UNIVERSIDADE FEDERAL DE SANTA CATARINA
Centro de Ciências, Tecnologias e Saúde
Departamento de Computação
PLANO DE ENSINO

SEMESTRE 2019.1

I. IDENTIFICAÇÃO DA DISCIPLINA:

CÓDIGO	NOME DA DISCIPLINA	Nº DE HORAS-AULA SEMANAIS		TOTAL DE HORAS-AULA SEMESTRAIS
		TEÓRICAS	PRÁTICAS	
DEC7552	Tópicos Especiais II: Tecnologias de Blockchain e Criptomoedas	2	2	72

HORÁRIO

TURMAS TEÓRICAS	TURMAS PRÁTICAS	MODALIDADE
07655 – 2-1010-2	07655 – 4-1010-2	**Presencial**

II. PROFESSOR(ES) MINISTRANTE(S)

Profª Martín Vigil
E-mail: martin.vigil@ufsc.br

III. PRÉ-REQUISITO(S) SUGERIDOS

Domínio da Língua Inglesa e as seguintes disciplinas

CÓDIGO	NOME DA DISCIPLINA
DEC7532	Linguagens de Programação II
DEC7521	Estruturas de Dados I

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

Graduação em Engenharia de Computação

V. JUSTIFICATIVA

Tecnologias de blockchain e criptomoedas 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 distribuidamente
- 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

- Primitivas Criptográficas. [8 horas-aula]
  - Funções Hash
  - Criptografia assimétrica
- Conceitos de criptomoedas [14 horas-aula]
  - Ativos
  - Carteiras
  - Transações em blockchain baseadas em hash
  - Mineração e prova de trabalho
  - Nodos e consenso distribuído
- Propriedades do Blockchain [12 horas-aula]
  - Anonimato
  - Comunidade, governos e regulamentação
  - Integridade pós-quântica
- Aplicações de Blockchain [12 horas-aula]
  - Criptomoedas: Bitcoin e altcoins
  - Aplicações não financeiras: serviços notariais, registro de nomes e troca de mensagens
- Desenvolvimento de contratos inteligentes na Ethereum [16 horas-aula]
  - Casos de uso: votação, manutenção de registros, identidades digitais
  - Ethereum Virtual Machine
  - Linguagem de programação solidity
  - Estrutura de um contrato: variáveis, funções
  - Tipos de dados
  - Unidades de Ether e tempo
  - Propriedades de bloqueio e transação
  - Criando contratos: Remix, teste e rede principal
  - Ethereum API: web3.js
- Desenvolvimento de Projetos [10 horas-aula]
  - Infraestrutura para realização de experimentos
  - Desenvolvimento experimental
  - 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 blockchains e criptomoedas. Adicionalmente, pelo menos um tópico do programa será abordado por meio de seminários. Para consolidar o aprendizado, atividades práticas via Moodle serão realizadas. Esta etapa será avaliada com os seminários e uma prova.

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

- Projetar um sistema inovador usando tecnologias vistas na primeira parte da disciplina.
- Estender ou adaptar um sistema existente alcançando diferentes objetivos para uma aplicação específica.

- Conduzir um estudo teórico aprofundando os conceitos vistos na primeira etapa da disciplina.

Esta etapa será avaliada através de um relatório no formato de artigo científico.

Horário das aulas, pontualidade e cobrança de presença

As aulas começarão pontualmente às 10h10. Após isso, ficará proibida a entrada de alunos. Eventuais entradas com atraso poderão ser permitidas se o professor entender que o andamento da aula não será prejudicado.

As presenças da primeira e segunda aulas serão cobradas somente no início da primeira aula e serão modificadas caso o aluno deixe a sala antes do término das aulas.

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).
- Serão realizadas três avaliações, sendo:
  - **P**: Prova
  - **S**: Seminários
  - **R**: Relatório
- A Média Final (MF) será calculada da seguinte forma:

$$MF = 0.2P + 0.2S + 0.6R$$

- A nota mínima para aprovação na disciplina será MF>=6,0 (seis) e Frequência Suficiente (FS). (Art. 69 e 72 da Res. nº 17/CUn/1997).
- Ao aluno que não comparecer às avaliações ou não apresentar trabalhos no prazo estabelecido será atribuída nota 0 (zero). (Art. 70, § 4º da Res. nº 17/CUn/1997)

Observações:

Avaliação de recuperação

- Não é prevista atividade de recuperação para esta turma, nos termos previstos no art. 70, parágrafo 2o, da Resolução 17/CUn/97, uma vez que cumpre pelo menos um dos seguintes requisitos:
  - ter pelo menos 50% de carga prática;
  - ter pelo menos 50% do peso da média final originado de trabalho prático;
  - ter a inadequação da aplicação de avaliação de recuperação reconhecida pelo colegiado do curso, a partir da avaliação de solicitação fundamentada de dispensa de avaliação de recuperação, encaminhada pelo(s) professor(es) autor(es) do respectivo plano de ensino, para disciplinas com carga prática prevista no programa da disciplina, com nota de trabalho prático considerada no cálculo da média final e que não tenham cumprido um dos requisitos anteriores.

