



MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

PROGRAMA DE ENSINO

1. Identificação

Disciplina: INE5458 - Tecnologias Blockchain e Criptomoedas
Nível: Graduação
Carga Horária: 72 horas-aula (Teórica: 52; Prática: 20)
Vigência: De 2020-2 até a presente data

2. Ementa

-Primitivas Criptográficas. Conceitos e protocolos de blockchain. Criptomoedas e aplicativos não financeiros em execução em blockchains. Desenvolvimento de contratos inteligentes.

3. Cursos Relacionados

- CIÊNCIAS DA COMPUTAÇÃO (208) - Currículo: 2007-1 (Optativa)
 - ENGENHARIA MECATRÔNICA [Campus Joinville] (605) - Currículo: 2016-1 (Optativa)
 - SISTEMAS DE INFORMAÇÃO (noturno) (238) - Currículo: 2011-1 (Optativa)
-

4. Objetivos

4.1 Objetivo Geral:

Compreender os conceitos do ecossistema de tecnologias de criptografia. Distinguir entre aplicações financeiras e não financeiras em blockchains e ledgers distribuídos. Aprender a desenvolver aplicativos descentralizados usando blockchains e ledgers distribuídos.

4.2 Objetivos Específicos:

- a) Compreender as primitivas de segurança como uma forma de fornecer segurança
- b) Entender os blocos básicos de criptomoedas
- c) Entender o conceito de livros distribuídos
- d) Entender como blockchains fornecem armazenamento distribuído e alcançam consenso
- e) Descrever como as transações podem ser usadas para transferir ativos em blockchains
- f) Usar criptografia como meio para identificar usuários em transações
- g) Compreender como as criptomoedas e aplicativos não financeiros funcionam em blockchains
- h) Criar e implantar contratos inteligentes para funcionar como aplicativos autônomos e livres de conflitos

5. Conteúdo Programático

- 1 Primitivas Criptográficas. [4 horas-aula]
 - 1.1 Funções Hash
 - 1.2 Criptografia assimétrica
- 2 Conceitos de criptomoedas [8 horas-aula]
 - 2.1 Ativos
 - 2.2 Carteiras
 - 2.3 Transações em blockchain baseadas em hashing
 - 2.4 Mineração e prova de trabalho
 - 2.5 Nodes e consenso distribuído
- 3 Propriedades do Blockchain [8 horas-aula]
 - 3.1 Anonimato
 - 3.2 Consenso
 - 3.3 Integridade pós-quântica
 - 3.4 Resiliência
- 4 Aplicações de Blockchain[8 horas-aula]
 - 4.1 Criptomoedas: Bitcoin e altcoins
 - 4.2 Aplicações não financeiras: serviços notariais, registro de nomes e troca de mensagens
- 5 Desenvolvimento de contratos inteligentes na Ethereum [12 horas-aula]
 - 5.1 Casos de uso: votação, manutenção de registros, identidades digitais
 - 5.2 Ethereum Virtual Machine
 - 5.3 Linguagem de programação solidity
 - 5.4 Estrutura de um contrato: variáveis, funções
 - 5.5 Tipos de dados
 - 5.6 Unidades de Ether e tempo
 - 5.7 Propriedades de bloqueio e transação
 - 5.8 Criando contratos: Remix, teste e rede principal
 - 5.9 Ethereum API: web3.js
- 6 Hyperledger[12 horas-aula]
 - 6.1 Hyperledger Fabric
 - 6.2 Chaincode e DAAs
 - 6.3 Hyperledger Indy
- 7 Desenvolvimento de Projetos [20 horas-aula]
 - 7.1 Infraestrutura para realização de experimentos
 - 7.2 Desenvolvimento experimental
 - 7.3 Experiências de reportagem

6. Bibliografia Básica

- [1] The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, William Mougayar, 2016, 209pp
- [2] Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Don Tapscott, 2016, 268pp
- [3] Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, 2016, 328pp

7. Bibliografia Complementar

- [1] Bitcoin and Cryptocurrency Technologies. Nayaran, Arvind et al. Online: <http://bitcoinbook.cs.princeton.edu>
- [2] Solidity. Online: <https://solidity.readthedocs.io/en/latest/index.html>
- [3] Hyperledger Fabric. <https://hyperledger-fabric.readthedocs.io/>
- [4] Hyperledger Indy. <https://hyperledger-indy.readthedocs.io/en/latest/>