



UNIVERSIDADE
E D U A R D O
MONDLANE

FACULDADE DE CIÊNCIAS
Departamento de Matemática e Informática

Trabalho de Licenciatura em
Informática

**Aplicação da Tecnologia Blockchain Em Sistema
De Votação Online**

**Caso de Estudo: Núcleo Dos Estudantes Da
Faculdade de Ciências - UEM**

Autor: Amal Vitorino Mbussila

Maputo, 15 de Dezembro de 2025



UNIVERSIDADE
E D U A R D O
MONDLANE

FACULDADE DE CIÊNCIAS
Departamento de Matemática e Informática

Trabalho de Licenciatura em
Informática

**Aplicação Tecnologia Blockchain Em Sistema De
Votação Online**

Autor: Amal Vitorino Mbussila

Supervisor: Mestre, Juvêncio Manjate, UEM

Co-supervisor(es): dr, Ernesto Cumbe, UEM

Maputo, 15 de Dezembro de 2025

Dedicatória

Dedico este trabalho às minhas mães, Dianora Tonela Vilanculo, Virginia Tonela Vilanculo e Helena Tonela Vilanculo, que, com esforço incansável e amor incondicional, têm lutado desde o início para que eu pudesse ter uma educação de qualidade. Cada conquista minha é reflexo da dedicação e sacrifício de vocês, e por isso, este trabalho é, em grande parte, de vocês também.

Declaração de Honra

Declaro por minha honra que o presente Trabalho de Licenciatura é resultado da minha investigação e que o processo foi concebido para ser submetido apenas para a obtenção do grau de Licenciado em Informática na faculdade de Ciências da Universidade Eduardo Mondlane.

Maputo, 15 de Dezembro de 2025

(Amal Vitorino Mbussila)

Agradecimentos

Em primeiro lugar, agradeço a Deus pelo dom da vida e por todas as bênçãos que tem me proporcionado ao longo da minha trajetória. Sem Sua graça e proctecção, este trabalho e todas as minhas conquistas não seriam possíveis.

Agradeço também à minha instituição de ensino, a UEM, por me proporcionar a oportunidade de adquirir conhecimentos e me desenvolver como profissional. Em especial, expresso minha gratidão DMI e a todos os docentes, que desempenharam um papel fundamental na minha formação acadêmica.

Meu sincero agradecimento vai ao meu supervisor, Juvêncio Manjate, pelo apoio, orientação e paciência ao longo deste trabalho. A sua experiência e dedicação foram essenciais para a realização deste projecto.

Por fim, agradeço a todos que, directa ou indirectamente, me apoiaram nesta jornada acadêmica, desde familiares, amigos e colegas. Cada palavra de incentivo e gesto de apoio contribuiu para que eu pudesse chegar até aqui.

Resumo

O presente trabalho aborda o problema da falta de segurança e integridade nos processos de votação, especialmente em contextos onde as fraudes e manipulações podem comprometer a credibilidade dos resultados eleitorais. A motivação por trás do estudo reside na crescente demanda por métodos eleitorais mais transparentes e confiáveis, principalmente no âmbito de organizações académicas e pequenas instituições, onde a confiança no processo é vital.

O objectivo principal deste trabalho é o desenvolvimento de um protótipo de sistema de votação *online* utilizando a tecnologia *Blockchain*, que assegure a imutabilidade dos votos, a transparência do processo e a confiança dos eleitores. Para atingir este objectivo, foi utilizado o *framework* Laravel para o desenvolvimento do protótipo e a *Blockchain* para o armazenamento seguro dos votos, garantindo que eles permaneçam invioláveis após a submissão.

A metodologia adoptada incluiu a criação de um sistema que faz a gestão de todo o processo eleitoral, desde o registo de candidatos, passando pela votação propriamente dita, até a contagem e verificação dos votos. O sistema integra a *Blockchain* como um meio de garantir que cada voto seja único e permanentemente registado, sem possibilidade de manipulação ou exclusão.

Como resultado, o protótipo demonstrou que a tecnologia *Blockchain* pode ser efectivamente aplicada em sistemas de votação *online*, proporcionando um nível elevado de segurança e integridade dos dados eleitorais. As implicações deste estudo sugerem que a adopção de *Blockchain* em processos eleitorais, especialmente em pequenos e médios contextos, pode representar um avanço significativo na garantia de eleições justas e transparentes.

Palavras-chave: *Blockchain*, votação *online*, segurança eleitoral, eleições.

Abstract

The present work addresses the problem of the lack of security and integrity in voting processes, especially in contexts where fraud and manipulation can compromise the credibility of electoral results. The motivation behind this study lies in the growing demand for more transparent and reliable electoral methods, particularly within academic organizations and small institutions, where trust in the process is crucial.

The main objective of this work is to develop a prototype of an *online* voting system using Blockchain technology, which ensures the immutability of votes, the transparency of the process, and the trust of voters. To achieve this objective, the Laravel framework was used for the development of the prototype, and Blockchain was employed for the secure storage of votes, ensuring that they remain inviolable after submission.

The methodology adopted included the creation of a system that manages the entire electoral process, from the registration of voters and candidates, through the actual voting process, to the counting and verification of votes. The system integrates Blockchain as a means of ensuring that each vote is unique and permanently recorded, without the possibility of manipulation or deletion.

As a result, the prototype demonstrated that Blockchain technology can be effectively applied to *online* voting systems, providing a high level of security and data integrity in the electoral process. The implications of this study suggest that the adoption of Blockchain in electoral processes, especially in small and medium-sized contexts, can represent a significant advancement in ensuring fair and transparent elections.

Keywords: Blockchain, *online* voting, electoral security, elections.

