

VALIDACIÓN Y TRANSFORMACIÓN DE CONTRATOS INTELIGENTES A SOLIDITY

Integrantes: Anabella Pessini, Valentina Rio, Lorena Baigorria, Ana Garis

Universidad Nacional de San Luis

Departamento de Informática, Facultad de Ciencias Físico Matemáticas y Naturales

Problema

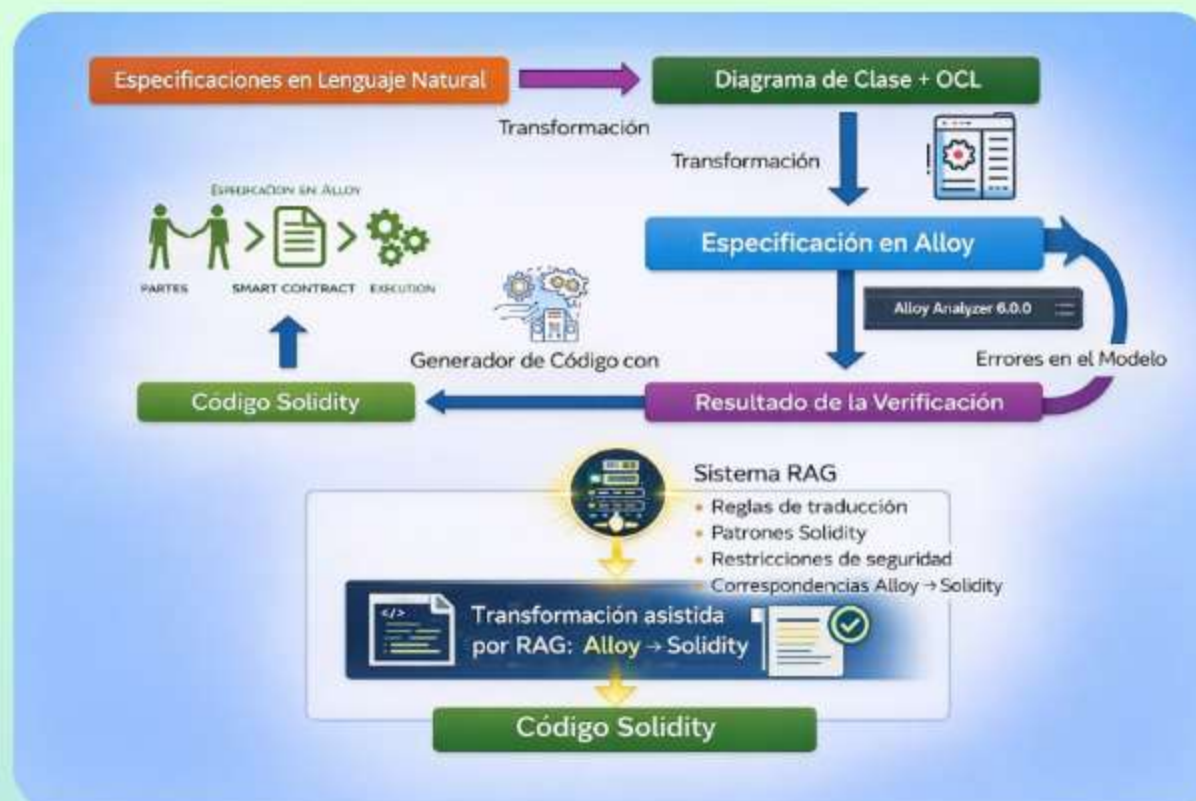
Los contratos inteligentes requieren alta precisión debido a la inmutabilidad de la blockchain. Sin embargo, la ambigüedad en la especificación y los errores de implementación pueden derivar en fallos críticos.

Propuesta

Se propone un enfoque basado en Ingeniería Dirigida por Modelos (MDE) que permite especificar contratos mediante UML/OCL, verificarlos en Alloy y generar automáticamente código en Solidity utilizando RAG.

Metodología

El enfoque propuesto integra modelado, verificación formal y generación automática de código en un flujo continuo.



Resultados Esperados

- Integración de UML/OCL con Alloy para reducir la brecha entre el modelado y la verificación formal.
- Automatización de la verificación de propiedades sin intervención manual intensiva.
- Detección temprana de inconsistencias, reduciendo costos en etapas posteriores.
- Viabilidad de la generación automática de contratos inteligentes en Solidity a partir de modelos formales, mediante RAG.

Validación

- Evaluación de la calidad del código generado (claridad estructural y adecuación al dominio)
- Correspondencia semántica entre la especificación formal y el contrato generado
- Validación por expertos del dominio para verificar coherencia funcional
- Verificación formal complementaria mediante búsqueda de contraejemplos
- Análisis mediante traducción inversa para contrastar el contrato generado con la especificación original.

Conclusión

El enfoque propuesto reduce la brecha entre la especificación formal y la implementación, mejorando la confiabilidad de los contratos inteligentes.

Proyecto de Investigación

Ingeniería de Software: Estrategias de Desarrollo, Mantenimiento y Migración de Sistemas en la Nube

Director: Dr. Daniel Riesco

- Línea 1: Desarrollo de Estrategias de Mantenimiento que Preserven la Calidad y Seguridad los Sistemas de Software que Ejecutan en la Nube.

Director de Línea: Dr. Mario Marcelo Berón.

- Línea 2: Desarrollo de Métodos, Estrategias y Herramientas de Migración Preventiva de Sistemas de Software que Ejecutan en la Nube.

Director de Línea: Dr. Germán Antonio Montejano.