

Verificação de *smart contracts* no lado do consumidor

Proposta de dissertação de mestrado

Orientador: Simão Melo de Sousa

1 Objetivos

O objetivo desta proposta é desenvolver um mecanismo que permita a verificação de propriedades de *smart contracts* para a blockchain Tezos no lado do consumidor com esforço minimal, através de *abstraction carrying code*[1].

Este tipo de técnicas permitem que um consumidor de um determinado programa possa verificar automaticamente que este cumpre certos requisitos através de um *certificado* gerado e fornecido pelo programador. Para tal, é esperado que o aluno utilize métodos de análise estática e interpretação abstrata por forma a extrair o comportamento e propriedades de um *smart contract* e desenvolva um mecanismo que permita a verificação automático do *smart contract* no lado do consumidor de acordo com uma política definida por este.

Assim, é esperado deste trabalho uma *framework* bi-partida que permita (1) gerar um *certificado* de um *smart contract* do lado do programador e (2) permitir a verificação do *smart contract* associado a esse *certificado* pelo consumidor com esforço reduzido.

2 Tarefas a realizar e cronograma

<i>Tarefa</i>	<i>Descrição</i>	<i>Tempo de execução</i>
T1:	Estudo do estado da arte em análise estática e interpretação abstrata de <i>smart contracts</i> , <i>abstraction carrying code</i> .	2 meses
T2:	Implementação de análises <i>proof-of-concept</i> .	2 meses
T3:	Desenvolvimento da plataforma de verificação através de <i>abstraction carrying code</i> .	2,5 meses
T4:	Validação e análise dos resultados.	1 mês
T5:	Escrita do relatório do projeto.	1,5 meses

3 Resultados esperados

- 1 protótipo de uma *framework* de verificação de *smart contracts* Tezos;
- 1 relatório do projeto.

4 Contact

Simão Melo de Sousa (desousa@di.ubi.pt)

5 Referências

[1] V. Rodrigues, B. Akesson, M. Florido, S. Melo de Sousa, J. P. Pedroso, P. Vasconcelos. Certifying Execution Time in Multicores. Science of Computer Programming Journal, Elsevier. 46 pages. 2015.