INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS TERESINA CENTRAL
TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

FABIANO DE SANTANA RIBEIRO SOBRINHO

SISTEMA DE ELEIÇÕES UTILIZANDO BLOCKCHAIN

TERESINA, PIAUÍ

2019

FABIANO DE SANTANA RIBEIRO SOBRINHO

SISTEMA DE ELEIÇÕES UTILIZANDO BLOCKCHAIN

Projeto apresentado à Banca Examinadora como requisito para aprovação na disciplina de Trabalho de Conclusão de Curso II do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Piauí.

Orientador: Prof. M^{e}. Ely da Silva Miranda

TERESINA, PIAUÍ

2019

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD

Ribeiro Sobrinho, Fabiano de Santana

R193c Sistema de eleções utilizando blockchain / Fabiano de Santana Ribeiro Sobrinho. - 2019.

33 f.: il. color.

Trabalho de Conclusão de Curso (Tecnologia em Análise e Desenvolvimento de Sistemas) - Instituto Federal do Piauí, Campus Teresina Central, 2019.

Orientador: Prof. Me. Ely da Silva Miranda.

1. Blockchain. 2. Sistema de votação. 3. Segurança. 4. Privacidade. I.Título.

CDD - 004.21

Elaborado por Sindya Santos Melo CRB 3/1085

FABIANO DE SANTANA RIBEIRO SOBRINHO

SISTEMA DE ELEIÇÕES UTILIZANDO BLOCKCHAIN

Projeto apresentado à Banca Examinadora como requisito para aprovação na disciplina de Trabalho de Conclusão de Curso II do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Piauí.

Aprovado pela banca examinadora em _____.

BANCA EXAMINADORA:

Prof. M^{e}. Ely da Silva Miranda
Instituto Federal de Educação, Ciência e Tecnologia do Piauí - IFPI

Prof. M^{e}. Rogério da Silva
Instituto Federal de Educação, Ciência e Tecnologia do Piauí - IFPI

Prof. Dr. Adalton de Sena Almeida
Instituto Federal de Educação, Ciência e Tecnologia do Piauí - IFPI

TERESINA, PIAUÍ

2019

Dedico este trabalho a todos que me ajudaram de alguma forma, obrigado!

AGRADECIMENTOS

Agradeço ao Prof. Ely Miranda, pelas orientações, por dividir seu conhecimento comigo e seu grande empenho em ajudar não somente a mim mas vários outros alunos.

Ao Prof. Rogério Silva, pela dedicação, comprometimento e por ser um Amigo/Pai quando necessário.

Aos amigos Daniel Farias(GOD), Leôncio Ferreira, Kairo Costa e Mateus Oliveira pelo incentivo e grande ajuda nessas horas difíceis.

À minha parceira Sywrah Gabriella por todo apoio e carinho, muito carinho. Eu te amo.

E por fim, ao Instituto Federal do Piauí pela oportunidade de realizar o curso de Análise e Desenvolvimento de Sistemas.

"We’re all pretty bizarre. Some of us are just better at hiding it, that’s all"
(Andrew - The Breakfast Club)

RESUMO

A maioria dos sistema digitais de votação estão vulneráveis a algum tipo de ameaça. Ameaças como manipulação do *software* de votação através da introdução de trechos de código maliciosos, abuso da arquitetura centralizada, utilizando-se do acesso administrativo para fraudar os resultados do processo e a manipulação do hardware por dispositivos externos especializados. Pesquisadores da Argonne National Laboratories relataram que qualquer indivíduo com acesso a um dispositivo eletrônico de votação podem instalar componentes específicos que manipulem as funções do dispositivo. Perante essas dificuldades, foi observada a necessidade de um sistema que utilize uma base de dados distribuída e assim possibilitar mais segurança e auditoria das informações armazenadas. Tendo isso em vista, o presente trabalho apresenta um protótipo de sistema eleitoral utilizando a tecnologia blockchain, considerando as suas características de segurança e privacidade que vêm se provando consistentes através das aplicações nos sistemas de transações do Bitcoin, difundindo sua utilização nos âmbitos da saúde, gestão pública e internet das coisas. Para o desenvolvimento do protótipo, foi utilizado um serviço de código aberto especializado em blockchain. O sistema permitirá o completo acompanhamento dos resultados da eleição, visando uma maior transparência do processo de votação.

Palavras-chaves: blockchain, sistema de votação, ameaças, segurança, privacidade.

ABSTRACT

Every digital voting system is vulnerable to some kind of threat. Threats like, manipulation of voting system through the introduction of malicious code snippets, abuse of the centralized architecture using administrative access to defraud the results and hardware manipulation by specialized external devices. Researchers of Argonne National Laboratories reported that any individual with access to a device Electronic voting machines may install specialized components that manipulate the functions of the device. Faced with these difficulties, it was observed that a system a distributed database and thus enable more security and audit of information stored. With this in mind, the present work presents a prototype system electoral process using blockchain technology, taking into account its security characteristics and privacy that has proven to be consistent across applications in transaction systems of Bitcoin, spreading its use in the areas of health, public management and internet of things. For the development of the prototype, an open source service was blockchain The system will allow the complete monitoring of the results of the election, aiming to transparency of the voting process.

Key-words: blockchain, voting system, threat, security, privacy.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

SBC	Sociedade Brasileira de Computação
API	Aplication Program Interface

SUMÁRIO

1 INTRODUÇÃO

Neste trabalho é apresentado um protótipo de sistema eleitoral de código aberto utilizando a tecnologia blockchain. Nele são evidenciados os aspectos de segurança e privacidade fornecidos pela mesma, justificando a importância desses aspectos no protótipo proposto.

1.1 CONTEXTUALIZAÇÃO

Desde o nascimento da democracia, as eleições realizadas pelo mundo recebem acusações de ilegitimidade [FOLLOWMYVOTE, 2016]. Notoriamente a sociedade democrática começa a adotar tecnologias para melhorar a eficiência do processo eleitoral. Muitas pessoas estão descobrindo que certos tipos de tecnologias como, urnas eletrônicas e aplicações web, podem ser extremamente vulneráveis [ROHR, 2012], podendo ter o potencial de influenciar injustamente os resultados das eleições.

O crescimento da Internet deu início a um conjunto de novos desafios à proteção do processo democrático. Em uma campanha eleitoral de apenas 45 dias, uma exposição negativa decorrente de notícias falsas (*fake news*) pode significar o fracasso de um candidato, além de outros danos [MARTINS, 2017]. Também, as recentes alegações de interferência dos russos em eleições ucranianas, francesas, alemãs e norte americanas através das mídias sociais ressaltaram as ameaças impostas pelo advento da internet [ANNAN, 2018]. Contudo, possivelmente um dos principais desafios da internet é o espectro de ataques cibernéticos contra o sistema de votação eletrônica. Cibersegurança era um tópico pouco explorado quando as primeiras máquinas de votação eletrônica chegaram ao mercado no começo da década de 90. Programadores eram meramente incentivados a trabalhar na segurança de seus softwares, e os organizadores da eleição estavam mais preocupados em tornar a votação barata, fácil e mais acessível ao eleitorado [KIRBY; MASI; MAYMI, 2016].

Segundo a análise de segurança do software da urna eletrônica brasileira realizada em 2012 [ARANHA et al., 2013], foram detectadas um conjunto de vulnerabilidades, como cifração inadequada, algoritmos obsoletos e desenvolvimento inadequado do software. Essas vulnerabilidade permitem a violação completa do sigilo do voto. Ainda, segundo a análise, tendo em vista o relatório feito sobre o mesmo sistema em 2002 pela SBC e as preocupações levantadas, pode-se concluir que não houve incremento significativo.

