UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Vinicius Macelai

ELEIÇÃO ELETRÔNICA AUTENTICADA COM CERTIFICADO DIGITAL AUDITADA EM BLOCKCHAIN

Florianópolis

2018

Vinicius Macelai

ELEIÇÃO ELETRÔNICA AUTENTICADA COM CERTIFICADO DIGITAL AUDITADA EM BLOCKCHAIN

Proposta de Trabalho de Conclusão de Curso 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 autenticada com certificado digital auditada em blockchain
Curso	Ciência da Computação/INE/UFSC
Área de Concentração	Segurança

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

As abordagens utilizadas nos sistemas de eleição da maioria dos países continuam a ser realizadas de forma manual, com cédulas na forma de papel. Tal modelo traz problemas enormes de logística e um alto custo para funcionamento devido aos requisitos de uma eleição segura, que deve fornecer privacidade, transparência, verificabilidade e confiabilidade. Já as abordagens eletrônicas via internet, permanacem com desconfiança sobre manter estas propiedades. Uma possível solução para melhorar uma abordagem eletrônica seria utilizar uma blockchain para melhorar sua auditabilidade, que é o ponto mais questionado nesse esquema. A blockchain possui propiedades intrínsecas, como a imutabilidade dos dados, e com esquemas utilizando contratos inteligentes na blockchain é possível realizar a verificação dos votos de forma descentralizada e aberta ao público. Assim, cria-se um sistema que mantém as propiedades citadas anteriormente, com um baixo custo e menor necessidade de confiar em uma entidade central.

Palavras-chave: criptografia, eleições, democracia, blockchain, privacidade

SUMÁRIO

1	**INTRODUÇÃO**	7
1.1	OBJETIVOS	7
1.2	PROCEDIMENTOS METODOLÓGICOS	8
2	**CRONOGRAMA**	9
3	**CUSTOS**	11
4	**RECURSOS HUMANOS**	13
5	**COMUNICAÇÃO**	15
6	**RISCOS**	17
	REFERÊNCIAS	19

1 INTRODUÇÃO

Eleições eletrônicas têm sido usadas no Brasil por mais de 20 anos e testes recentes mostram que, mesmo com o desenvolvimento durante todo esse período, o atual sistema não consegue se mostrar realmente seguro (ARANHA, 2018). O maior problema com a solução proposta pelo Governo Brasileiro é a falta de auditabilidade, em que só é possível se voluntariar para testar o sistema em um ambiente controlado. Ainda durante o processo eleitoral, é necessário confiar cegamente no sistema, não há instrumento nenhum que permita verificar se o voto foi realmente computado.

Uma maneira de se realizar a autencicação no sistema seria utilizando certificados digitais, que são arquivos digitais, que permitem que uma pessoa seja identificada virtualmente, com garantia de autenticidade (ADAMS, 2002). Sendo no Brasil, o modelo adotado para gerenciar o sistema, é a Infraestrutura de Chaves Públicas Brasileira. Já na área da educação, há a Infraestrutura de Chaves Públicas para Ensino e Pesquisa.

Para realizar a auditabilidade das votações, é possível utilizar da tecnologia blockchain, que são bases de registro de dados distrubuídos e compartilhados, desta forma criando um consenso e confiança. (NAKAMOTO, 2009) Com essas propriedades intrínsecas, como a imutabilidade dos dados, é um bom sistema para manter o registro dos votos.

Este trabalho visa implementar uma solução que integre todas estas partes, um sistema de eleição eletrônico autenticado com certificado digital que permite ter informações sobre o votante de forma confiável. Além disso, realizar a verificação da eleição em uma blockchain de forma descentralizada e pública.

1.1 OBJETIVOS

Objetivo geral: Estudar e criar uma implementação de um sistema online de eleição, com seu foco principal na parte de realizar auditoria e verificação dos votos em uma blockchain, sendo possível utilizar de um sistema já desenvolvido que suporte autenticação com certificado digital. Além disso, analisar as implicações que esse sistema teria no funcionamento e custos de uma eleição.

Objetivos específicos:

- Analisar o estado da arte: estudar as principais soluções já propostas na literatura, com o objetivo de identificar problemas e oportunidades para melhorar o trabalho.

- Implementar autenticação com certificado digital: Utilizar de um sistema já existente de votação e implementar a possiblidade de autenticar via certificado.
- Implementar possibilidade de verificação na blockchain: Implementar um sistema para tornar o sistema mais auditável e verificável para o público em geral.
- Comparar e analisar as consequências do esquema.

