UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Vinicius Macelai

ELEIÇÃO ELETRÔNICA UTLIZANDO BLOCKCHAIN E CERTIFICADO DIGITAL

Florianópolis

2019

Vinicius Macelai

ELEIÇÃO ELETRÔNICA UTLIZANDO BLOCKCHAIN E CERTIFICADO DIGITAL

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

2019

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

Ainda que vivemos no momento onde tudo é digital e fazemos as mais diversas tarefas de maneira eletrônica e online, quando o assunto é votação no meio eletrônico, existem as mais diversas e controversas opiniões a respeito.

No Brasil eleições eletrônicas têm sido utlizadas 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.

Os sistemas de votação eletrônicos atuais se baseiam em esquemas que utilizam de criptografia homomórfica, que permite que dados cifrados possam ser processados sem serem decifrados, assim garantidos propriedades importantes para o sistema.(SMART; VERCAUTEREN, 2010). Entretanto, esses esquemas são utilizados de forma centralizada, rodando apenas em um servidor central, sem a possiblidade de tais informações serem acessadas para o público em geral de maneira transparente.

Uma maneira de se realizar a autencicação no sistema seria utilizando certificado digital, que são arquivos digitais, que permite que uma pessoa seja identificada virtualmente, com garantia de autenticidade (ADAMS, 2002). Sendo no Brasil, o modelo adotado para gerenciar o sistema, a Infraestrutura de Chaves Públicas Brasileira (ICPBrasil). Já na área da educação, há a Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEdu), que pode ser utilizada em votações no âmbito acadêmico.

Para realizar a auditoria 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, além da possiblidade de rodar contratos inteligentes que podem processar os votos de maneira decentralizadas junto com a criptografia homomórfica para garantir o anonimato.

Neste trabalho foi optado por enfatizar o estudo e a utilização da blockchain e protocolo Ethereum, a qual fornece contratos inteligentes de alto nível. É apresentado um esquema que utliza esses contratos para garantir as propriedades já ditas, além do estudo de seu impacto financeiro.

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 MOTIVAÇÃO

1.2 PERGUNTA DE PESQUISA

1.3 HIPÓTESES

1.4 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.

1.5 OBJETIVO ESPECÍFICO

- 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 com certificado digital.

- 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.

1.6 METODOLOGIA

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.

1.7 RESULTADOS ESPERADOS

1.8 DESCRIÇÃO DO TRABALHO

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>.

SMART, N. P.; VERCAUTEREN, F. Fully homomorphic encryption with relatively small key and ciphertext sizes. In: NGUYEN, P. Q.; POINTCHEVAL, D. (Ed.). **Public Key Cryptography – PKC 2010**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. p. 420–443. ISBN 978-3-642-13013-7.