UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Vinicius Macelai

ELEIÇÃO ELETRÔNICA UTILIZANDO CERTIFICADO DIGITAL AUDITADA EM BLOCKCHAIN

Florianópolis

2018

Vinicius Macelai

ELEIÇÃO ELETRÔNICA UTILIZANDO CERTIFICADO DIGITAL AUDITADA EM BLOCKCHAIN

Monografia submetida ao Programa de Graduação em Ciência da Computação para a obtenção do Grau de Bacharel em Ciência da Computação.
Orientador: Prof. Dr. Jean Everson Martina

Florianópolis

2018

FOLHA DE APROVAÇÃO DE PROPOSTA DE TCC

Acadêmico(s)	Vinicius Macelai
Título do trabalho	Eleição eletrônica utilizando certificado digital auditada em blockchain
Curso	Ciência da Computação/INE/UFSC
Área de Concentração	Aplicações em Computação

Instruções para preenchimento pelo ORIENTADOR DO TRABALHO:

- Para cada critério avaliado, assinale um X na coluna SIM apenas se considerado aprovado. Caso contrário, indique as alterações necessárias na coluna Observação.

Critérios	Aprovado				Observação
	Sim	Parcial	Não	Não se aplica	
1. O trabalho é adequado para um TCC no CCO/SIN (relevância / abrangência)?					
2. O título do trabalho é adequado?					
3. O tema de pesquisa está claramente descrito?					
4. O problema/hipóteses de pesquisa do trabalho está claramente identificado?					
5. A relevância da pesquisa é justificada?					
6. Os objetivos descrevem completa e claramente o que se pretende alcançar neste trabalho?					
7. É definido o método a ser adotado no trabalho? O método condiz com os objetivos e é adequado para um TCC?					
8. Foi definido um cronograma coerente com o método definido (indicando todas as atividades) e com as datas das entregas (p.ex. Projeto I, II, Defesa)?					
9. Foram identificados custos relativos à execução deste trabalho (se houver)? Haverá financiamento para estes custos?					
10. Foram identificados todos os envolvidos neste trabalho?					
11. As formas de comunicação foram definidas (ex.: horários para orientação)?					
12. Riscos potenciais que podem causar desvios do plano foram identificados?					
13. Caso o TCC envolva a produção de um software ou outro tipo de produto e seja desenvolvido também como uma atividade realizada numa empresa ou laboratório, consta da proposta uma declaração (Anexo 3) de ciência e concordância com a entrega do código fonte e/ou documentação produzidos?					

Avaliação	☐ **Aprovado**		☐ **Não Aprovado**
Professor Responsável	Jean Everson Martina	12/11/2018	

RESUMO

Palavras-chave: criptografia, eleição, blockchain

SUMÁRIO

1 INTRODUÇÃO

1.1 OBJETIVOS

Objetivo geral. Apresentar um estudo detalhado sobre esquemas

Objetivos específicos. Descrever os esquemas de assinatur

Escopo do trabalho. Não se aplica ao conteúdo deste trabalho

Critérios de aceitação. Estudo e implementação de pelo menos

Entregas do projeto. Relatórios referentes às disciplinas

Restrições e premissas. Espera-se reunir com os orientadores,

1.2 PROCEDIMENTOS METODOLÓGICOS

O trabalho será desenvolvido utilizando a infraestrutura e recursos do Laboratório de Segurança em Computação (LabSEC/UFSC), onde será estudada bibliografia referente aos temas abordados nesta pesquisa buscando encontrar as vantagens e desvantagens entre cada um dos esquemas de assinatura digital escolhidos, bem como observar seu desempenho e tamanho de elementos como par de chaves e assinatura, ao utilizar funções de resumo criptográficas distintas em implementações produzidas ou fornecidas.

2 CRONOGRAMA

Etapas	Meses – 2018					
	jan.	**fev.**	**mar.**	**abr.**	**mai.**	**jun.**
Fundamentação teórica						
Revisão do estado da arte						
Desenvolvimento do TCC						
Implementação						
Relatório de TCC I						

Etapas	Meses – 2018					
	jul.	**ago.**	**set.**	**out.**	**nov.**	**dez.**
Ajustes na implementação						
Redação da monografia						
Ajustes na monografia						
Relatório de TCC II						
Defesa pública						
Ajustes finais do TCC						

3 CUSTOS

Item	Quantidade	Valor unitário (R$)	Valor Total (R$)
Material permanente			
Computador	1	R$ 3.000,00	R$ 3.000,00
Internet	1	R$ 1.000,00	R$ 1.000,00
Artigos	10	R$ 90,00	R$ 900,00
Livros	2	R$ 200,00	R$ 400,00
Material de consumo			
Alimentação	264	R$ 10,00	R$ 2.640,00
CDs/DVDs	4	R$ 2,00	R$ 8,00
Outros recursos e serviços			
Impressões	200	R$ 1,00	R$ 200,00

4 RECURSOS HUMANOS

Nome	Função
Vinicius Macelai	Autor
Jean E. Martina	Orientador
Renato Cislaghi	Coordenador de projetos
A definir	Membro(s) da banca

5 COMUNICAÇÃO

O que precisa ser comunicado	Por quem	Para quem	Melhor forma de comunicação	Quando e com que frequência
Enviar plano de projeto	Autor	Orientador, coorientador, coordenador de projetos	Sistema de TCC	Única vez, até dia 12/11/2018
Entrega de relatório de TCC I	Autor	Orientador, coorientador, coordenador de projetos, membro(s) da banca	Sistema de TCC	Única vez, ao final do semestre 2017/2
Entrega de relatório de TCC II	Autor	Orientador, coorientador, coordenador de projetos, membros(s) da banca	Sistema de TCC	Única vez, em meados do semestre 2018/1
Defesa do TCC	Autor	Orientador, coorientador, coordenador de projetos, membro(s) da banca	Pessoalmente	Única vez, em meados do semestre 2018/1
Entrega final da monografia	Autor	Orientador, coorientador, coordenador de projetos, membro(s) da banca	Sistema de TCC	Única vez, após a defesa, antes do término de 2018/1
Reuniões de acompanhamento da pesquisa	Autor	Orientador, coorientador	Pessoalmente, webconferência	Quinzenalmente
Monitoramento do projeto	Autor	Orientador, coorientador	E-mail	Esporadicamente
Convite de membro(s) da banca	Autor	A definir	Sistema de TCC	Única vez, em meados do semestre 2017/2

6 RISCOS

Risco	Proba-bilidade	Impacto	Priori-dade	Estratégia de resposta	Ações de prevenção
Paralisação de transporte público	Média	Médio	Baixa	Transportar-se à Universidade utilizando meios alternativos	Combinar transporte alternativo
Paralisação de servidores públicos	Muito baixa	Alto	Média	Produzir monografia e pesquisa utilizando recursos pessoais	Não se aplica
Problemas de saúde	Baixa	Alto	Alta	Tratamento médico das condições identificadas	Diminuição do fator de exposição em caso de doenças com fator ambiental, e exames para verificar condições genéticas
Perda de dados	Muito baixa	Alto	Média	Recuperar cópia de segurança	Cópias de segurança periódicas do material produzido
Queima de equipa-mento(s) eletrô-nico(s)	Muito baixa	Alto	Média	Comprar novo(s) equipamento(s)	Evitar utilização do(s) equipamento(s) em más condições de tempo ou por períodos muito prolongados