NTATRUST 简介

智能合约和区块链协议是用诸如 Solidity、C / C ++、Java 和 Go 等语法语义丰富的编程语言开发。这些图灵完备的语言意味着它们具有很强的表达能力和灵活性。其代价是几乎所有测试验证的问题都是不可判定的。所以无法开发出基于单一技术来确保区块链生态系统的质量的软件工具。因此，我们提出一种综合了多种系统分析方法优势的整体解决方案。

NTATRUST 是区块链生态系统的质量保证平台，可以验证效率属性和功能属性（包括正确性和安全性）。该平台基于五项核心技术，包括动态分析、模糊测试、符号执行、模型检测和静态分析，它们可以协同工作优势互补。

动态分析引擎 *NtaDyamic* 不仅仅在给定输入下监察程序执行，还通过对程序行为的预测分析来检测缺陷。根据当前程序行为，它能够推导出一个包含未测试行为的预测模型。*NtaDyamic* 能够使用约束求解检测隐藏在预测模型中的缺陷，从而避免运行这些程序行为的额外开销。

模糊测试引擎 *NtaFuzzy* 能够揭示被区块链开发人员忽视的许多严重缺陷，该方法有很高的性价比。它通过为测试对象生成大量输入数据（称为种子）来实现。NtaFuzzy 利用静态分析技术和约束求解技术，大大提高了种子质量, 从而能够更大概率的发掘缺陷。

符号执行引擎 *NtaSymbolic* 设定输入为符号值，而不是常规执行时的具体值。它可以系统地搜索程序路径并检查边角情况。具体来说，*NtaSymbolic* 利用自定义的符号执行算法来枚举影响功能属性和性能属性的路径，包括由回退函数引起的路径。

模型检测引擎 *NtaFormal* 能够证明一个属性在所有可能的执行环境下都成立。当功能属性或性能属性成立时，它能够生成数学证明。 *NtaFormal* 包括三个创新组件：用于捕获智能合约或区块链协议的精确语义的模型构建器、用于描述各种功能属性和性能属性的框架，以及一组有效验证模型属性的算法，包括使用完全自动抽象和精化技术。

静态分析引擎 *NtaStatic* 在不执行程序的情况下检查源代码。该工具有助于更好的理解代码结构，并确保代码符合行业标准。*NtaStatic* 设计了专门的算法来检查和评估智能合约和区块链协议源代码的各个方面。

综上所述，*NtaDyamic* 和 *NtaFuzzy* 在计算上非常高效。*NtaDyamic* 可以预测固定输入下的缺陷行为，而 *NtaFuzzy* 自动改变输入以监控更多的程序行为。 *NtaSymbolic* 利用更全面和系统的技术来检查程序路径并发现不易发现的缺陷。这三种方法分析的行为构成了实际程序行为的正确下近似。另一方面，*NtaStatic* 和 *NtaFormal* 专注于 程序行为的正确过近似。因此，在NTATRUST 内部，*NtaStatic* 和 *NtaFormal* 适用于 证明属性正确性，而 *NtaDyamic*、*NtaFuzzy* 和 *NtaSymbolic* 适用于检测属性违规性。