Abreviaturas

API – *Application Programming Interface*

DMI – Departamento de Matemática e Informática

FC – Faculdade de Ciências

HTML - *Hypertext Markup Language*

HTTP – *HyperText Transfer Protocol*

IP – *Internet Protocol*

JSON – *JavaScript Object Notation*

NEDMI - Núcleo dos Estudantes do Departamento de Matemática e Informática

NEFAC-UEM – Núcleo dos Estudantes da Faculdade de Ciências da Universidade Eduardo Mondlane

PHP – *Hypertext Preprocessor*

SDK – *Software Development Kit*

SI - Sistema de Informação

SQL – *Structured Query Language*

TCC – Trabalho de Conclusão de Curso

TIC - Tecnologia de informação e comunicação

UEM – Universidade Eduardo Mondlane

UML - *Unified Modeling Language*

XML – *Extensible Markup Language*

Índice

Dedicatória.....	i
Declaração de Honra.....	ii
Agradecimentos.....	iii
Resumo.....	iv
Abstract	v
Abreviaturas.....	vi
Lista de Figuras.....	x
Lista de Tabelas.....	xi
Introdução.....	1
1.1. Contextualização	1
1.2. Definição do problema.....	2
1.3. Objectivos	3
1.3.1. Objectivo Geral:.....	3
1.3.2. Objectivos Específicos:.....	3
1.4. Motivação	3
1.5. Estrutura do trabalho.....	4
Revisão de Literatura.....	5
2.1. UEM & FC.....	5
2.2. NEFAC e sua Estrutura Organizacional	6
2.1.1. História dos Sistemas de Votação	7
2.1.2. Desafios dos Processos Eleitorais	8
2.1.3. Transição para Sistemas de Votação Eletrónica.....	8
2.1.4. Fraudes e Segurança em Processos Eleitorais	8
2.1.5. Vantagens e Desvantagens dos Sistemas de Votação Eletrónica	9
2.1.6. Processos Eleitorais em Contextos Académicos.....	9

2.2	Criptografia	10
2.3	<i>Blockchain</i> e Sistemas de Votação Eletrónica	11
2.3.1.	Como funciona o <i>Blockchain</i>	12
2.3.2.	Vantagens dos Sistemas de Votação Eletrónica com <i>Blockchain</i>	13
2.3.3.	Desafios e Limitações dos Sistemas de Votação Eletrónica com <i>Blockchain</i>	13
2.3.4.	Aplicações da <i>Blockchain</i> em Eleições Académicas e Institucionais	14
2.3.5.	Futuro dos Sistemas de Votação com <i>Blockchain</i>	15
	Material e Métodos	16
3.1	Metodologia de pesquisa	16
3.1.1.	Pesquisa Quanto à Natureza	16
3.1.2.	Pesquisa Quanto à Forma de Abordagem	16
3.1.3.	Técnicas de Recolha de Dados	17
3.2	Metodologia de desenvolvimento	17
3.2.1.	Ferramentas de Desenvolvimento.....	18
	Caso de Estudo	21
4.1	Organização Estudada: NEFAC-UEM	21
4.2	Modelo Actual	21
4.2.1.	Descrição do Fluxo de Informação no Modelo Actual	21
4.3.	Modelo proposto	22
4.3.1.	Principais características do modelo proposto	22
4.3.2.	Fluxo de Informação no Sistema Proposto	23
4.3.3.	Requisitos do sistema proposto	23
4.3.3.1.	Requisitos Funcionais.....	24
4.3.3.2.	Requisitos não funcionais	25
4.3.3.3.	Funcionalidades Adicionais (opcional)	26
4.4.	Modelação do modelo Proposto.....	26
4.4.1.	Diagrama de Classes	26
4.4.2.	Diagramas de caso de uso.....	27

4.4.2.1.	Diagrama de Caso de Uso Para Registo de Usuários	27
4.4.2.2.	Diagrama de Caso de Uso Para Configuração da Eleição	28
4.4.2.3.	Diagrama De Caso De Uso Para o Processo De Votação	29
4.4.2.4.	Diagrama de Caso de Uso para Visualização de resultados	30
4.4.3.	Diagramas de Sequência de Eventos.....	31
4.4.3.1.	Diagrama de sequência de eventos para o registo de Administradores.....	32
4.4.3.2.	Diagrama de sequência de eventos para a configuração de uma eleição.....	32
4.4.3.3.	Diagrama de sequência de eventos para o processo de votação.....	33
4.4.3.4.	Diagrama de sequência de eventos para a consulta dos resultados das eleições	33
Conclusões e Recomendações		34
5.1	Conclusão	34
5.1.1.	Implicações da pesquisa.....	35
5.2	Recomendações para futuras implementações	35
5.2.1.	Rede <i>Blockchain</i> Distribuída.....	35
Referências Bibliográficas		36
Anexos.....		38
Anexo 1.....		38
Anexo 2:.....		39
Apêndices.....		41

