



UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS, TECNOLOGIAS E SAÚDE - CTS
DEPARTAMENTO DE COMPUTAÇÃO – DEC

PLANO DE ENSINO

SEMESTRE 2021.1

I. IDENTIFICAÇÃO DA DISCIPLINA:

CÓDIGO	NOME DA DISCIPLINA	Nº DE HORAS-AULA SEMANAIS		TOTAL DE HORAS-AULA SEMESTRAIS
		TEÓRICAS	PRÁTICAS	
DEC7551	Tópicos Especiais I: Tecnologias de Contabilidade Distribuída	2	2	72

HORÁRIO

MODALIDADE

TURMAS TEÓRICAS	TURMAS PRÁTICAS	Remota
06655 – 3.1830-2	06655 – 5.1830-2	

II. PROFESSOR(ES) MINISTRANTE(S)

Prof. Martín Vigil

Email: martin.vigil@ufsc.br

Horário de Atendimento: Segundas e Quartas das 13h00 às 14h00 em sala virtual a combinar

III. PRÉ-REQUISITO(S) SUGERIDOS

Domínio da Língua Inglesa e as seguintes disciplinas

CÓDIGO	NOME DA DISCIPLINA
DEC7532	Linguagens de Programação II
DEC0006	Estruturas de Dados

IV. CURSO(S) PARA O(S) QUAL(IS) A DISCIPLINA É OFERECIDA

Bacharelado em Engenharia de Computação

V. JUSTIFICATIVA

Tecnologias de contabilidade distribuída (conhecidas por blockchain) são tendências atuais no desenvolvimento de sistemas computacionais. Portanto, conhecer essas tecnologias é importante para a atualização dos Engenheiros da Computação.

VI. EMENTA

Primitivas criptográficas. Conceitos e protocolos de blockchain. Aplicações financeiras e não financeiras em plataformas blockchain. Contratos inteligentes.

VII. OBJETIVOS

Objetivos Gerais: O aluno deverá ser capaz de aplicar tecnologias blockchain na solução de problemas computacionais onde consenso e imutabilidade de dados são necessários.

Objetivos Específicos:

- Compreender primitivas de criptográficas como método de prover segurança computacional
- Entender como blockchains alcançam consenso e armazenam dados distribuídamente
- Descrever como transações são usadas para transferir ativos através de blockchains
- Aplicar meios criptográficos para identificar usuários que participam de transações

- Compreender como aplicações financeiras e não financeiras funcionam sobre blockchains
- Criar e instanciar contratos inteligentes para conceber aplicações autônomas e livres de conflito

VIII. CONTEÚDO PROGRAMÁTICO

- Unidade 1: Primitivas Criptográficas
 - o Funções Hash
 - o Criptografia assimétrica
- Unidade 2: Conceitos de criptomoedas
 - o Ativos
 - o Carteiras
 - o Transações
 - o Algoritmo de consenso baseado em prova de trabalho
- Unidade 3: Propriedades do Blockchain
 - o Anonimato
 - o Comunidade, governos e regulamentação
- Unidade 4: Aplicações de Blockchain
 - o Criptomoedas: Bitcoin e altcoins
 - o Aplicações não financeiras: serviços notariais, registro de nomes e troca de mensagens
- Unidade 5: Desenvolvimento de contratos inteligentes na Ethereum
 - o Casos de uso: votação, manutenção de registros, identidades digitais
 - o Ethereum Virtual Machine
 - o Linguagem de programação solidity
 - o Estrutura de um contrato: variáveis, funções
 - o Tipos de dados
 - o Unidades de Ether e tempo
 - o Propriedades de bloqueio e transação
 - o Criando contratos: Remix, teste e rede principal
 - o Ethereum API: web3.js
- Unidade 6: Desenvolvimento de Projetos
 - o Infraestrutura para realização de experimentos
 - o Desenvolvimento experimental
 - o Experiências de reportagem

IX. METODOLOGIA DE ENSINO / DESENVOLVIMENTO DO PROGRAMA

A disciplina será dividida em duas partes. A primeira parte consistirá em aulas expositivas sobre os conceitos de tecnologias de contabilidade distribuída. Adicionalmente, pelo menos um tópico do programa será abordado por meio de seminários apresentados por grupos de alunos. Para consolidar o aprendizado, atividades práticas serão realizadas.

A segunda parte da disciplina consistirá em desenvolver um projeto em grupos de alunos. As possibilidades de projeto são as seguintes.

1. Projetar produto para o mercado utilizando tecnologias de contabilidade distribuída.
2. Projetar aplicação na forma de contribuição científica utilizando tecnologias de contabilidade distribuída.
3. Conduzir um estudo teórico aprofundando os conceitos vistos na primeira etapa da disciplina.

O entregável da segunda etapa será um vídeo do *pitch* do produto ou artigo científico sobre a aplicação ou estudo teórico.

X. METODOLOGIA E INSTRUMENTOS DE AVALIAÇÃO

A verificação do rendimento escolar compreenderá frequência e aproveitamento nos estudos, os quais deverão ser atingidos conjuntamente. Será obrigatória a frequência às atividades correspondentes a cada disciplina, no mínimo a 75% das mesmas (Frequência Suficiente - FS), ficando nela reprovado o aluno que não comparecer a mais de 25% das atividades (Frequência Insuficiente - FI).