Nova oportunidade de realizar atividade avaliativa

- *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.* (Ver formulário)

XI. CRONOGRAMA PRÁTICO

AULA (semana)	DATA		ASSUNTO
1	11/03/2019	13/03/2019	Resumo criptográfico

2	18/03/2019	20/03/2019	Criptografia assimétrica
3	25/03/2019	27/03/2019	Conceitos de criptomoedas: ativos, carteiras, transações
4	01/04/2019	03/04/2019	Conceitos de criptomoedas: blocos e listas ligadas baseadas em resumo criptográfico, mineração e prova de trabalho
5	08/04/2019	10/04/2019	Conceitos de criptomoedas: nodos e consenso distribuído
6	15/04/2019	17/04/2019	Seminários: algoritmos alternativos de consenso
7	22/04/2019	24/04/2019	Propriedades de blockchain: anonimato, comunidade,
8	29/04/2019	01/05/2019	Propriedades de blockchain: integridade pós-quântica
9	06/05/2019	08/05/2019	**Applicações de blockchain: Bitcoin e altcoins**
10	13/05/2019	15/05/2019	**Applicações de blockchain**: serviços notariais, registro de nomes, troca de mensagens
11	20/05/2019	22/05/2019	Contratos Inteligentes Ethereum: casos de uso: votação, guarda de registros, identidades digitais
12	27/05/2019	29/05/2019	Contratos Inteligentes Ethereum: Solidity
13	03/06/2019	05/06/2019	Contratos Inteligentes Ethereum: Remix, redes de teste e principal, web3js. Prova
14	10/06/2019	12/06/2019	Desenvolvimento de projeto
15	17/06/2019	19/06/2019	Desenvolvimento de projeto
16	24/06/2019	26/06/2019	Desenvolvimento de projeto
17	01/07/2019	03/07/2019	Desenvolvimento de projeto. **Entrega do relatório**
18	08/07/2019	10/07/2019	Divulgação de notas

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

XII. FERIADOS PREVISTOS PARA O SEMESTRE 2019.1:

DATA	
03/04/2019	Aniversário de Araranguá
01/05/2019	Dia do Trabalhor

XIII. BIBLIOGRAFIA BÁSICA

1. NAYARAN et al. Bitcoin and Cryptocurrency Technologies. Online: http://bitcoinbook.cs.princeton.edu
2. Solidity. Online: https://solidity.readthedocs.io/en/latest/index.html
3. STALLINGS, William. Criptografia e segurança de redes: princípios e práticas. 4. ed. São Paulo: Prentice-Hall, c2008. xvii, 492 p.
4. CARVALHO, Daniel Balparda de. Criptografia: métodos e algoritmos. 2. ed. Rio de Janeiro: Book Express, 2001. xvi, 215 p.

XIV. BIBLIOGRAFIA COMPLEMENTAR:

1. STINSON, Douglas R. Cryptography: theory and practice. 3rd. ed. Boca Raton: Chapman & Hall, c2006. 593 p.
2. TANENBAUM, Andrew S.; WETHERALL, D. Redes de computadores. 5. ed. São Paulo: Pearson, 2011. xvi, 582 p.

Os livros acima citados constam na Biblioteca Universitária e Setorial de Araranguá. Algumas bibliografias também podem ser encontradas no acervo da disciplina, via sistema Moodle.

XV. INFRAESTRUTURA E MATERIAS NECESSÁRIOS:

1. Laboratório de informática com, no mínimo, um computador por aluno
2. Espaço físico com mesas, cadeiras e tomadas em quantidades adequadas
3. Acesso à internet
4. Projetor (datashow)
5. 20 folhas de papel A4 por aluno
6. 10 folhas prova por aluno
7. Quadro branco e canetas
8. Impressão: monocromática e colorida

Obs.: A indisponibilidade de infraestrutura/materiais listados pode causar prejuízos ao processo pedagógico, inviabilizando tanto as atividades dos docentes como as dos alunos, podendo, ainda, acarretar em cancelamento de aulas em último caso.

Martin Augusto Gagliotti Vigil:04300078920

Digitally signed by Martin Augusto Gagliotti Vigil:04300078920 Date: 2019.03.07 08:21:23 -03'00'

Professor da Disciplina

/ / 2019

Aprovado na Reunião do colegiado do Curso

27 / 03 / 2019

Prof. Fabrício de Oliveira Ourique, Ph.D. Coordenador do Curso de Eng. de Computação - UFSC Portaria 2703/2018/GR

Coordenador do Curso

/ / 2019