Blockchain e criptomoedas: conceitos básicos e avançados

Introdução

Web3 é o nome dado para uma nova iteração da World Wide Web (Internet) que incorpora conceitos como descentralização, transparência, e economia baseada em tokens e criptomoedas. Primitivas incluem blockchain; bitcoin, ethereum e outras criptomoedas. Junto com a Inteligẽncia Artificial, é a tendência mais importante atualmente em tecnoologia da informação. A ideia desta disciplina é estudar estas tecnologias detalhadamente, como também seus possíveis impactos no médio e longo prazo.

A criptografia é indispensável neste contexto. Trata-se de técnicas matemáticas proporcionando a comunicação e computação segura e confiável na presença de partes maliciosas. Uma parte significativa do curso será dedicada a estudar seus fundamentos matemáticos.

AVISO:
O foco da disciplina é tecnico, não é financeiro. Portanto nenhuma informação pode ser interpretada como uma recomendação de "investimento". Na verdade, comprar criptomoedas não é "investimento", mas é especulação: você arrisca perder todo seu dinheiro, como já aconteceu a milhares de pessoas. Nunca compre cripto-moedas com dinheiro destinado a outros fins.

Objetivos da disciplina

- entender o que é um blockchain;
- entender como um blockchain é aplicada em criptomoedas, como Bitcoin, Ethereum e outras;
- estudar mecanismos de consenso: Proof-of-Work, Proof-of-Stake, Practical Byzantine Fault Tolerance, outros;
- estudar smart contracts de Ethereum;
- estudar outras aplicações do block chain como Hyperledger, e seu eventuais implicações;
- estudar a privacidade neste contexto, provas ZK, SNARKs, STARKs etc;
- estudar as primitivas criptográficas subjacentes e os outros aspectos de segurança envolvidos.

Pré-requisitos:

Estas tecnologias combinam várias técnicas avançadas da CC e portanto exige mais maturidade do aluno. Disciplinas exigidas: Algebra A, linguagens de programação. Redes. Ainda, para realmente entender a criptografia, um bom domínio da matemática é indispensável. Não há literatura em português, então um bom domínio do inglês é indispensável.

Avaliação (a ser detalhada):
* duas provas: 25 + 25 = 50%
* exercícios: 20%
* projeto: 20%
* aula: 10%

Literatura (incompleto):

Referência principal:
Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained. (fourth edition) Imran Bashir, Packt Publishing, 2023 ISBN: 978-1803241067.

O seguintes livros discutem apenas bitcoin:

Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction
Arvind Narayanan , Joseph Bonneau , Edward Felten, Andrew Miller, Steven Goldfeder
Princeton University Press (July 19, 2016)
ISBN-10: 0691171696

Mastering Bitcoin
Andreas M. Antonopoulos
O'Reilly
ISBN-13: 9781449374044

Outras referências serão dadas durante a disciplina.