Um compilador para uma DSL especializada para algoritmos de consenso em Blockchains

Proposta de Projeto

Orientador: Simão Melo de Sousa

1 Objetivos

Esta proposta de projecto final de curso insere-se num projecto de investigação (COPES: COnsensus Protocols Environments and Specifications) envolvendo empresas e parceiros académicos internacionais e será realizado com a colaboração/*feedback* dos mesmos. O projecto de investigação incide sobre o desenho robusto de novos algoritmos de consenso para *blockchains*.

Os algoritmos de consenso são o mecanismo que permite, numa *blockchain*agrupando possivelmente um grande número de nodos em rede, que os nodos chegam a acordo, consenso, sobre o estado do *distributed ledger* (livro conta distribuído) onde possivelmente nodos operam de forma maliciosa e lesiva do interesse global. O mecanismo de consenso permite assegurar que cada bloco inserido na *blockchain*representa a verdade última e única sobre as transacções que estão nela contida. Assim, os algoritmos de consenso são responsáveis pela segurança e integridade do funcionamento de uma *blockchain*.

Definir e afinar um algoritmo de consenso pode dramaticamente melhorar o desempenho e a acuidade de uma *blockchain*. No entanto esta actividade é complexa e essencialmente realizada manualmente por um perito e os seus ajustes acertados participam da magia negra que só alguns dominam.

Objectivo do projecto final de curso: Incluído no projecto COPES que visa fornecer ferramentas e suporte computacional para (i) expressar e afinar algoritmos de consenso; (ii) experimentar e simular o comportamento e (iii) constatar impacto destes numa determinada *blockchain*, este projecto final de curso visa desenvolver um pequeno compilador, simples, de uma DSL (*Domain Specific Language*) para OCaml. Esta DSL, definida por especialistas do projecto COPES em algoritmos de consenso, permite a expressão facilitada destes algoritmos e posterior análise.

Ser capaz de gerar código de produção (aqui OCaml) directamente integrável em *blockchains*de referência é um factor determinante para a pertinência deste projecto.

2 Tarefas a Realizar

T1 Estudo dos conceitos envolvidos

T2 Estudo das tecnologias por utilizar

T3 Desenho e Implementação da solução

T4 Validação, teste e analises dos resultados

T5 Escrita do relatório de projeto

3 Cronograma

T1 1 mês

T2 1 mês

T3 2 mês

T4 0,5 mês

T5 0,5 mês

4 Requisitos Técnicos

Gosto em programar e em resolver com rigor problemas de natureza informática. Gosto em desenvolver capacidade em programação, algoritmos e estruturas de dados. Vontade em aprender novos conceitos e novas tecnologias.

5 Requisitos Académicos

UE. de Matemáticas, Programação, Algoritmos e Estruturas de Dados, Lógica Computacional, Teoria da Computação, Processamento de Linguagens.

6 Resultados esperados

- 1 protótipo.
- 1 relatório de projeto.

7 Contactos

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