Uma introdução matemática a blockchains

Augusto Teixeira

September 19, 2018

1 Detalhes do curso

- Nível: Introdutório
- Assistente: Felipe Argento

2 Descrição detalhada

Nesse curso iremos rever alguns conceitos básicos de criptografia e introduzirermos o algoritmo de blockchain baseado em Proof of Work.

Desde o surgimento do Bitcoin, um grande interesse econômico e acadêmico tem se voltado para o algoritmo de blockchain, que tornou essa moeda possível. Essa tecnologia permite que diversos agentes entrem em consenso, sem a necessidade de que exista um agente centralizador confiável e mesmo na presença de uma porcentagem grande de agentes maliciosos. Esse tópico, além de muito atual, se relaciona com diversas áreas da matemática tais como: a criptografia, teoria de jogos e passeios aleatórios. Portanto, nada mais natural do que preparar um curso de blockchain especialmente pensado para matemáticos.

O curso será voltado para alunos de graduação em matemática ou computação, assumindo apenas conhecimentos básicos sobre aritmética modular. Após uma introdução motivadora do problema central, a primeira parte do curso será focada em criptografia básica. Mais precisamente, apresentaremos o algoritmo de RSA e um algoritmo simples para a geração hashs criptográficos. Pretendemos apresentar esses conceitos com uma linguagem próxima à dos matemáticos, aumentando assim a acessibilidade para esses alunos.

Em um segundo momento, apresentaremos um design bastante simplificado de moeda descentralizada, com o objetivo de ilustrar o algoritmo de blockchain. Esse modelo será baseado em Proof of Work e mostraremos rigorosamente as garantias de segurança oferecidas pelo sistema. Finalmente daremos uma visão informal das várias direções de pesquisa que tem surgido nos últimos anos sobre o tema, tanto para melhorar a segurança e a eficiência do sistema, quanto para fazer uso dessa inovação em outras áreas.

As notas de aula seguirão a mesma linha do curso, apresentando os seguintes capítulos:

1. Introdução e motivação
2. Aritmética modular e criptografia
3. Blockchain em uma moeda descentralizada
4. Direções futuras

3 Bibliografia

Nesse curso utilizaremos os livros: [Gol06] e [Ant17].

4 Pre-requisitos

Serão assumidos poucos conhecimentos prévios para o curso. Espera-se que o(a) aluno(a) já tenha sido exposto à aritmética modular e possua maturidade matemática compatível com a de um curso de Análise Real ou Matemática Discreta.

References

[Ant17] Andreas M. Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly Media, Inc., 2nd edition, 2017.

[Gol06] Oded Goldreich. *Foundations of Cryptography: Volume 1*. Cambridge University Press, New York, NY, USA, 2006.