1.2 JUSTIFICATIVA

As bases de dados tradicionais são mantidas individualmente por organizações, as quais têm completo controle sobre as informações, incluindo a possibilidade de fraudá-las. Em muitos casos nenhum problema é gerado, pois a organização que mantém os dados os mantém para seu próprio e único benefício, logo, os motivos para fraudá-los são incoerentes [FOLLOWMYVOTE,

2016].

Porém, existem casos em que os dados que estão sendo armazenados são muito sensíveis e prejudiciais a terceiros, como dados financeiros e dados estritamente pessoais. Então, mesmo que uma organização responsável pudesse garantir que nunca efetuaria uma operação fraudulenta na base de dados, a possibilidade de invasão e manipulação dos dados continua existente [FOLLOWMYVOTE, 2016].

Portanto, um modo claro de assegurar a integridade dos dados e impedir a sua manipulação sem fiscalização, é tornando-os públicos. Por exemplo, o portal da transparência [Portal da Transparência, 2004] oferece ferramentas de acessibilidade às informações, que permitem aos cidadãos de forma cada vez mais eficiente assegura a correta aplicação dos recurso públicos.

A aplicação de novas tecnologias podem reduzir a dependência em autoridades centrais, além de fornecer melhorias na segurança, transparência e integridade nos sistemas de votação. Consoante a isso, a tecnologia Blockchain possui uma infraestrutura cuja a segurança é baseada na descentralização dos registro de dados, tornando os dados auditáveis para qualquer indivíduo [FOLLOWMYVOTE, 2016].

O blockchain vem sendo aplicado e provado em diversos campos, tendo seu maior destaque no registro de transações de cryptomoedas (Bitcoin, Ethereum, Ripple). Em 2015, Marc Andreessen, um notório empreendedor do vale do silício, listou o blockchain como a maior invenção desde a internet. Johann Palychata do banco francês BNP Paribas escreveu na revista Quintessence que a invenção do blockchain deveria ter a mesma relevância das máquinas a vapor, pois tem o potencial de mudança que vai além do mundo das finanças [CROSBY et al., 2016].

A apresentação de novas tecnologia à sociedade geralmente produz custos financeiros exacerbados aos investidores pioneiros. Porém, contrariando esse costume, a tecnologia blockchain pode reduzir drasticamente os custos do processo eleitoral e liberar o investimento do contribuinte para outros projetos [FOLLOWMYVOTE, 2016]. Perante as dificuldades de se armazenar seguramente os votos e manter o sigilo dos usuários votantes, este trabalho propõe um protótipo de sistema eleitoral baseado em blockchain, usufruindo das características de segurança e privacidade oferecidos pela tecnologia.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

O objetivo geral deste trabalho é desenvolver um protótipo de sistema eleitoral baseado em blockchain, dispondo dos mecanismos de segurança, integridade e transparência oferecidos pela tecnologia, objetivando averiguar e entender tais mecanismos.

1.3.2 Objetivos Específicos

- Promover um aprendizado das tecnologias e conceitos que cercam a arquitetura do blockchain;
- Desenvolver um protótipo de sistema eleitoral utilizando um serviço blockchain implementado por terceiros;
- Demonstrar os benefícios da tecnologia e sua arquitetura.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 CRIPTOGRAFIA ASSIMÉTRICA

Modelo de criptografia criado na década de 1970 pelo matemático Clifford Cocks que trabalhava no serviço secreto inglês, o GCHQ, na qual cada parte envolvida na comunicação usa duas chaves diferentes (assimétricas) e complementares, uma privada e outra pública. A chave pública pode ficar disponível para qualquer pessoa que queira se comunicar com outra de modo seguro, mas a chave privada deverá ficar em poder apenas de cada titular. É com a chave privada que o destinatário poderá decodificar uma mensagem que foi criptografada para ele com sua respectiva chave pública [OLIVEIRA, 2012].

2.2 ASSINATURA DIGITAL

O sistema de criptografia assimétrica também é utilizado como um meio de assinatura digital. A assinatura digital é uma aplicação criptográfica que aplica ao meio digital os princípios de uma assinatura convencional. Existem duas propriedades essenciais em uma assinatura convencional [PIRES, 2016]:

1. Autenticidade: qualquer pessoa pode saber quem fez a assinatura, mas apenas o autor deve saber fazê-la;
2. Endosso: a assinatura deve estar vinculada ao documento que se pretende endossar e a nenhum outro.

O processo da assinatura digital pode ser descrito como: o emissor cifra (ou seja, atesta autenticidade) a mensagem com sua chave privada e a envia, em um processo denominado de assinatura digital. Cada um que receber a mensagem deverá verificar a validade da assinatura digital, utilizando para isso a chave pública do emissor, reconhecendo de fato, que a mensagem não foi adulterada. Como a chave pública do emissor apenas decifra (ou seja, verifica a validade) mensagens cifradas com sua chave privada, obtém-se a garantia de autenticidade, integridade e não repudiação da mensagem, o que é apoiado pela função hashing, pois se alguém modificar um bit do conteúdo da mensagem ou se outra pessoa assiná-la ao invés do próprio emissor, o sistema de verificação não irá reconhecer a assinatura digital dele como sendo válida [OLIVEIRA, 2012].

2.3 FUNÇÃO HASHING

A assinatura digital obtida através do uso da criptografia assimétrica ou de chave pública infelizmente não pode ser empregada, na prática, de forma isolada, é necessário o emprego de um mecanismo fundamental para o adequado emprego da assinatura digital. Este mecanismo é a função hashing. Na prática é inviável e contraproducente utilizar puramente algoritmos de chave

pública para assinaturas digitais, principalmente quando se deseja assinar grandes mensagens, que podem levar preciosos minutos ou mesmo horas para serem integralmente cifradas com a chave privada de alguém, ao invés disso, é empregada uma função hashing, que gera um valor pequeno, de tamanho fixo, derivado da mensagem que se pretende assinar, de qualquer tamanho, para oferecer agilidade nas assinaturas digitais, além de integridade confiável [OLIVEIRA, 2012].

Serve, portanto, para garantir a integridade do conteúdo da mensagem que representa, por isto, após o valor hash de uma mensagem ter sido calculado através do emprego de uma função hashing, qualquer modificação em seu conteúdo mesmo em apenas um bit da mensagem será detectada, pois um novo cálculo do valor hash sobre o conteúdo modificado resultará em um valor hash bastante distinto [OLIVEIRA, 2012].

2.4 BLOCKCHAIN

Em 2008, um indivíduo (ou grupo) chamado Satoshi Nakamoto publicou um artigo intitulado "Bitcoin: A Peer-To-Peer Electronic Cash System". Este artigo descreve uma versão *Peer-To-Peer* de uma moeda eletrônica que possibilita o pagamento online entre duas partes sem a necessidade da intervenção de instituições financeiras [CROSBY et al., 2016].

Meses depois, uma implementação baseada no artigo foi lançada com um registro inicial de um bloco de 50 moedas, dando início ao Blockchain. Qualquer pessoa poderia instalar o software de código aberto e fazer parte da rede *Peer-To-Peer*, aumentando a popularidade da rede de gerenciamento do blockchain [CROSBY et al., 2016].

O blockchain funciona como um registro de auditoria para um banco de dados, ele é administrado por uma rede de computadores a qual nenhum computador é individualmente responsável por armazenar e manter o banco de dados. Qualquer computador pode entrar e sair da rede quando desejar sem danificar a integridade e disponibilidade dos dados. O blockchain possibilita que os computadores reconstruam o banco de dados a partir dos seus blocos armazenados [FOLLOWMYVOTE, 2016].

2.4.1 Transação

A tecnologia blockchain utiliza a criptografia assimétrica, também conhecida como criptografia da chave pública, onde cada indivíduo da transação possui uma chave privada que é mantida em segredo, como uma senha, e uma chave pública que é conhecida por todos e quaisquer indivíduos. Uma transação é iniciada quando o futuro proprietário do artefato transacionado envia sua chave pública para o atual proprietário. As chaves públicas no blockchain representam endereços gerados criptograficamente, e cada artefato é associado a um endereço. A transação acontece quando um artefato é enviado de um endereço para outro.