Lista de Figuras

Figura 1: Organograma da Faculdade de Ciências da Universidade Eduardo Mondlane	6
Figura 2: Representação da forma de votação tradicional no Brasil, conforme descrito no artigo "O Voto no Brasil"	7
Figura 3: https://www.universidadejava.com.br/outros/criptografia-simetrica/	10
Figura 4: Exemplo de blockchain (learn.microsoft).....	11
Figura 5: Funcionamento da metodologia de desenvolvimento Scrum, Somemerville (2011)	18
Figura 6: Modelo actual, Autor (2024).....	22
Figura 7: Modelo proposto, Autor (2024).....	23
Figura 8: Diagrama de Entidade e Relacionamento DER. Autor (2024)	27
Figura 9: Diagrama de Caso de Uso Para Registo de Usuários. Autor (2024).....	28
Figura 10: Diagrama de Caso de Uso Para Configuração da Eleição. Autor (2024).....	29
Figura 11: Diagrama De Caso De Uso Para o Processo De Votação. Autor (2024).....	30
Figura 12: diagrama de Caso de Uso para Visualização de resultados. Autor (2024).	31
Figura 13: Diagrama de sequência de eventos para o registo de Administradores e Eleitores, Autor (2024)	32
Figura 14: Diagrama de sequência de eventos para a configuração de uma eleição, Autor (2024)	32
Figura 15: Diagrama de sequência de eventos para o processo de votação, Autor (2024)	33
Figura 16: Diagrama de sequência de eventos para a consulta dos resultados das eleições, Autor (2024)	33
Figura 17: credencial.....	38
Figura 18: questionário part1. Autor (2024).....	39
Figura 19: questionário part 2. Autor (2024).....	40
Figura 20: pagina de login no mobile. Autor (2024).....	41
Figura 21: Pagina de login no computador. Autor (2024)	42
Figura 22: tela de registo do candidato. Autor (2024)	42
Figura 23: Tela para registo e configuração da eleição. Autor (2024)	43
Figura 24: Tela para visualização de eleições para voto. Autor (2024)	43
Figura 25: tela para votar no candidato escolhido. Autor (2024).....	44
Figura 26: Tela para seleccionar a eleição para ver resultados. Autor (2024).....	44
Figura 27: Tela para Visualizar os resultados. Autor (2024)	45

Lista de Tabelas

Tabela 1: Requisitos funcionais. Autor (2024).....	24
Tabela 2: Requisitos não funcionais. Autor (2024)	25
Tabela 3: Funcionalidades adicionais (2024)	26
Tabela 4: Diagrama de Caso de Uso Para Registo de Usuários (2024).....	27
Tabela 5: Diagrama de Caso de Uso Para Configuração da Eleição. Autor (2024)	28
Tabela 6: Diagrama De Caso De Uso Para o Processo De Votação. Autor (2024)	29
Tabela 8: Diagrama de Caso de Uso para visualização resultados. Autor (2024).....	30

Introdução

Neste capítulo, são abordados a contextualização, a definição do problema, os objectivos, a motivação e a estrutura do trabalho, com o intuito de proporcionar uma visão clara e detalhada sobre o tema principal da pesquisa. O capítulo oferece um panorama geral do contexto em que o problema está inserido, explicando os desafios e questões que justificam a sua investigação. Além disso, os objectivos são delineados para esclarecer as metas que o estudo pretende alcançar, enquanto a motivação destaca a importância e relevância do tema, tanto em termos práticos quanto académicos. Por fim, a estrutura do trabalho é apresentada, orientando o leitor sobre a organização dos capítulos e o fluxo lógico da argumentação ao longo da monografia.

1.1. Contextualização

Nos últimos anos, a uso de tecnologias digitais em processos eleitorais tem ganhado destaque devido à necessidade de sistemas mais seguros, transparentes e acessíveis. Entre essas tecnologias, a *Blockchain* se destaca por sua capacidade de garantir a integridade de dados e a transparência das transacções [Zheng et al. 2018], características essenciais para a realização de eleições justas e confiáveis.

Com o crescimento do uso da tecnologia na modernização de processos tradicionais, as instituições de ensino superior não estão isentas de explorar novas abordagens para melhorar a eficiência e a confiabilidade de seus sistemas. Sistemas de votação *online* surgem como uma alternativa interessante para melhorar ou até mesmo substituir o método tradicional de votação em papel, permitindo maior comodidade, maior participação dos eleitores e, potencialmente, maior segurança. Contudo, tais sistemas enfrentam desafios significativos em termos de confiança dos eleitores, integridade do processo eleitoral e protecção contra fraudes.

O NEFC-UEM desempenha um papel essencial na organização e representação dos interesses dos estudantes, promovendo actividades que fortalecem o relacionamento entre os estudantes, além de interagir com a administração da faculdade e representar os estudantes em órgãos decisórios. A eleição para a presidência do Núcleo é um momento crítico, pois define a liderança que guiará as iniciativas estudantis e representará o corpo discente nas instâncias superiores. No entanto, como qualquer processo eleitoral, ele enfrenta desafios relacionados à transparência, segurança e confiança dos eleitores.

Neste contexto, a tecnologia *Blockchain* vem sendo amplamente discutida como uma solução viável para aumentar a segurança e a transparência em sistemas de votação digital. Ao contrário de bases de dados centralizadas, o *Blockchain* opera de forma descentralizada, garantindo que cada transação ou voto, neste caso seja registada de maneira imutável e transparente para todos os participantes. As propriedades criptográficas do *Blockchain* também oferecem verificabilidade e auditabilidade, o que reduz significativamente a possibilidade de fraudes eleitorais, corrupção de votos ou manipulação dos resultados.

Portanto, a proposta deste trabalho é desenvolver um protótipo de um sistema de votação *online* utilizando *Blockchain*, aplicado ao processo eleitoral do NEFAC-UEM. Este sistema tem como objectivo garantir que os votos sejam registados de forma segura e transparente, permitindo auditoria e reduzindo as chances de irregularidades no processo. A partir deste estudo de caso, pretende-se explorar como a tecnologia pode ser aplicada em um contexto académico para aprimorar a governança estudantil, elevando o padrão de confiança e participação nas eleições do núcleo.

A escolha do NEFAC como estudo de caso baseia-se na relevância da faculdade dentro da UEM, por ser uma das maiores e mais influentes, com um número significativo de estudantes distribuídos por vários cursos e departamentos. Essa diversidade torna o processo eleitoral mais complexo, e um sistema de votação eficiente e seguro pode proporcionar benefícios claros em termos de logística, confiabilidade e engajamento dos estudantes. Além disso, ao focar no núcleo de uma faculdade inteira, a pesquisa tem a possibilidade de ser replicada em outras faculdades ou instituições, ampliando o impacto do trabalho.