Escopo do trabalho: Não se aplica ao conteúdo deste trabalho a análise profunda das provas de segurança do sistema utilizado como base.

Critérios de aceitação: Estudo e implementação do sistema proposto. Juntamente com a análise das consequências do esquema.

Entregas do projeto: Relatórios referentes às disciplinas de Trabalho de Conclusão de Curso do INE/UFSC, incluindo monografia completa ao final da disciplina. Assim como implementação documentada do sistema.

Restrições e premissas: Espera-se reunir com os orientadores, de forma periódica, para a discussão dos resultados obtidos e a definição dos passos seguintes. As restrições consistem na finalização do projeto até o prazo de entrega final da disciplina de Trabalho de Conclusão de Curso II do INE/UFSC, utilização de software livre e de código aberto, normatização dos documentos referentes ao projeto de acordo com órgãos especializados (ABNT, BU/UFSC).

1.2 PROCEDIMENTOS METODOLÓGICOS

O trabalho será desenvolvido utilizando a infraestrutura e recursos do Laborarório de Segurança em Computação (LabSEC/UFSC), onde será estudada a bibliografia referente aos assuntos abordados nesta pesquisa, visando encontrar uma abordagem para um sistema de eleição eletrônica utilizando certificação digital juntamente com blockchain. Frisando suas vantagens e desvantanges juntamente com seus custos.

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$ 2.500,00	R$ 2.500,00
Internet	1	R$ 1.000,00	R$ 1.000,00
Artigos	4	R$ 50,00	R$ 200,00
Material de consumo			
Mídia óptica	4	R$ 2,00	R$ 8,00
Outros recursos e serviços			
Impressões	200	R$ 0,20	R$ 40,00

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
Entrega do projeto do TCC	Autor	Orientador, coorientador, coordenador de projetos	Sistema de TCC	Uma 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	Uma vez, ao final do semestre 2019/1
Entrega de relatório de TCC II	Autor	Orientador, coorientador, coordenador de projetos, membros(s) da banca	Sistema de TCC	Uma vez, aproximadamente na metade do semestre 2019/2
Defesa do TCC	Autor	Orientador, coorientador, coordenador de projetos, membro(s) da banca	Pessoalmente	Uma vez, aproximadamente na metade do semestre 2019/2
Entrega final da monografia	Autor	Orientador, coorientador, coordenador de projetos, membro(s) da banca	Sistema de TCC	Uma vez, após a defesa, antes do término de 2019/2
Reuniões de acompanhamento do desenvolvimento	Autor	Orientador, coorientador	Pessoalmente, webconferência	Quinzenalmente
Monitorar o projeto	Autor	Orientador, coorientador	E-mail	Eventualmente
Convite de membro(s) da banca	Autor	A definir	Sistema de TCC	Uma vez, em meados do semestre 2019/1

6 RISCOS

Risco	Proba-bilidade	Impacto	Priori-dade	Estratégia de resposta	Ações de prevenção
Alteração de tema	Baixa	Alto	Alta	Alterar o escopo do tema, ou modificar completamente o tema.	Ter interação constante com o orientador.
Paralisação dos servidores da UFSC	Baixa	Alto	Média	Desenvolver o trabalho e pesquisa utilizando recursos próprios	Não se aplica
Problemas de saúde	Baixa	Alto	Alta	Procurar ajuda especializada para tratar corretamente	Evitar ambientes de exposição em caso de doenças, fazer exames para checar condição atual.
Perda de dados	Muito baixa	Alto	Média	Recuperar as cópias armazenadas na nuvem	Realizar backup de forma periódica de todo desenvolvimento
Falha nos equipa-mento(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 longos

REFERÊNCIAS

ADAMS, S. L. C. **Understanding PKI: Concepts, Standards, and Deployment Considerations**. [S.l.: s.n.], 2002.

ARANHA, Y. Execução de código arbitrário na urna eletrônica brasileira. 2018. Disponível em: <https://www.researchgate.net/publication-/326261911_Execucao_de_codigo_arbitrario_na_urna_eletronica_brasileira>.

NAKAMOTO, S. **Bitcoin: A peer-to-peer electronic cash system**. 2009. Disponível em: <http://www.bitcoin.org/bitcoin.pdf>.