Toda transação precisa ser assinada digitalmente com a chave privada do executor da

transação. A assinatura digital é dividida em duas fases: fase de assinar e a fase de verificação. Por exemplo, um usuário Alice deseja enviar uma mensagem para um usuário Bob. Na fase de assinar, Alice encripta seus dados com sua chave privada e os envia a Bob, junto com os dados originais. Na fase de verificação, Bob valida os dados enviados com a chave pública de Alice, pois através da chave pública, Bob pode checar se a integridade dos dados foi corrompida [ZHENG et al., 2017].

Cada transação é enviada para todos os nós da rede e registrada em um bloco do blockchain depois da verificação. Toda transação precisa ser verificada pelos nós de verificação da rede. Os nós de verificação seguem as duas regras abaixo para certificar que a transação é válida [CROSBY et al., 2016]:

1. Verificar a posse do artefato através da assinatura digital presente na transação;
2. Certificar que o proprietário possui o montante que está sendo transacionado, analisando cada transação relacionada à chave pública do proprietário registrada no blockchain. Isso confirma que o proprietário possui a quantidade necessária do artefato a ser transferido.

2.4.2 Cronologia e Segurança da Transação

O sistema baseado em blockchain ordena as transações colocando elas em blocos. É considerado que as transações pertencentes ao mesmo bloco tenham o mesmo tempo de geração. Os blocos são vinculados cronologicamente de forma linear e cada bloco possui informação do bloco anterior. Porém, qualquer nó da rede pode coletar transações não confirmadas, criar um novo bloco e transmiti-lo para o resto da rede como o próximo bloco a ser registrado no blockchain. Existem vários blocos criados ao mesmo tempo, por diferentes nós. Para delimitar o registro foi utilizado o *proof of work*, conforme descrito a seguir. [CROSBY et al., 2016].

Proof of work é uma estratégia de consenso. Em um sistema distribuído, algo ou alguém tem que ser selecionado para registrar as transações. O modo mais fácil consiste em uma seleção randômica. Contudo, seleção randômica é vulnerável a ataques. Então, caso um nó pretenda registrar um bloco de transações, um esforço precisa ser feito para provar que o nó não possui intenções de danificar a rede, geralmente o esforço significa cálculo computacional. Embora seja raro, um ou mais nós podem efetuar o cálculo computacional concomitantemente, gerando ramificações do blockchain. Porém, baseado no protocolo do *proof of work*, a subdivisão a ser aceita será a que se tornar maior. Por exemplo, considere duas ramificações criadas pelo blocos validados simultaneamente U4 e B4. U4 e B4 são blocos validados que continuarão validando blocos, até que um deles se torne a maior ramificação [ZHENG et al., 2017].

Sabendo que cada bloco é vinculado ao bloco anterior, possuindo informações do mesmo, qualquer entidade que queira fraudar as transações registradas no sistema terá que modificar não somente o bloco desejado, mas também todos os outros blocos subsequentes. Então, quanto mais antiga a transação for, mais ao fundo da cadeia blockchain ela estará, tornando-a mais segura.

3 TRABALHOS RELACIONADOS

3.1 VOTE WATCHER

VoteWatcher é uma *start-up* proveniente da Blockchain Technologies Corporation, uma empresa que oferece serviços utilizando blockchain e funciona como incubadora para novas iniciativas [Blockchain Technologies Corporation, 2018]. O sistema utilizado já fora utilizado em mais de 20 eventos, possuindo mais de 100,000 votos contados [VOTEWATCHER, 2016], sendo assim, um dos sistemas mais maduros do ramo. A *start-up*, através do uso do blockchain, propõe trazer completa transparência ao modelo de sistema eleitoral atual.

A plataforma desenvolvida utiliza um sistema de votação por cédula, pois a familiaridade do usuário com o mesmo é um fator extremamente relevante. Os progressos da eleição são disponíveis online no blockchain, sendo assim, cada passo do processo é auditável [VOTEWATCHER, 2016].

3.2 FOLLOW MY VOTE

Follow My Vote é uma *start-up* que fornece uma plataforma de votação transparente onde cada participante pode acompanhar o progresso da eleição em tempo real. De acordo com os integrantes da *start-up*, o intuito do trabalho é revolucionar os sistemas de votações atuais utilizando a tecnologia blockchain, utilizando-se de uma plataforma fácil, segura e de baixo custo [FOLLOWMYVOTE, 2016].

O sistema de votação é livre para ser instalado em *tablets*, computadores e *smartphones*. Quando instalado, o sistema segue a logística de uma cabine de votação com cédulas. O usuário se identifica e os organizadores analisam as credenciais apresentadas, caso aprovado, o usuário ganha permissão ao voto que será registrado em um blockchain.

3.3 VOTEBOOK

Votebook é uma proposta escrita por KIRBY; MASI; MAYMI para estabelecer normas em sistemas de votação utilizando blockchain. A proposta elencou os seguintes requisitos para o sistema de votação [KIRBY; MASI; MAYMI, 2016]:

1. Assegurar que uma pessoa cheque seu voto, para verificar se o mesmo foi contabilizado;
2. O sistema deve evitar voto forçado;
3. Dependendo das regras da eleição, o sistema deve fornecer ou omitir resultados temporários da votação;
4. O sistema não deve forçar votantes indecisos a votar;

5. Caso o resultado da eleição seja contestado, o sistema deve permitir uma completa auditoria.

Considerando diversos cenários, a proposta elencou as seguintes observações adicionais relacionadas aos usuários [KIRBY; MASI; MAYMI, 2016]:

1. Nem todo votante possui um computador com acesso a internet;
2. A eleições não são globais, como por exemplo, somente cidadãos podem votar;
3. O sistema mais prático será aquele que mudará menos o comportamento do votante;
4. Votação remota não é possível devido a grande quantidade de ameaças.

Analisando os trabalho relacionados, o protótipo desenvolvido neste trabalho segue as diretrizes propostas por KIRBY; MASI; MAYMI. Enfatizando a impossibilidade de votação remota devido às fragilidades provenientes dos usuários. Este protótipo segue uma linha voltado para o aprendizado, o que o difere das iniciativas dos trabalhos relacionados aqui citados.

4 PROTÓTIPO ELEIÇÃO BASEADO EM BLOCKCHAIN

A fim de registrar os votos e garantir a democracia, todo sistema de eleição têm de ser tão seguro quanto possível, auditável e consistente com a expectativa de privacidade dos eleitores [KIRBY; MASI; MAYMI, 2016]. Além disso, a descentralização sobre os dados torna-se um adicional relevante, tendo em vista que ela possibilita a fiscalização dos resultados por quaisquer que seja o indivíduo fiscalizador.

Diante da necessidade de se obter um sistema seguro, auditável e descentralizado, é proposto neste trabalho um protótipo de sistema de eleição baseado na tecnologia blockchain, utilizando-se de benefícios como integridade , acuidade e auditabilidade para atender aos requisitos. A plataforma web do protótipo proposto foi desenvolvida em Python, utilizando o framework Django. Para o registro de transações estritamente sensíveis, como os votos, foi utilizado o Bigchain [BigchainDB, 2018], um serviço blockchain. Os demais dados foram armazenados em um banco de dados PostgreSQL. O cadastramento de partidos e candidatos na plataforma, é realizado pelos administradores da eleição, evento o qual antecede a realização da votação. Após o cadastramento de candidatos e partidos, a alteração dos mesmos só pode ser efetuada no período pré votação.

