Tezos Blockchain Security Enforcement
Part 1: Language Based Security

Proposta de Mestrado

Orientador: Simão Melo de Sousa
Co-orientador Paul Crocker

1 Contexto

Propomos nesta proposta de dissertação o estudo e a implementação de mecanismos de segurança acrescida na blockchain Tezos.

Tezos é uma blockchain que pode evoluir atualizando-se. As partes interessadas votam nas alterações ao protocolo, incluindo alterações ao próprio procedimento de votação, para chegar a um consenso social sobre as propostas. A Tezos suporta contratos inteligentes (smart contracts) e oferece uma plataforma para criar aplicativos descentralizados cuja logica de negócio é formalmente assegurada.

Esta proposta enquadra-se num projecto de colaboração da UBI com a Fundação Tezos onde é, entre outros, esperado uma colaboração próxima do mestrando com a Fundação.

2 Objectivo

Neste plano de trabalho, é objectivo explorar como as construções disponíveis na linguagem de programação própria aos smart contracts (**Michelson**) possam ser extendidas para melhorar a segurança e a confiança que se pode ter nos contratos de negócio definidos e da sua execução. Genéricamente fala-se em explorar e atuar na área da "*language based security*".

3 Plano

- Setembro a Novembro: Aprendizagem dos conceitos e das tecnologias envolvidos, estado da arte.
- Dezembro a Janeiro: Desenho dos mecanismos de verificação de segurança ao nível da linguagem.
- Fevereiro a Março: Implementação/Extensão da linguagem, do compilador e do sistema de tipos.
- Abril: Proof-of-concept, casos de estudos e testes para fins de validação empírica.
- Maio a Junho: Elaboração do Relatório de Tese, divulgação dos resultados.

4 Contactos

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