MEI/MiEI UC de Laboratório de Engenharia Informática

Verificação Formal de Smart-Contracts

Contexto:
A tecnologia *blockchain*, com origem nas estruturas criptográficas, tem evoluído rapidamente nos últimos anos e em particular na emergência dos designados *smart-contracts*, um modelo de computação descentralizado que tem vindo a ser aplicado num vasto conjunto de áreas aplicativas inovadoras. Mas trata-se de uma tecnologia muito recente, onde não é possível ainda estabelecer garantias rigorosas relativas à correcção e confiabilidade das aplicações desenvolvidas, e com a agravante que já foram documentados episódios onde "pequenas falhas" na codificação desses *smart-contracts* resultaram em falhas graves que conduziram a prejuízos avultados.

Objectivo:
Com este projeto pretende-se estudar/avaliar em que domínios as metodologias de verificação de programas e as ferramentas computacionais associadas.

Projeto:
Este projeto pretende estudar e avaliar em que domínios as metodologias de verificação formal de programas e as ferramentas computacionais associadas podem ser aplicadas ao desenvolvimento de smart-contracts. Em concreto, deve ser realizado um levantamento das propriedades cuja verificação formal é mais crítica, assim como a avaliação de sistemas de verificação recentemente propostos (e.g. https://forum.ethereum.org/discussion/3779/formal-verification-for-solidity-contracts).

Acompanhamento:
Este projeto será acompanhado por José Carlos Bacelar (jba@di.uminho.pt) e Jorge Sousa Pinto (jsp@di.uminho.pt). É ainda previsível uma interacção grande com outros projectos em curso no DI/HasLab na área da tecnologia Blockchain.