4.1 BIGCHAIN

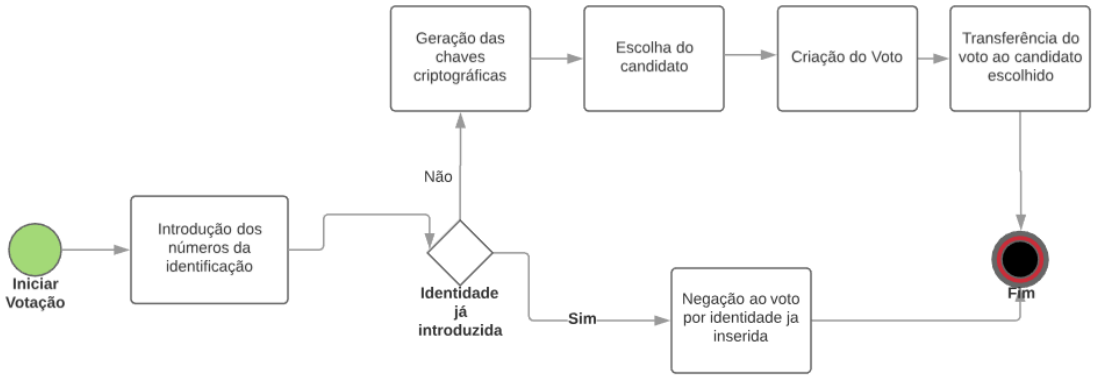
Conforme citado acima, Bigchain é um serviço blockchain de codigo aberto empregado no protótipo para o armazenamento de dados sensíveis. Este serviço consiste em uma base de dados que oferece as funcionalidades necessárias de descentralização e imutabilidade preteridas por um serviço blockchain. O serviço é de fácil conexão com as linguagens de programação Python e Javascript, possuindo uma documentação detalhada. Além disso, o Bigchain oferece a possibilidade de integração com a plataforma MongoDB [MongoDB, 2018], utilizando os comandos de consulta da plataforma para seu enriquecimento.

4.2 FLUXO DO PROCESSO DE VOTAÇÃO

Para realizar a votação, conforme exposto no fluxograma de processos da figura 1, o votante insere os números de identidade contido no documento de identificação oficial optado pelos administradores da eleição. Caso o usuário queira votar mais de uma vez, o sistema acusará um erro ao introduzir sua identidade novamente, tendo em vista que o votante tem direito a apenas um voto. Entretanto, se a identidade passar pelo processo de checagem, o sistema gera um par de chaves criptográficas para o votante, uma pública e outra privada. Logo após a geração das chaves, o votante escolhe seu candidato e uma transação de criação do voto é iniciada no blockchain, sendo registrada e assinada com as chaves pública e privada respectivamente. E por fim, a posse do voto que está sob a chave pública do votante, é transferida para chave pública do

candidato através de uma transação de transferência no blockchain, contabilizando o voto para aquele candidato.

Ilustração 1 – Fluxograma do processo de votação



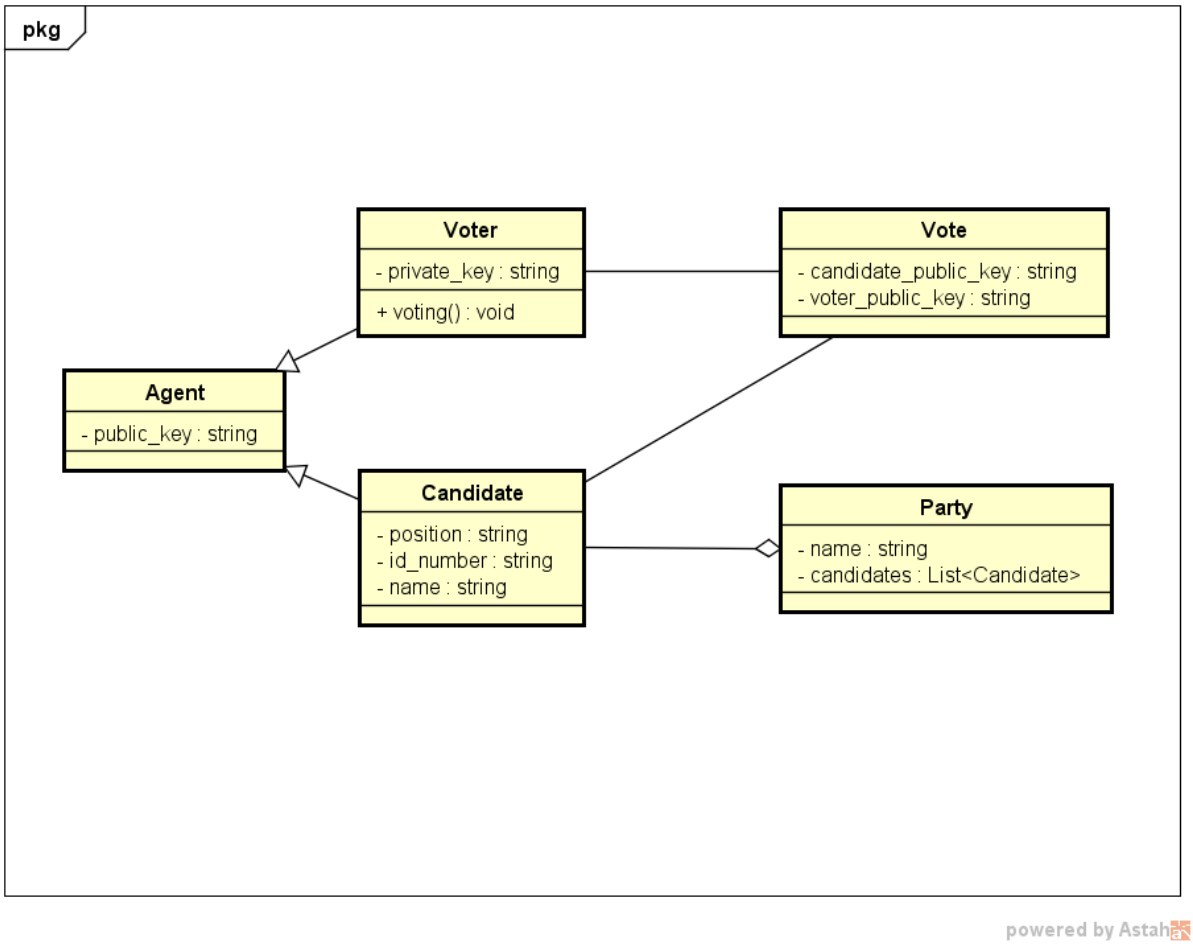
FONTE: Elaborado pelo autor

A contabilização dos votos registrados no blockchain é feita online através da plataforma web, onde quaisquer indivíduos, autenticados como votante ou não, podem acompanhar os resultados do processo de votação. Ao fim do processo de votação, a aplicação seleciona os candidatos eleitos.