1.2. Definição do problema

Embora os sistemas de votação *online* ofereçam inúmeras vantagens em termos de conveniência e acessibilidade, a segurança e a integridade dos votos continuam sendo questões críticas que precisam ser abordadas. Muitos sistemas de votação tradicionais enfrentam desafios significativos, como fraudes eleitorais, manipulação de resultados e falta de transparência, o que compromete a confiança dos eleitores no processo.

Numa eleição tradicional, por vezes para garantir a segurança do voto usam-se técnicas que exigem o envolvimento de forças armadas para impedir a intervenção de agentes maliciosos no processo, pois o perigo está sempre a espreita. Assim, surge a questão: **como a tecnologia *Blockchain* pode ser aplicada de maneira eficaz em sistemas de votação *online*, de modo a garantir a segurança, transparência e integridade no processo eleitoral, onde o voto circula de forma digital e não física??**

O uso de *Blockchain* poderia mitigar os problemas enfrentados pelos sistemas tradicionais, garantindo que os votos sejam imutáveis, auditáveis e acessíveis de forma transparente, promovendo maior confiança no processo e minimizando os riscos de fraudes e manipulações.

Essa pesquisa visa investigar como a aplicação de *Blockchain* poderia transformar o cenário actual de votação no NEFAC-UEM, criando um sistema mais seguro, transparente e que possa ser adaptado a outras faculdades ou instituições educacionais, contribuindo para a modernização dos processos eleitorais dentro do ambiente universitário.

1.3. Objectivos

1.3.1. Objectivo Geral:

Desenvolver um de protótipo de sistema de votação *online* e aplicar a tecnologia *Blockchain*, de modo a garantir a segurança, integridade e transparência dos votos no processo eleitoral.

1.3.2. Objectivos Específicos:

- Analisar o processo eleitoral actual do NEFAC-UEM;
- Identificar as limitações e vulnerabilidades do sistema actual;
- Avaliar o funcionamento da tecnologia *blockchain* e identificar como suas características podem ser aplicadas a sistemas de votação;
- Modelar o sistema de votação *online* com aplicação da *blockchain*
- Desenvolver um sistema com base no modelo proposto.

1.4. Motivação

A motivação para o desenvolvimento deste trabalho vem da necessidade de garantir que os processos eleitorais sejam confiáveis e transparentes, especialmente em ambientes académicos como o NEFAC-UEM. A escolha de bons representantes estudantis é importante para a organização e gestão da faculdade, e um sistema de votação seguro ajuda a garantir que essa escolha seja justa. Além disso, o avanço da tecnologia *Blockchain* apresenta uma oportunidade única para modernizar e otimizar esses processos, proporcionando maior segurança e confiança por parte dos eleitores. O desenvolvimento de um sistema de votação *online* para o NEFAC-UEM não apenas contribuirá para a integridade das eleições, mas também servirá como um modelo replicável em outras instituições e organizações.

1.5. Estrutura do trabalho

O presente trabalho está dividido em cinco (5) capítulos que estão organizados da seguinte forma:

- **Introdução:** Neste capítulo, são abordados a contextualização, a definição do problema, os objectivos, a motivação e a estrutura do trabalho, com o intuito de proporcionar uma visão clara e detalhada sobre o tema principal da pesquisa. O capítulo oferece um panorama geral do contexto em que o problema está inserido, explicando os desafios e questões que justificam a sua investigação.
- **Revisão da Literatura:** Neste capítulo, serão abordados conceitos fundamentais para a compreensão do desenvolvimento de sistemas de votação *online* baseados em *Blockchain*. A revisão de literatura explorará temas como a estrutura e funcionamento dos núcleos de estudantes, processos eleitorais em ambientes académicos, e as vantagens e desafios da adopção de tecnologias emergentes, com ênfase especial na aplicação de *Blockchain*. Por fim, serão discutidos sistemas de votação tradicionais e *online*, seus problemas e limitações, e como a tecnologia *Blockchain* pode revolucionar esse campo.
- **Materiais e Métodos:** Neste capítulo, serão detalhados os materiais e métodos utilizados para conduzir esta pesquisa. Será descrita a metodologia adotada para o desenvolvimento do protótipo do sistema de votação *online* baseado em *Blockchain*, bem como os métodos de recolha e análise de dados que fundamentaram o trabalho. Este capítulo também aborda as ferramentas, linguagens de programação e tecnologias selecionadas para o desenvolvimento do protótipo, além de justificar suas escolhas com base na revisão de literatura.
- **Caso de estudo (Modelo actual e Modelo proposto):** Neste capítulo, serão descritos o modelo actual de eleição do presidente do núcleo, identificando as limitações e desafios. Posteriormente, será proposto um novo modelo baseado em um sistema de votação online utilizando a tecnologia *Blockchain*, detalhando as melhorias esperadas em termos de segurança, transparência e eficiência no processo eleitoral.
- **Conclusão e Recomendações:** Neste capítulo, apresentamos as conclusões obtidas a partir do desenvolvimento do protótipo de um sistema de votação *online* baseado em tecnologia *Blockchain*. Serão discutidos os principais resultados e as implicações do projecto, além de sugestões para futuras implementações e melhorias

Revisão de Literatura

Neste capítulo, serão abordados conceitos fundamentais para a compreensão do desenvolvimento de sistemas de votação *online* baseados em *Blockchain*. A revisão de literatura explorará temas como a estrutura e funcionamento dos núcleos de estudantes, processos eleitorais em ambientes acadêmicos, e as vantagens e desafios da adoção de tecnologias emergentes, com ênfase especial na aplicação de *Blockchain*. Por fim, serão discutidos sistemas de votação tradicionais e *online*, seus problemas e limitações, e como a tecnologia *Blockchain* pode revolucionar esse campo.

