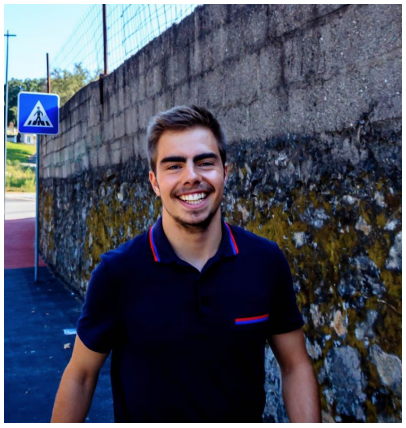
Escola de Engenharia
Universidade do Minho

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA
Mestrado em Engenharia Informática
Engenharia de Segurança

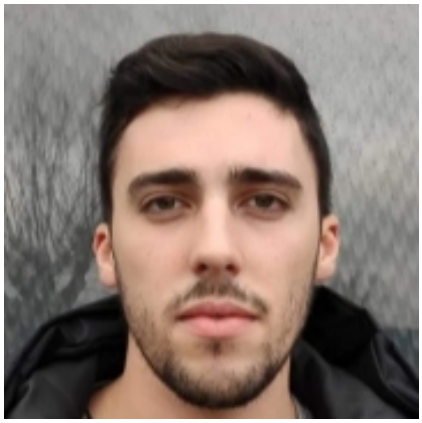
Aula 5

9 de Março de 2020

Grupo 1



Ricardo Pereira a73577



Tiago Ramires pg41101

Braga, 23 de Março de 2020

1. Blockchain

Pergunta P1.1

Tal como é pedido, no código do ficheiro main.experiencia1.1.js, foram introduzidas as informações em questão.

Pergunta P1.2

Posto isto, adicionamos mais 3 blocos à *blockchain* cujo "*amount*"foi 73577, 41101 e 0.001, por esta ordem. As alterações foram feitas no mesmo ficheiro (main.experiencia1.1.js).

2. Proof of Work Consensus Model

Pergunta P2.1

Como se pode ler nos artigos referidos anteriormente, a mineração é um estratagema que serve como "prova de trabalho", isto é, garante que cada bloco, antes de entrar na *blockchain* tenha sido submetido a um processo propositadamente moroso. O facto da criação de um bloco demorar tanto tempo, impossibilita que um agente malicioso altere o conteúdo de uma *blockchain*. Ora como as capacidades de computação aumentam a cada dia, a dificuldade do processo de mineração aumenta também de forma a combater essa capacidade.

Dificuldade	Tempo (segundos)
2	2,948
3	5,455
4	17,783
5	228.680

A alteração dessa dificuldade é aquilo que se tenta mostrar neste exercício e na tabela em baixo é possível observar que à medida que se aumenta a dificuldade aumenta-se também o tempo de mineração dos blocos.

Pergunta P2.2

1

No algoritmo em questão, "para se mostrar ao sistema"que o bloco demorou algum tempo para ser criado, o minerador tem que obter um código *hash* com um prefixo com um determinado número de zeros, o que implica que se esteja constantemente a recalcular esse código até obter esse prefixo. Para se obter sempre um código diferente altera-se o *nouce*, um campo que existe de propósito para o efeito.

2

Sim, visto que obriga a que os blocos passem por um processo moroso e também porque é possível adaptar a dificuldade de mineração de acordo com a crescente capacidade de computação.