4.3 DIAGRAMA DE CLASSES

O diagrama de classes, presente na figura 2, demonstra todas as entidades e seus respectivos atributos e métodos contidos no sistema. As entidades são descritas a seguir:

Ilustração 2 – Diagrama de Classes



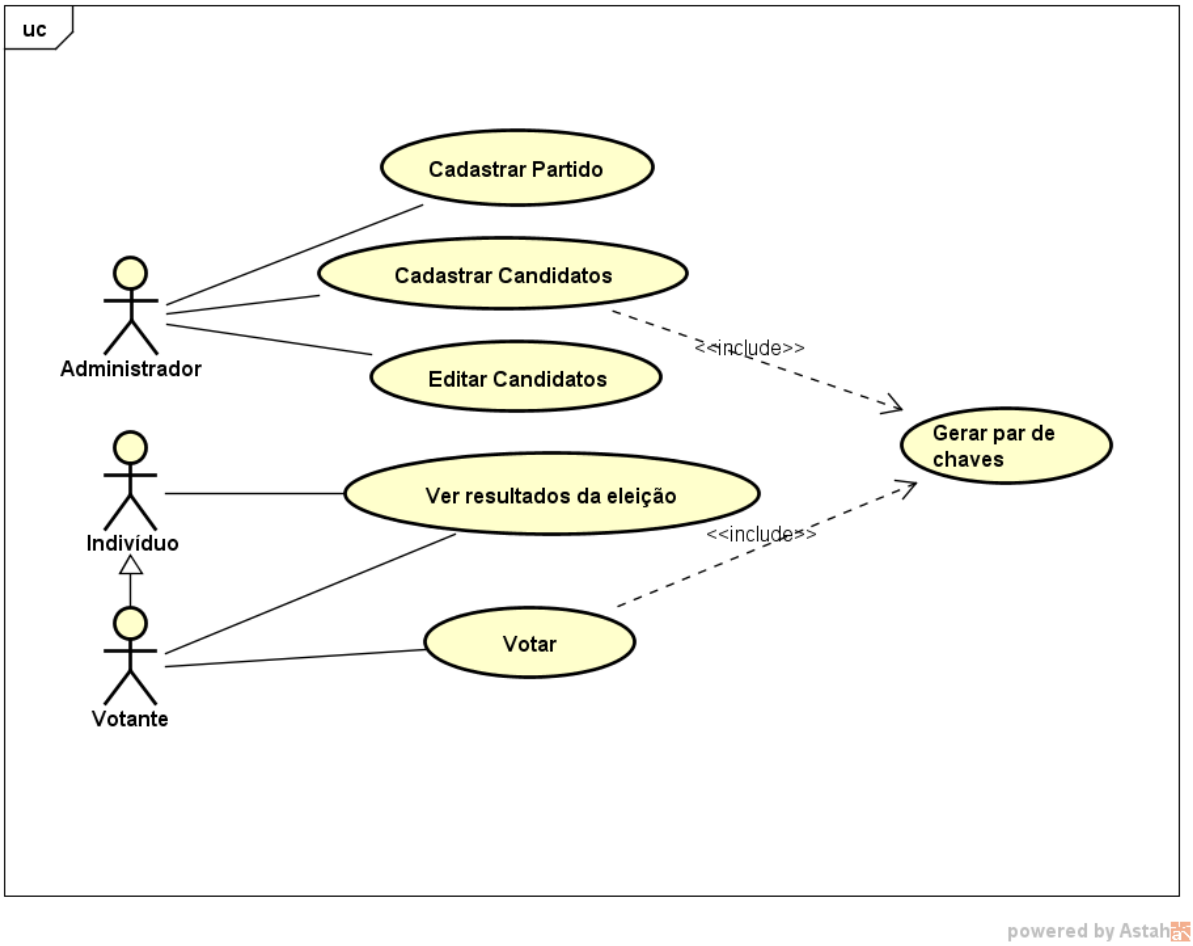
FONTE: Elaborado pelo autor

- *Voter*(Votante): Todo votante possui um par de chaves criptográficas, uma privada e outra pública, que serão utilizadas no método de votação.
- *Candidate*(Candidato): Todo candidato possui uma chave pública onde o voto é atribuído;
- *Vote*(Voto): Todo voto registra duas chaves públicas, uma do votante e outra do candidato;
- *Party*(Partido): Todo partido é composto por um ou mais candidatos.

4.4 DIAGRAMA DE CASO DE USO

O diagrama de caso de uso, presente na figura 3, apresenta os casos de usos e os atores relacionados. Os principais casos de usos são descritos abaixo.

Ilustração 3 – Diagrama de Caso de Uso



FONTE: Elaborado pelo autor

4.4.1 Cadastrar Partido

- Descrição: Este caso de uso é utilizado para cadastrar um partido no sistema.
- Pré-condição: Este caso de uso pode iniciar se e somente se o ator tiver permissões administrativas.
- Pós-condições: Após o final deste caso de uso, o sistema deve retornar uma mensagem "Partido cadastrado com sucesso".
- Ator Primário: Administrador.
- Fluxo de Eventos Principal:

  1. O usuário acessa o modulo administrativo;
  2. O usuário preenche os campos de cadastro do partido;
  3. Ao clicar em salvar, o sistema registra uma instância de partido no banco de dados;

4. Mensagem de sucesso é retornada; O caso de uso se encerra.

- Exceções:

1. Campos Vazios;
2. Nome de partido ja existente;

4.4.2 Cadastrar Candidato

- Descrição: Este caso de uso é utilizado para cadastrar um candidatos no sistema.
- Pré-condição: Este caso de uso pode iniciar se e somente se o ator tiver permissões administrativas.
- Pós-condições: Após o final deste caso de uso, o sistema deve retornar uma mensagem "Candidato cadastrado com sucesso".
- Ator Primário: Administrador.
- Fluxo de Eventos Principal:

1. O usuário acessa o modulo administrativo;
2. O usuário preenche os campos de cadastro do candidato;
3. Ao clicar em salvar, o sistema registra uma instância de candidato no banco de dados;
4. Mensagem de sucesso é retornada; O caso de uso se encerra.

- Exceções:

1. Campos Vazios;

4.4.3 Ver resultado da eleição

- Descrição: Este caso de uso é utilizado para verificar o resultado das eleições;
- Pós-condições: Após o final deste caso de uso, o sistema deve retornar uma tela com o resultado das eleições;
- Ator Primário: Indivíduo;
- Fluxo de Eventos Principal:

1. O usuário acessa a tela de resultado de eleições;
2. Sistema gera os resultados da eleição.

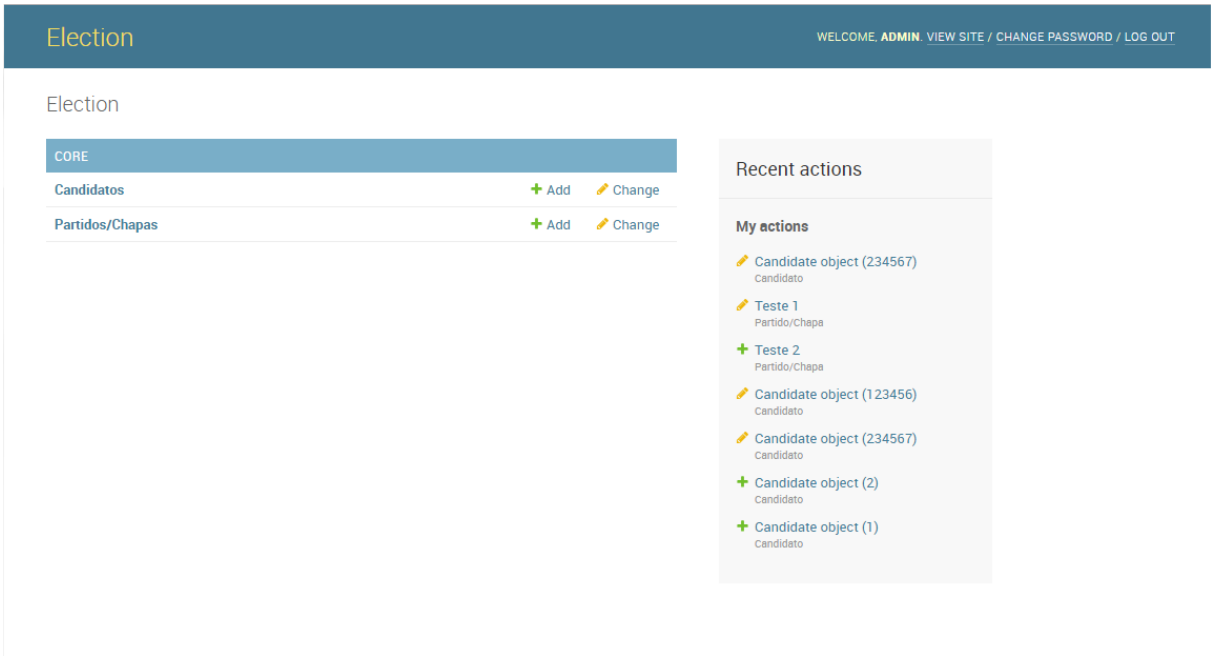
4.4.4 Votar

- Descrição: Este caso de uso é utilizado para efetuar um voto.
- Pós-condições: Após o final deste caso de uso, o sistema deve retornar uma mensagem "voto registrado com sucesso".
- Ator Primário: Votante.
- Fluxo de Eventos Principal:
    1. O usuário acessa o a tela de votação;
    2. O usuário seleciona o candidato desejado;
    3. Ao clicar em salvar, o sistema cria um voto no blockchain e o transfere ao candidato desejado;
    4. Mensagem de sucesso é retornada.
- Exceções:
    1. Campos Vazios;
    2. Já existe um voto registrado com esse usuário.