A pesquisa bibliográfica é desenvolvida através de material já elaborado apoiando-se em fontes documentais ou bibliográficas, em quase todos os estudos é imprescindível o uso de pesquisa bibliográfica, principalmente para caso de aplicação da pesquisa exploratória na qual se tem como objectivo proporcionar maior familiaridade com o tema tendo em vista torná-lo mais explícito, ou seja, garantir que haja esclarecimento ou modificação das ideias para evitar uma possível duplicação de esforços, assumindo que em algum momento tenha se feito uma pesquisa igual ou similar.

2.1. UEM & FC

Segundo o portal da FC (ciencias.uem.mz) A Universidade Eduardo Mondlane foi fundada no dia 21 de agosto de 1962, sob a designação de Estudos Gerais Universitários de Moçambique, e em 1968 ascende à categoria de Universidade, sendo então designada Universidade de Lourenço Marques (ULM). Em 1980 cria-se a Faculdade de Ciências (FC) integrando as Faculdades de Física, Química e Geologia, que se encontravam no mesmo Campus Universitário, e estas passam a ser designadas de Departamentos Acadêmicos da FC. Cinco anos mais tarde, em 1985, a FC cria o Departamento de Ciências Básicas da Faculdade de Ciências “BUSCEP”.

A FC da UEM tem como missão promover o desenvolvimento do ensino, pesquisa e extensão em diversas áreas das Ciências Naturais, Puras e Aplicadas. O departamento destaca-se por sua capacidade de formar profissionais qualificados para enfrentar os desafios da sociedade moderna, nas áreas de Ciências Biológicas, Físicas, Geológicas, Matemáticas e Químicas. Além disso, busca ser um ponto de

referência na produção e disseminação de conhecimento científico, contribuindo para a construção de uma sociedade mais próspera por meio da inovação e excelência acadêmica.

Com base em valores fundamentais como rigor, competência, criatividade e trabalho em equipe, a Faculdade de Ciências promove uma cultura de colaboração e liberdade acadêmica, essencial para o desenvolvimento do pensamento científico. A faculdade também valoriza a internacionalização e parcerias, incentivando a cooperação com instituições de pesquisa e o sector productivo, tanto nacional quanto internacionalmente. A visão da FC é consolidar-se como uma referência na promoção de excelência e inovação, garantindo que sua atuação tenha impacto direto no desenvolvimento e na melhoria da sociedade. Na figura1, é apresentado o organograma da FC.

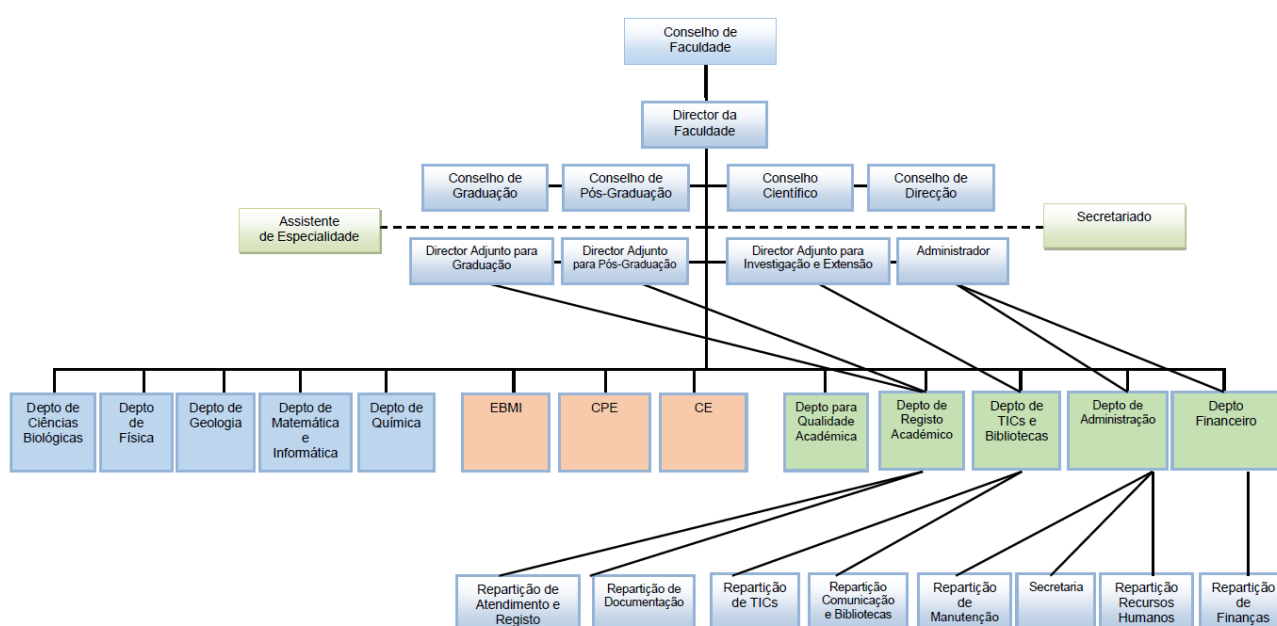


Figura 1: Organograma da Faculdade de Ciências da Universidade Eduardo Mondlane (<https://ciencias.uem.mz/>)

2.2. NEFAC e sua Estrutura Organizacional

NEFAC-UEM é uma organização que tem como objectivo principal representar e defender os interesses dos estudantes da faculdade. Sua estrutura é composta por representantes de diferentes departamentos, como Química, Matemática, Informática, entre outros. Segundo um dos respondentes (2024), o NEFAC "é uma pequena organização que tem como objectivos melhorar a comunicação da comunidade académica de ciências, zelar pelas melhores condições para os estudantes, e manter a comunidade académica unida" (Questionário, 2024).

