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 submetido 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

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

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, ainda carregam desconfiança sobre manter estas propriedades. 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 propriedades 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, contratos inteligentes

SUMÁRIO

1 INTRODUÇÃO

Ainda que vivamos no momento onde tudo é digital e façamos 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 garantindo propriedades importantes para o sistema.(SMART; VERCAUTEREN, 2010). Entretanto, esses esquemas são utilizados de forma centralizada, rodando apenas em um servidor central, sem a possibilidade de tais informações serem acessadas pelo o público em geral de maneira transparente.

Uma maneira de se realizar a autenticação 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 sobre o estado atual do sistema.(NAKAMOTO, 2009). Garantir 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 descentralizadas junto com a criptografia homomórfica para garantir o anonimato.

Neste trabalho, optou-se por enfatizar o estudo e a utilização da blockchain e protocolo Ethereum, a qual fornece contratos inteligentes de alto nível(BUTERIN, 2014). É apresentado um esquema que utiliza esses contratos para garantir as propriedades já citadas, 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, possibilitar a realização da verificação da eleição em uma blockchain de forma descentralizada e pública.

1.1 MOTIVAÇÃO

Os modelos de eleição utilizados nos dias de hoje são em sua maioria em cédulas de papel. Dependendo da dimensão da votação, isso externaliza grandes problemas, no que concerne a logística, que tem como consequência um aumento de custos. Já as abordagens que utilizam do meio eletrônico e online, geram grande desconfiança para a maioria das partes interessadas, com receio que o resultado seja hackeado e alterado. Consequentemente há uma demanda por um modelo de votação que seja mais auditável e aberto para sanar esse problema de desconfiança.

1.2 JUSTIFICATIVA

Este tema foi escolhido devido sua grande importância, que impacta basicamente todos os setores da sociedade, pois existem votações nas mais diversas esferas, desde a governança de empresas, até consultas de opinião sobre assuntos delicados. Além dos pontos anteriores citados, a utilização da recente tecnologia blockchain para a solução destes problemas é uma grande inovação na área. Este trabalho visa contribuir com modelos mais eficientes e transparentes, que beneficiarão a sociedade como um todo.

1.3 PERGUNTA DE PESQUISA

Este trabalho visa responder se é possível construir um modelo de eleição eletrônica utlizando a blockchain para garantir uma maior auditabilidade do sistema. Além de responder até qual volume de dados seria possível processar em contratos inteligentes na blockchain, juntamente com o cálculo ecônomico.

1.4 HIPÓTESES

- É possível criar um modelo de eleição eletrônica utilizando blockchain para forncer maior auditabilidade.
- É viável utilizar a blockchain Ethereum até qual volume dados.
- É economicamente viável esse modelo.

1.5 OBJETIVO GERAL

Estudar e criar a implementação de um sistema online de eleição, com foco principal na parte de realizar auditoria e verificação dos votos em blockchain com auxílio de contratos inteligentes, utilizando 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.

1.6 OBJETIVO ESPECÍFICO

i. 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.

ii. Implementar autenticação com certificado digital: Utilizar de um sistema já existente de votação e implementar a possiblidade de autenticar com certificado digital.

iii. Implementar possibilidade de verificação na blockchain Implementar um módulo para tornar o sistema mais auditável e verificável para o público em geral.

iv. Comparar e analisar as consequências do esquema.

1.7 METODOLOGIA

O trabalho será desenvolvido utilizando a infraestrutura e recursos do Laborarório de Segurança em Computação (LabSEC/UFSC), em que 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 e contratos inteligentes. Frisando suas vantagens e desvantanges juntamente com seus custos.

1.8 RESULTADOS ESPERADOS

Espera-se contribuir para o estado da arte em eleição eletrônica utilizando blockchain de forma que aumente a transparência e a auditabilidade do processo. É esperado também que tal abordagem tenha um gargalo no volume de dados processados, visto que a tecnologia blockchain por ser descentralizada, não conseguirá processar diversas transações por segundo. Além de que, como há muito processamento de dados, devido a criptografia homomórfica, tende a ser inviável economicamente para casos onde não há necessidade de tanta segurança.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 CRIPTOGRAFIA HOMOMÓRFICA

A ideia de usar homomorfismo na criptografia surgiu em um paper publicado com o objetivo de propor um criptossistema onde com o aumento da utilização de terminais remotos, não seria o ideal ter acesso a todo o banco de dados cifrados e então decifra-los para trabalhar os dados. Então surge o conceito de se conseguir operar com dados cifrados.(RIVEST; ADLEMAN; DERTOUZOS, 1978)

O nome criptografia homomórfica é derivado do conceito de homomorfismo em algébra abstrata, um homomorfismo é uma aplicação que preserva a estrutura entre duas estruturas algébricas X e Y.

$$f : X \longrightarrow Y \tag{2.1}$$

Seja α uma função de ciframento e β uma função de desencriptação correspondente. Sejam $x1$, $x2$ dados em texto plano. A tupla (α, β) é uma cifra homomórfica com o operador $\star$ se a proprieade for satisfeita:

$$\beta(\alpha(x1)) \star (\alpha(x2)) = x1 \star x2 \tag{2.2}$$

2.2 BLOCKCHAIN

Da sua tradução literal, blockchain significa cadeia de blocos, numa maneira simplista pode ser definido como cada bloco está ligado com o anterior, gerando assim uma cadeia. Estes blocos carregam as informações que são importantes para a rede, no caso de uma criptomoeda como Bitcoin, cada bloco teria dados sobre as transações realizadas naquele dado instante, ou seja, uma definição do estado atual do sistema.