4.5 MÓDULO ADMINISTRADOR

O módulo administrador é a divisão responsável pela criação, remoção e edição de candidatos e partidos. Os candidatos e partidos são os únicos elementos manipuláveis, votos e votantes são imutáveis. A imagem 4 ilustra os elementos manipuláveis, onde o botão verde, situado ao lado direito do elemento, é responsável pelo redirecionamento para a tela de criação e o amarelo pelo redirecionamento à tela de edição dos elementos.

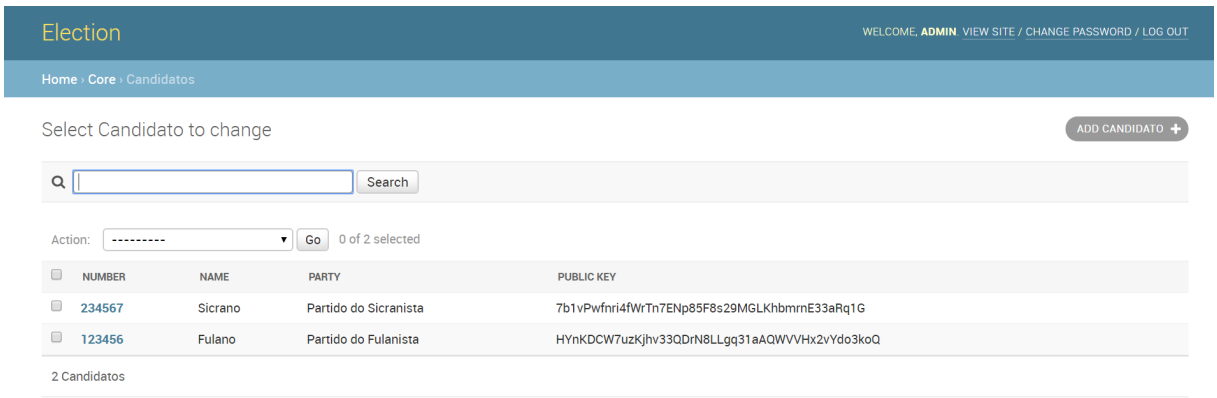
Ilustração 4 – Painel inicial da administração



FONTE: Elaborado pelo autor

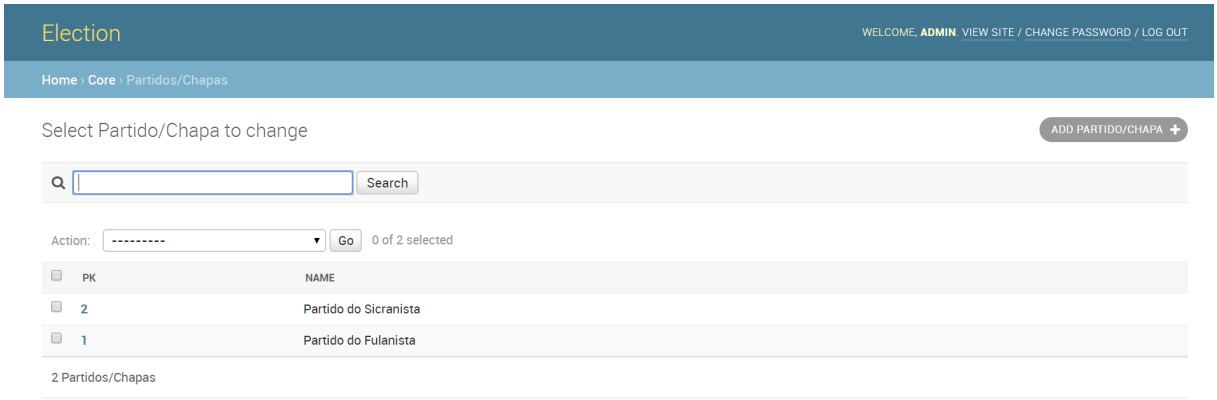
A gerencia de candidatos e partidos é autorizada somente aos usuários com permissão de administradores. As imagens 5 e 6 demonstram os painéis de gerenciamento dos candidatos e partidos respectivamente.

Ilustração 5 – Painel gerencial dos candidatos



FONTE: Elaborado pelo autor

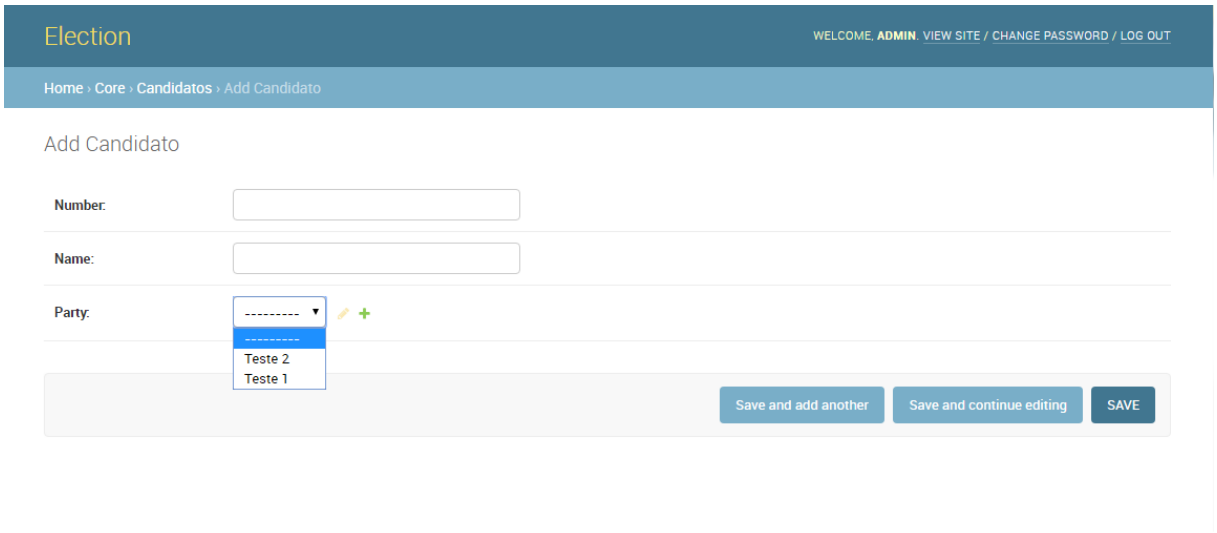
Ilustração 6 – Painel gerencial dos partidos



FONTE: Elaborado pelo autor

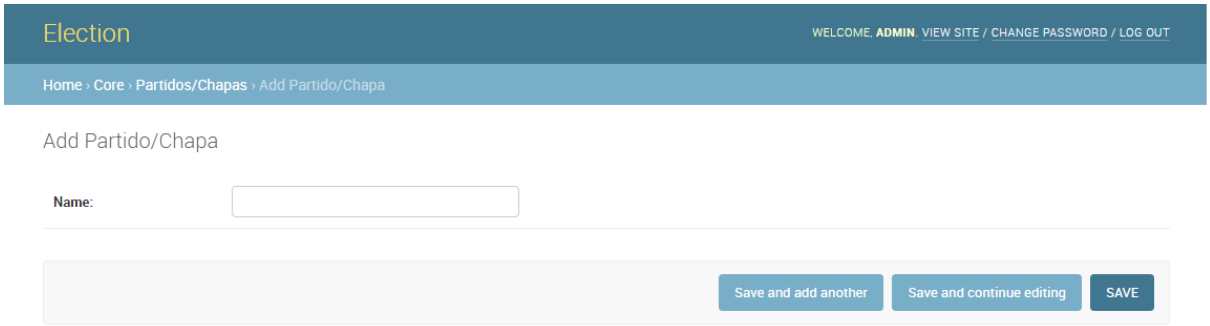
A criação de um candidato só é possível com a atribuição de um partido a ele, logo, o candidato não poderá ser criado sem o registro de partidos antecipadamente. As imagens 7 e 8 demonstram a criação de candidatos e partidos respectivamente.