De acordo com o actual presidente do NEDMI, suas principais funções incluem "organizar actividades académicas e culturais, promover eventos que beneficiem os estudantes, servir de ponte entre os

estudantes e o departamento, além de apoiar o desenvolvimento académico e social de todos" (Questionário, 2024). Essas actividades visam não apenas integrar os estudantes dentro de suas áreas de estudo, mas também fomentar um ambiente de crescimento académico e pessoal.

A estrutura organizacional do NEFAC é composta por vários níveis de governança estudantil, com destaque para o cargo de presidente, que lidera as actividades e a comunicação entre os estudantes e a administração da faculdade. As eleições para esse cargo ocorrem periodicamente, sendo organizadas por uma comissão eleitoral, que pode incluir tanto docentes quanto estudantes. A comissão é responsável por supervisionar o processo de candidatura, campanhas eleitorais e contagem dos votos, assegurando que as regras eleitorais sejam respeitadas.

Este sistema de governança estudantil dentro da Faculdade de Ciências é essencial para manter a representatividade e garantir que as vozes dos estudantes sejam ouvidas, especialmente em questões relacionadas às condições académico e à infraestrutura da faculdade. Embora a estrutura actual do NEFAC seja funcional, alguns desafios foram identificados, como a comunicação inadequada sobre as eleições, o que resulta em baixa participação estudantil. Segundo um dos presidentes entrevistados, "a comunicação dos estudantes sobre as eleições é uma das principais dificuldades enfrentadas" (Questionário, 2024).

2.1.1. História dos Sistemas de Votação

Historicamente, os sistemas de votação evoluíram consideravelmente ao longo do tempo. No passado, as votações eram feitas de forma completamente manual, com cédulas de papel, como Bovens e Bartsch (2009) descrevem em suas pesquisas sobre o desenvolvimento de métodos eleitorais. Este sistema, ainda utilizado em muitos lugares, é susceptível a erros humanos, manipulação e fraudes. As principais críticas ao sistema manual de votação incluem a falta de segurança, lentidão na contagem de votos e vulnerabilidades no armazenamento das cédulas.



Figura 2: Representação da forma de votação tradicional no Brasil, conforme descrito no artigo "O Voto no Brasil"

Nos últimos anos, com a ascensão da tecnologia, muitos países e instituições passaram a adoptar sistemas de votação electrónica, que buscam aumentar a precisão, reduzir o tempo de apuração e melhorar a

acessibilidade para eleitores. Niemi e Weisberg (2011) apontam que a introdução da votação eletrônica trouxe vantagens, como a redução de erros na contagem de votos, mas também introduziu novas preocupações, principalmente relacionadas à segurança cibernética, privacidade dos eleitores e confiança pública.

2.1.2. Desafios dos Processos Eleitorais

Independentemente do sistema utilizado, os processos eleitorais enfrentam uma série de desafios. De acordo com Pratchett e Wingfield (2013), um dos principais problemas é garantir que o processo seja acessível e inclusivo para todos os eleitores. Em contextos tradicionais, como o de eleições presenciais, barreiras físicas podem impedir que eleitores com dificuldades de locomoção ou aqueles que estão em áreas distantes participem plenamente do processo. Em instituições acadêmicas, isso pode ser particularmente desafiador, já que muitos estudantes têm horários conflitantes ou podem estar distantes da universidade no período de votação.

Além disso, outro desafio importante é a integridade do processo eleitoral. Alvarez e Hall (2008) destacam que fraudes eleitorais, como a manipulação de votos, votos duplos ou a exclusão de eleitores, continuam a ser problemas em diversos sistemas eleitorais, principalmente naqueles que dependem de métodos manuais. Em muitos casos, a falta de transparência no processo de contagem de votos pode minar a confiança dos eleitores ao sistema.

2.1.3. Transição para Sistemas de Votação Eletrônica

Com o avanço das tecnologias, a transição para sistemas de votação eletrônica foi vista como uma solução para muitos dos desafios enfrentados pelos sistemas tradicionais. Cranor e Cytron (1997) afirmam que a votação eletrônica permite maior precisão na contagem, reduzindo a possibilidade de erro humano e acelerando o processo de apuração. Entretanto, a transição para o meio eletrônico não foi isenta de controvérsias.

Segundo Carter e Bélanger (2005), os sistemas eletrônica trazem preocupações adicionais relacionadas à segurança, especialmente em ambientes onde a infraestrutura tecnológica pode ser vulnerável a ataques cibernéticos. Os autores também destacam a importância de garantir que os sistemas eletrônicos mantenham a privacidade dos eleitores, protegendo suas escolhas de forma inviolável.

2.1.4. Fraudes e Segurança em Processos Eleitorais

Mesmo em ambientes acadêmicos, como o caso do NEFAC - UEM, há o risco de fraudes eleitorais, que podem comprometer a legitimidade dos resultados. Tufte (1978) discute a ideia de que fraudes podem ocorrer em diferentes fases do processo eleitoral, desde a identificação dos eleitores até a contagem dos votos. Em sistemas tradicionais, a fraude pode ocorrer por meio da alteração de votos ou da inserção de

votos falsos. Já em sistemas electrónica, fraudes podem ocorrer por meio de manipulação de dados ou vulnerabilidades nos sistemas de contagem.

No contexto universitário, fraudes eleitorais podem incluir desde a exclusão deliberada de votos até a falsificação de identidades para aumentar o número de votos de um candidato específico. Ehrlich (2000) destaca que, em muitos casos, a falta de monitoramento adequado e a ausência de auditoria transparente nos processos eleitorais aumentam o risco de manipulação, tanto em ambientes manuais quanto electrónicos.