A nota mínima para aprovação na disciplina será $MF \geq 6,0$ (seis) e Frequência Suficiente (FS). (Art. 69 e 72 da Res. nº 17/CUn/1997).

O aluno com Frequência Suficiente (FS) e média das notas de avaliações do semestre MF entre 3,0 e 5,5 terá direito a uma nova avaliação no final do semestre (REC), exceto as atividades constantes no art.70, § 2º. A Nota Final (NF) será calculada por meio da média aritmética entre a média das notas das avaliações parciais (MF) e a nota obtida na nova avaliação (REC). (Art. 70 e 71 da Res. nº 17/CUn/1997).

Ao aluno que não efetuar as avaliações ou não apresentar trabalhos no prazo estabelecido será atribuída nota 0 (zero). (Art. 70, § 4º da Res. nº 17/CUn/1997)

Avaliações:

- Média das Avaliações Assíncronas (A) com prazo de pelo menos 48 horas para conclusão
- Seminário Assíncrono (S) através da criação de vídeos no Youtube
- Avaliações do desenvolvimento do projeto (P)

A Média Final (MF) será calculada da seguinte forma:

$$MF = A \cdot 0.2 + S \cdot 0.3 + P \cdot 0.5$$

• A prova REC é uma atividade assíncrona que se inicia no horário regular da disciplina com prazo máximo para a conclusão de 24 horas

• O registro de frequência será efetuado para aulas assíncronas e síncronas. No primeiro caso serão disponibilizadas atividades com tempo de execução de 48 horas em que, a partir da execução destas, os alunos terão a presença registrada. Para o segundo caso ao final das aulas será realizado o registro. Na eventual impossibilidade do aluno estar presente será aplicada a regra da aula assíncrona.

Observações:

Avaliação de recuperação:

• Não há avaliação de recuperação nas disciplinas de caráter prático que envolve atividades de laboratório (Res.17/CUn/97).

Nova avaliação:

O aluno, que por motivo de força maior e plenamente justificado, deixar de realizar atividades avaliativas previstas no plano de ensino, deverá formalizar pedido à Chefia do Departamento de Ensino ao qual a disciplina pertence, dentro do prazo de 3 (três) dias úteis, apresentando documentação comprobatória. O pedido de nova avaliação deverá ser formalizado na Secretaria Integrada de Departamentos.

XI. CRONOGRAMA TEÓRICO/PRÁTICO

AULA (semana)	DATA	ASSUNTO
1	14/06/2021 a 19/06/2021	Unidade 1 (aula assíncrona)
2	21/06/2021 a 26/06/2021	Unidade 1 (aula síncrona e assíncrona)
3	28/06/2021 a 03/07/2021	Unidade 2 (aula assíncrona)
4	05/07/2021 a 10/07/2021	Unidade 2 (aula síncrona e assíncrona)
5	12/07/2021 a 17/07/2021	Unidade 3 (aula assíncrona)
6	19/07/2021 a 24/07/2021	Unidade 3 (aula síncrona e assíncrona)
7	26/07/2021 a 31/07/2021	Unidade 4 (aula assíncrona)
8	02/08/2021 a 07/08/2021	Unidade 4 (aula síncrona e assíncrona)
9	09/08/2021 a 14/08/2021	Unidade 5 (aula assíncrona)

10	16/08/2021 a 21/08/2021	Unidade 5 (aula síncrona e assíncrona)
11	23/08/2021 a 28/08/2021	Unidade 6 (aula assíncrona)
12	30/08/2021 a 04/09/2021	Unidade 6 (aula síncrona e assíncrona)
13	06/09/2021 a 11/09/2021	Desenvolvimento do projeto (atividade assíncrona)
14	13/09/2021 a 18/09/2021	Desenvolvimento do projeto (atividade síncrona e assíncrona)
15	20/09/2021 a 25/09/2021	Entrega do relatório do projeto
16	27/09/2021 a 02/10/2021	Prova de recuperação e divulgação das notas (atividades assíncronas)

Obs: O calendário está sujeito a pequenos ajustes de acordo com as necessidades das atividades desenvolvidas.

XII. Feriados previstos para o semestre 2021.1:

DATA	
04/09/2021	Data reservada ao Vestibular 2021.2
05/09/2021	Data reservada ao Vestibular 2021.2
06/09/2021	Data reservada ao Vestibular 2021.2
07/09/2021	Independência do Brasil

XIII. BIBLIOGRAFIA BÁSICA

NAYARAN et al. **Bitcoin and Cryptocurrency Technologies**. Online: <http://bitcoinbook.cs.princeton.edu>

Solidity. Online: <https://solidity.readthedocs.io/en/latest/index.html>

ROSULEK, Mike. **The Joy of Cryptography**. Online: <https://web.engr.oregonstate.edu/~rosulekm/crypto/>

XIV. BIBLIOGRAFIA COMPLEMENTAR

STINSON, Douglas R. **Cryptography: theory and practice**. 3rd. ed. Boca Raton: Chapman & Hall, c2006. 593 p.

TANENBAUM, Andrew S.; WETHERALL, D. **Redes de computadores**. 5. ed. São Paulo: Pearson, 2011. xvi, 582 p.

	Professor da Disciplina
Aprovado na Reunião do Colegiado do Curso em: ___/___/_____	

	Coordenador do Curso