Ilustração 7 – Painel de criação de candidatos



FONTE: Elaborado pelo autor

Ilustração 8 – Painel de criação de candidatos



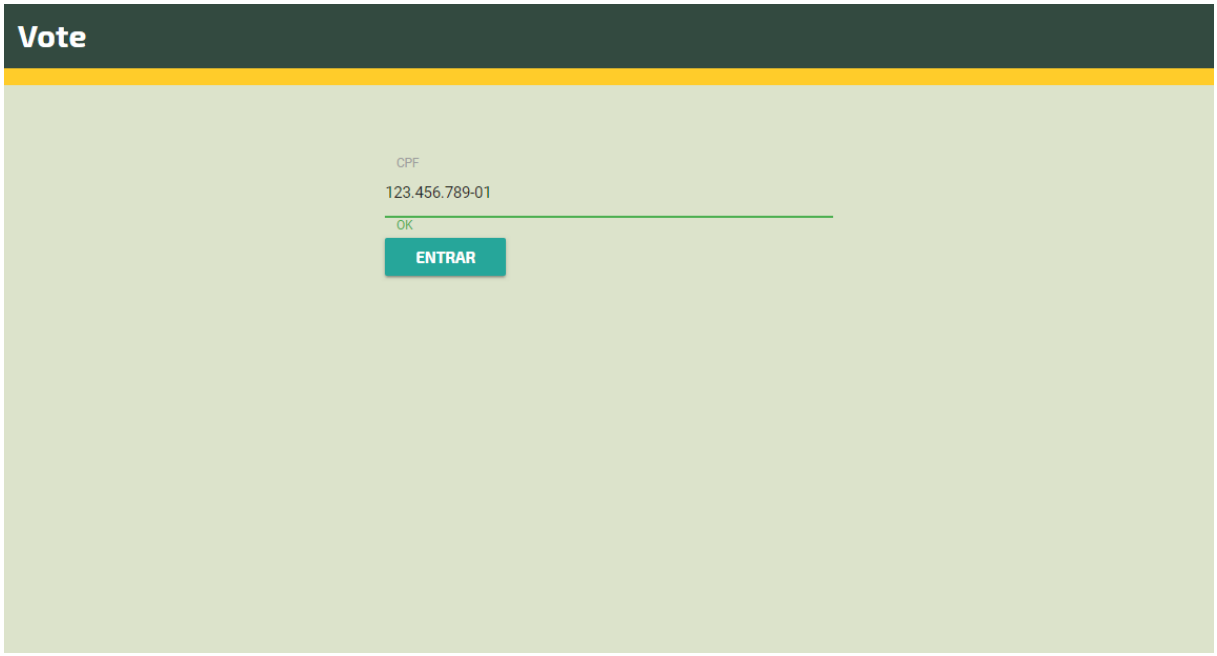
FONTE: Elaborado pelo autor

4.6 MÓDULO PRINCIPAL

O módulo principal é onde ocorre todo o fluxo do processo de votação descrito na seção 4.2.

A imagem 9 ilustra a autenticação do usuário. O numero de identificação preterido pelo protótipo foi o CPF. Ao introduzir o CPF, é analisado se não há registros de utilização do mesmo, caso não conste nenhum registro, o usuário é redirecionado para tela de votação, caso contrario surge um alerta assinalando que o CPF ja fora utilizado.

Ilustração 9 – Tela de autenticação do usuário

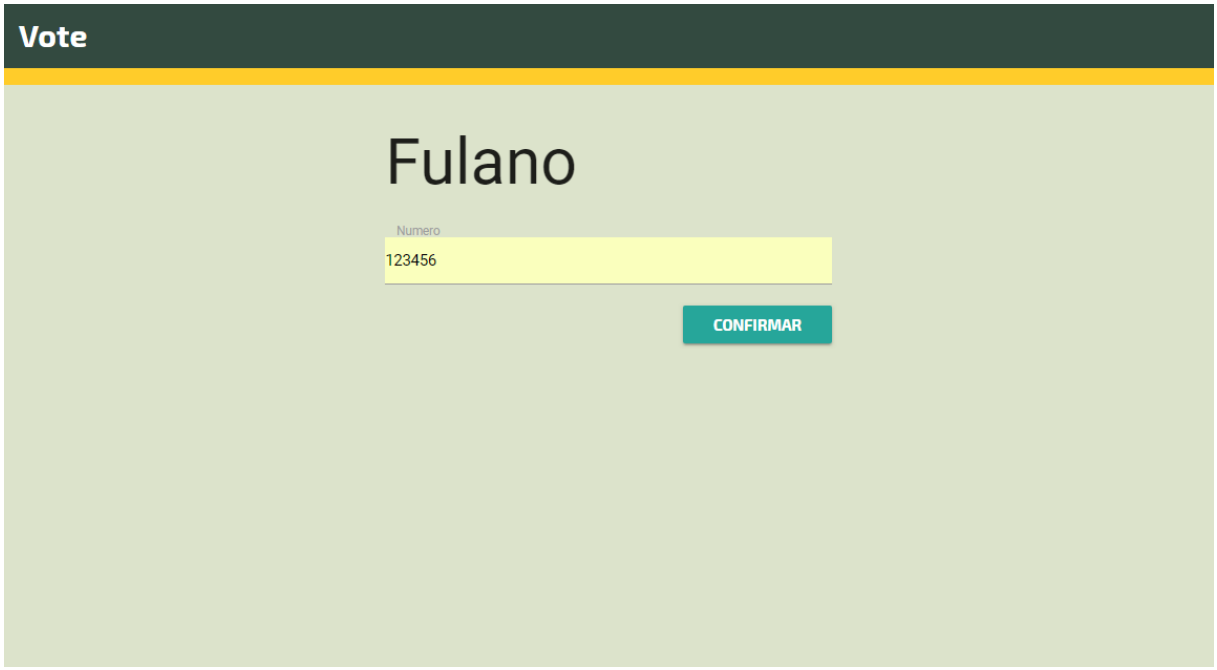


FONTE: Elaborado pelo autor

Na tela de votação apresentada na imagem 10, o usuário introduz o numero de cadastro do candidato. O nome do candidato é exibido se o numero inserido coincidir com o número de cadastro do mesmo, caso o numero inserido não coincidir com nenhum número de cadastro dos candidatos, é exibido o nome "NULO"na tela.

Ao clicar no botão confirmar, o voto do usuário é registrado no blockchain através do uso da aplicação do Bigchain, logo em seguida o CPF inserido na autenticação é registrado como ja utilizado. Ao término deste processo, o sistema é redirecionado para tela de resultados exibido na imagem 11, finalizando o fluxo de votação.

Ilustração 10 – Tela de votação



FONTE: Elaborado pelo autor

Ilustração 11 – Tela de resultados

FONTE: Elaborado pelo autor

Os votos computados na imagem 11 são resgatados diretamente do blockchain, onde a busca é feita pela chave pública de cada candidato, mitigando a possibilidade de erros, tendo em vista que a chave pública é única para cada ator do blockchain.