2.1.5. Vantagens e Desvantagens dos Sistemas de Votação Electrónica

Os sistemas de votação electrónica oferecem diversas vantagens em relação aos métodos tradicionais. Smith (2010) aponta que esses sistemas podem ser configurados para impedir a votação dupla, garantir a precisão da contagem de votos e oferecer maior acessibilidade aos eleitores. Além disso, sistemas de votação electrónica podem ser integrados a plataformas *online*, permitindo que os eleitores votem de qualquer lugar, desde que tenham acesso à *internet*.

No entanto, Maret (2015) adverte que os sistemas electrónicos também trazem riscos, especialmente no que diz respeito à cibersegurança. A possibilidade de ataques, como *hacking* ou manipulação de resultados, pode minar a confiança dos eleitores no sistema, especialmente se não houver mecanismos de auditoria robustos. Além disso, há o risco de falhas técnicas, como a interrupção do sistema durante a votação, o que poderia impedir que alguns eleitores exerçam seu direito ao voto.

2.1.6. Processos Eleitorais em Contextos Académicos

Em instituições académicas, como no caso do NEFAC, os processos eleitorais frequentemente enfrentam desafios logísticos, como o acesso dos estudantes às urnas e a contabilização de votos em tempo hábil. Chavez e Manuel (2014) sugerem que a implementação de tecnologias modernas, como a votação electrónica ou *online*, pode ser uma solução viável para aumentar a participação dos estudantes e garantir a integridade do processo. Essas tecnologias podem ser integradas com sistemas de autenticação digital, garantindo que apenas os estudantes elegíveis possam votar, e oferecendo maior transparência ao processo.

No entanto, é importante que o desenvolvimento de tais sistemas considere as necessidades específicas do ambiente académico, como a simplicidade de uso e a acessibilidade para todos os estudantes, independentemente de suas habilidades tecnológicas. A votação *online* oferece conveniência e acessibilidade, mas também enfrenta desafios significativos, como a segurança e a privacidade dos eleitores. A resistência a ataques cibernéticos e a falta de confiança do público são barreiras para a adoção generalizada desses sistemas. Chaum et al. (2008) foram pioneiros ao desenvolver um sistema que

emprega criptografia avançada para garantir a segurança e a privacidade dos votos, enquanto Kshetri e Voas (2018) discutem como o *Blockchain* pode mitigar muitos dos problemas enfrentados por esses sistemas.

2.2 Criptografia

A criptografia é a ciência que utiliza algoritmos matemáticos para proteger informações confidenciais. Inicialmente, a criptografia clássica utilizava canetas e papéis para cifrar mensagens, mas com o avanço da tecnologia, a criptografia moderna surgiu, trazendo novas ferramentas e conceitos como a *Enigma Machine*, desenvolvida pelos alemães durante a Segunda Guerra Mundial, e algoritmos de *Hash* criptográfica utilizados em meios digitais. Hoje em dia, a criptografia é considerada um dos principais mecanismos de segurança no meio digital, sendo utilizada para garantir a proteção contra o vazamento de dados. A criptografia tem sido objecto de uma corrida armamentista contínua, onde uma das partes busca novas formas de cifrar informações e a outra busca formas rápidas e eficientes de quebrar essas criptografias.

De acordo com Mendes, Paulicena, Souza (2011) a criptografia é a ciência de utilizar algoritmos (cálculos matemáticos) para ofuscar uma informação, sendo considerada um dos principais mecanismos de segurança no meio digital, usada para garantir a proteção contra os riscos associados a vazamento de dados [fig. 3].

Com o avanço da criptografia e a capacidade de cifrar dados e informações, iniciou-se uma corrida armamentista que ainda dura até os dias de hoje, onde uma das partes busca novas e melhores formas de cifrar informações, enquanto a outra procura formas rápidas e eficientes de quebrar essas criptografias.

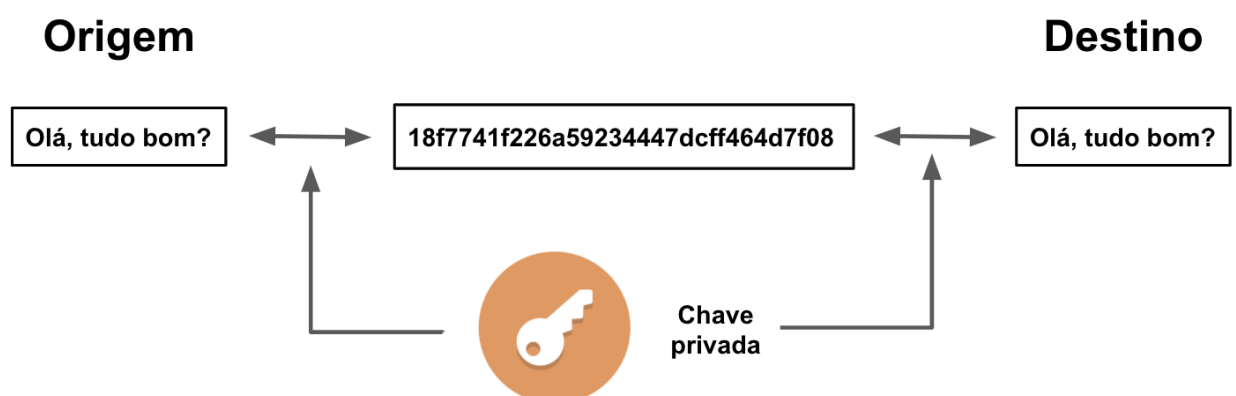


Figura 3: <https://www.universidadejava.com.br/outros/criptografia-simetrica/>

2.3 Blockchain e Sistemas de Votação Electónica

Blockchain – Para entender o porquê de se usar uma *blockchain*, é preciso primeiro entender o que é categoriza uma *blockchain*. De acordo com Santos, Prata, Araujo (2019) *blockchain* pode ser definido como um base de dados que armazena dados em blocos (*block*) ligados em uma cadeia ou corrente (chain).