A concepção da blockchain foi feita para ser um encadeamento de registros imutáveis, distribuídos e públicos. Os registros são imutáveis devido ao tipo de encadeamento que é feito com os blocos, onde o ponteiro para o bloco anterior é projetado para garantir a imutabilidade dos dados. Como é um protocolo distribuído, todas as informações não estão armezenadas em um sevidor central, não há um nodo mestre que coordene a rede. Justamente o oposto disso, a blockchain está replicada em todos os nodos participantes da rede, que podem estar espalhadas pelo mundo inteiro. Além de ser um esquema distribuído, o mesmo também é público, pois não há como censurar

uma parte de participar da rede, basta o interessado ter acesso a internet que ele poderá realizar a sua cópia da base de dados.(UNDERWOOD, 2016)

2.2.1 Cadeia de blocos

A estrutura de um bloco é basicamente a seguinte:

- Constante de valor 0xD9B4BEF9.
- Tamanho do bloco em *bytes*.
- Cabeçalho do bloco, que consiste em 6 itens.
- Quantidade de transações no bloco.
- Transações em si.

Vale notar aqui que as transações detêm de uma estrutura de dados que permite a criação de *scripts*, além de permitir a inserção de dados arbitrários.

Já a estrutra do cabeçalho do bloco:

- Versão do bloco.
- *Hash* do bloco anterior.
- *Hash* do bloco atual, baseado em todas as transações do bloco.
- *Timestamp* em que o bloco foi criado.
- *Nonce*, número aleatório que é utilizado na mineração dos blocos.
- *Bits*, objetivo atual da mineração em formato compactado.

Esta estrutura de dados permite que qualquer participante da rede possa validar o bloco de maneira rápida. Existe o desafio matemático para a criação de blocos, isto é, para criar um novo bloco, ele deve calcular um *Hash* com uma pseudo colisão de acordo com a variável *Bits* do cabeçalho. Resolver esse desafio matemático é chamado de mineração, e a cada bloco que passa ele se torna mais difícil, entretanto, uma vez que sua solução é conhecida, é extremamente fácil de validar sua corretude. Há diversas soluções possíveis para determinado bloco, porém basta apenas uma ser resolvida.(ANTONOPOULOS, 2014)

Como a mineração de blocos se torna cada vez mais difícil, a probabilidade de algum atacante conseguir reescrever um bloco anterior é mínima. Visto que ele teria que concluir o desafio matemático para o bloco que deseja modificar e ainda todos os sucessores dele.

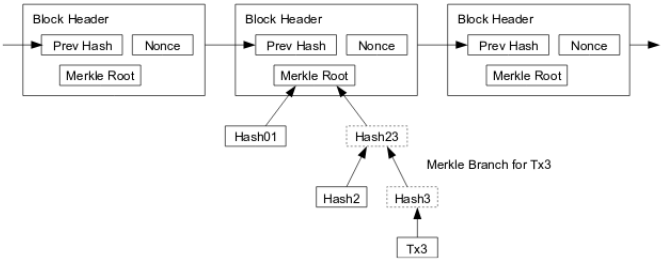

Figura 1 – Imagem tirada do whitepaper do Bitcoin

2.3 CONTRATOS INTELIGENTES

Já no surgimento da blockchain descrito no protocolo do Bitcoin, havia espaço para criação *scripts* nas transações. Porém estes *scripts* foram concebidos para serem simples, com a ideia de não sobrecarregar a rede com a execução de códigos complexos. Um exemplo de *script* trivial seria o congelamento de fundos até certa data futura. Como não é permitido *loops* em sua estrutura, isto impacta na não Turing completude da linguagem de *script*.(NAKAMOTO, 2009)

Com o desejo de se ter *scripts* mais potentes foi criado o conceito de contratos inteligentes que são Turing-completos e ainda guardam o estado atual do sistema. (BUTERIN, 2014)

Desta forma é possível criar aplicações que rodam de forma descentralizada e que podem ter seu estado atual verificado por qualquer participante do sistema em qualquer dado momento. Ainda garantindo as propriedades da blockchain.

REFERÊNCIAS

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

ANTONOPOULOS, A. M. **Mastering Bitcoin: Unlocking Digital Crypto-Currencies**. 1st. ed. [S.l.]: O'Reilly Media, Inc., 2014. ISBN 1449374042, 9781449374044.

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>.

BUTERIN, V. **Ethereum: A next-generation smart contract and decentralized application platform**. 2014. Accessed: 2016-08-22. Disponível em: <https://github.com/ethereum/wiki/wiki/White-Paper>.

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

RIVEST, R. L.; ADLEMAN, L.; DERTOUZOS, M. L. On data banks and privacy homomorphisms. **Foundations of Secure Computation, Academia Press**, p. 169–179, 1978.

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.

UNDERWOOD, S. Blockchain beyond bitcoin. **Communications of the ACM**, v. 59, p. 15–17, 10 2016.