4.6.1 Benefícios das Aplicações Blockchain

Os benefícios do blockchain perante outras aplicações é algo a se destacar. Os dados do blockchain são mais difíceis de alterar (ou excluir) do que o normal, tornando-o mais seguro. Dados de blockchain podem ser tornados imutáveis de várias maneiras [BigchainDB Contributors Revision, 2018]:

1. Nenhuma API(*Aplication Program Interface*) para alterar ou excluir dados. O software Blockchain geralmente não exibe APIs para alterar ou excluir os dados armazenados. Isso não impede que alterações ou exclusões ocorram de outras maneiras. é apenas uma linha de defesa;

2. Replicação. Todos os dados são replicados (copiados) para vários locais diferentes. Quanto maior o fator de replicação, mais difícil será alterar ou excluir todas as réplicas;

3. Vigias internos. Todos os nós monitoram todas as alterações, caso ocorra alguma alteração não permitida, as medidas apropriadas podem ser executadas;

4. Vigias externos. Um consórcio pode optar por ter terceiros confiáveis para monitorar e auditar seus dados, procurando por irregularidades. Para um consórcio com dados publicamente legíveis, o público pode atuar como auditor;

5. As assinaturas criptográficas são frequentemente usadas como uma maneira de verificar se as mensagens (transações) foram adulteradas no trafego e como forma de verificar quem assinou as mensagens;

6. Forte segurança. Os proprietários de nós podem adotar e impor políticas de seguranças pessoais, consequentemente incrementando a segurança do blockchain.

7. Diversidade de nós. A diversidade faz com que nenhuma coisa (por exemplo, desastres naturais ou falhas no sistema operacional) comprometa suficientemente o blockchain.

4.7 UTILIZANDO OUTRO MODO DE ARMAZENAMENTO

Ao utilizar outro modo de armazenamento para as informações cruciais, como fremework Django em conjunto com o Banco de Dados PostgreSQL, nota-se algumas possibilidades mais graves de adulteração, como por exemplo, o Django oferece uma gama de comandos para administrar os dados inseridos no banco, possibilitando qualquer pessoa com acesso ao servidor aterá-los. Na imagem 12 é demonstrado um trecho de código com um conjunto de comandos que adulteram os votos caso seja executado no servidor.

Ilustração 12 – Código de adulteração de votos

```
1  from core.models import *
2
3
4  fulano = Candidate.objects.get(name="Fulano") #Buscando o candidato fulano na base de dados
5
6  for voto in Vote.objects.all(): #Percorrendo todos os Votos
7      voto.candidate = fulano #Atribuindo os votos a fulando
8      voto.save() #Salvando a alteração na base de dados
```

FONTE: Elaborado pelo autor

Como demonstrado na imagem 12, a linha 4 do código é responsável por recuperar o candidato "Fulano"da base de dados; a linha 6 executa um ciclo que resgata os votos da base de dados e, para cada voto resgatado, é executado as linhas 7 e 8; as linhas 7 e 8 são responsáveis pela atribuição dos votos ao candidato resgatado na linha 4 e o armazenamento das alterações respectivamente.

A ilustração 13 exibe os resultados da adulteração, os votos pertencentes ao candidato "Sicrano", que foram demonstrados na ilustração 11, foram atribuídos ao candidato "Fulano".

Ilustração 13 – Votos no Banco PostgreSQL

Vote

Candidato	Partido	Votos
Fulano	Partido do Fulanista	3
Sicrano	Partido do Sicranista	0

FONTE: Elaborado pelo autor

A replicação dos dados pelos usuários dos nós da rede blockchain, seria uma das maneiras de excluir a possibilidade de um indivíduo alterar os votos em uma invasão ao servidor, pois os outros nós, em posse dos dados corretos, acusariam as alterações ilegais registradas e corrigiriam os dados inválidos.

5 CONCLUSÃO

A comunidade blockchain frequentemente descreve blockchain como "imutável". Se interpretarmos essa palavra literalmente, isso significa que os dados de blockchain são imutáveis ou permanentes, o que é um absurdo. Os dados podem ser alterados. Por exemplo, uma praga pode levar a humanidade à extinção; os dados seriam corrompidos ao longo do tempo devido a danos causados pela água, ao ruído térmico e ao aumento geral da entropia. Portanto, no contexto de blockchain, interpretamos a palavra "imutável"como praticamente imutável, para todos os efeitos. (Os linguistas diriam que a palavra "imutável"é um termo de arte na comunidade blockchain [BigchainDB Contributors Revision, 2018].

Este trabalho apresentou um protótipo de sistema de eleição baseado em blockchain, uma tecnologia emergente caracterizada por ter uma arquitetura capaz de ofertar os princípios básicos da segurança da informação(Confidencialidade, Integridade, Autenticidade e Disponibilidade) de forma eficiente. O protótipo teve por objetivo a exploração do serviço blockchain e para melhor aplicação da tecnologia, foi utilizado o Bigchain, um serviço de código aberto especializado em blockchain.

Por fim, este protótipo foi concebido para proporcionar uma experiencia de aprendizado sobre uma nova tecnologia, explorando os conceitos e propriedades computacionais que foram utilizados na sua construção, além de prover a oportunidade de utilizar vários conhecimentos adquiridos durante o curso de Análise e Desenvolvimento de Sistemas. O código do sistema é disponibilizado na plataforma GitHub, possibilitando a auditoria do sistema a qualquer indivíduo.

REFERÊNCIAS

ANNAN, K. A. *How information technology poses a threat to democracy*. 2018. Disponível em: <https://www.japantimes.co.jp/opinion/2018/02/19/commentary/world-commentary/information-technology-poses-threat-democracy/#.W1N389VKjIV>.

ARANHA, D. F. et al. Vulnerabilidades no software da urna eletrônica brasileira. Universidade de Brasília - UnB, 2013.

BigchainDB. 2018. Disponível em: <https://www.bigchaindb.com>.

BigchainDB Contributors Revision. 2018. Disponível em: <https://http://docs.bigchaindb.com>.

Blockchain Technologies Corporation. 2018. Disponível em: <https://blockchaintechcorp.com/>.

CROSBY, M. et al. Blockchain technology: Beyond bitcoin. *AIR Applied Innovation Review*, 2016.

FOLLOWMYVOTE. *Blockchain Technology in Online Voting*. 2016. Disponível em: <https://followmyvote.com/online-voting-technology/blockchain-technology/>.

KIRBY, K.; MASI, A.; MAYMI, F. Votebook: A proposal for a blockchain-based electronic voting system. New York University, 2016.

MARTINS, H. *Fake news e controle na internet são desafios para as eleições de 2018*. 2017. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2017-12/fake-news-censura-e-controle-na-internet-desafios-para-eleicoes-de-2018>.

MongoDB. 2018. Disponível em: <https://www.mongodb.com/>.

OLIVEIRA, R. R. Criptografia simétrica e assimétrica: os principais algoritmos de cifragem. Revista Seguranca Digital, 2012.

PIRES, T. P. Tecnologia blockchain e suas aplicações para provimento de transparência em transações eletrônicas. Faculdade de Tecnologia da UNB, 2016.

Portal da Transparência. 2004. Disponível em: <http://www.portaltransparencia.gov.br/>.

ROHR, A. *Conheça vulnerabilidades em sistemas de voto eletrônico*. 2012. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/conheca-vulnerabilidades-em-sistemas-de-voto-eletronico.html>.

VOTEWATCHER. *Cutting Edge Blockchain Voting System*. 2016. Disponível em: <http://votewatcher.com/#voting>.

ZHENG, Z. et al. An overview of blockchain technology: Architecture, consensus, and future trends. IEEE 6th International Congress on Big Data, 2017.