

Формальная верификация в блокчейн-системах

Даня Рогозин

В докладе мы рассмотрим проблему построения общей модели блокчейн-системы (и мотивацию) и возможности математической логики и функционального программирования в верификации свойств данных систем на примере разработки фреймворка, предназначенного для проектирования криптовалют. Формализация общей модели блокчейн системы предполагает использование системы типов языка Haskell, а формальная верификация — систему так называемых зависимых типов, реализованных в языке Agda, а в данном докладе мы опишем основные идеи, позволяющие реализовать данную цель.