контрактов.

Цель работы

1. Обзор существующих методов формальной верификации и автоматической генерации смарт-контрактов.
2. Анализ применимости методов синтеза конечных автоматов на основе сценариев поведения и формальной спецификации для генерации моделей смарт-контрактов.
3. Использование данных методов для автоматической генерации смарт-контрактов, удовлетворяющих заданной спецификации.

Описание предлагаемого подхода

В работе предлагается использование существующего метода синтеза конечных автоматов на основе сценариев поведения и формальной спецификации для автоматической генерации моделей смарт-контрактов. Данный подход основан на сведении задачи поиска автомата, удовлетворяющего заданным критериям, к задаче выполнимости булевой формулы [3]. Анализируется несколько широко применимых типов смарт-контрактов, логика которых может быть смоделирована при помощи конечных автоматов, после чего предложенный подход применяется для генерации моделей и верификации рассмотренных контрактов. С помощью повышения уровня абстракции и моделирования некоторых аспектов блокчейн-систем верифицируются специфичные для них свойства.

Литература

1. Wood G. Ethereum: A secure decentralised generalised transaction ledger //Ethereum project yellow paper. – 2014. – Т. 151. – С. 1-32.
2. Delmolino K., Arnett M., Kosba A., Miller A., Shi. E. Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab //International Conference on Financial Cryptography and Data Security. – Springer, Berlin, Heidelberg, 2016. – С. 79-94.
3. Ulyantsev V., Buzhinsky I., Shalyto A. Exact finite-state machine identification from scenarios and temporal properties //International Journal on Software Tools for Technology Transfer. – 2018. – Т. 20. – №. 1. – С. 35-55.