Blocos possuem em si registo de informações que devem ser inseridos na corrente, o primeiro bloco chamado Bloco Genesis (*Genesis Block*) serve-se como o estado inicial do sistema, todos blocos subsequentes irão possuir uma *hash* criptografada de seus dados e a *hash* de seu antecessor formando se assim a corrente, conforme mostrado na Figura 4.

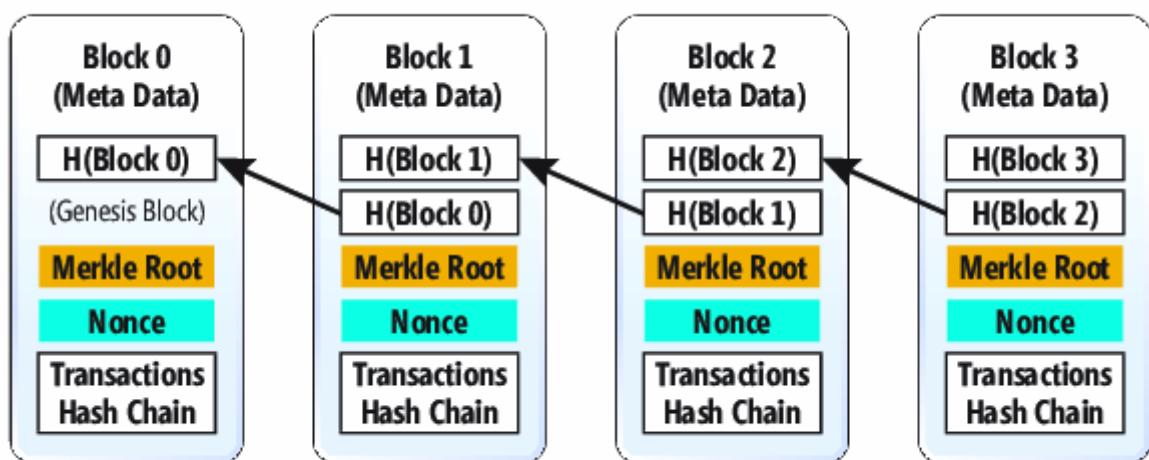


Figura 4: Exemplo de blockchain (learn.microsoft)

Blockchain como um todo possui uma rede descentralizada consistindo em múltiplos nós de cópias exatas dos blocos publicados, para evitar erros de confiabilidade são utilizados algoritmos de consenso como Proof of Work (PoW).

PoW é a validação mais utilizada em redes *blockchain* requerendo que o nó que deseje inserir um bloco na cadeia necessite calcular uma *hash* correspondente as condições impostas pela rede. Cada bloco é validado por um consenso entre os participantes da rede, garantindo sua integridade e impedindo a alteração de dados já registados. Essa validação é feita por meio de criptografia, utilizando chaves públicas e privadas.

Além de registrar transacções financeiras, o *blockchain* pode ser utilizado para armazenar quaisquer tipos de dados, como contratos, registros médicos ou até mesmo votos em eleições. Sua descentralização e segurança tornam a tecnologia atraente para aplicações em diversos setores.

Os valores de *hash* são únicos e a alteração de qualquer dado do bloco gera alteração no valor causando inconsistência na *blockchain* e, como consequência, a detecção da alteração. As principais características da *blockchain* são [Zheng et al. 2018]:

- **Descentralização:** Ao contrário de sistemas centralizados, onde cada transacção é validada por um único agente, uma transacção em uma *blockchain* tem sua validação realizada por dois ou mais nós, reduzindo custos e reduzindo gargalos.
- **Persistência:** Como cada transacção é validada e armazenada por todos os nós da rede e torna-se praticamente impossível de se alterar um bloco. Além disso, todo bloco transmitido para rede seria validado pelos outros nós detetando qualquer tentativa de fraude.
- **Anonimato:** não existe nenhum agente central com informações dos usuários da rede e cada usuário interage com a *blockchain* por um ou mais endereços gerados.

Nos últimos anos, a votação electrónica tornou-se uma alternativa cada vez mais popular para resolver os problemas associados aos sistemas tradicionais de votação. A aplicação de novas tecnologias, como a *Blockchain*, no desenvolvimento de sistemas de votação visa proporcionar maior segurança, transparência e confiança no processo eleitoral. Niemi e Weisberg (2011) destacam que a tecnologia tem o potencial de revolucionar os métodos de votação, eliminando fraudes e falhas humanas, mas também apresenta desafios únicos que precisam ser abordados.

A *blockchain* pode ainda ser vista como um livro-razão compartilhado e imutável que facilita o processo de registo de transacções e rastreamento de activos em uma rede de negócios. Um activo pode ser tangível (uma casa, carro, dinheiro, terra) ou intangível (propriedade intelectual, direitos autorais, voto, marca). Praticamente qualquer coisa de valor que pode ser rastreada e negociada em uma rede *blockchain*, reduzindo riscos e cortando custos para os envolvidos.

2.3.1. Como funciona o *Blockchain*

À medida que cada transacção ocorre, ela é registada como um "bloco" de dados. Essas transacções mostram o movimento de um activo que pode ser tangível (um produto) ou intangível (intelectual). O bloco de dados pode registar as informações de sua escolha: quem, o quê, quando, onde, quanto. Pode até registar a condição, como a temperatura de uma remessa de alimentos.

Cada bloco é conectado aos anteriores e posteriores, esses blocos formam uma cadeia de dados à medida que um activo se move de um lugar para outro ou a propriedade muda de mãos. Os blocos confirmam o tempo exacto e a sequência de transacções, e os blocos se ligam de forma segura para impedir que qualquer bloco seja alterado ou que um bloco seja inserido entre dois blocos existentes.

As transacções são agrupadas em uma cadeia irreversível: um *blockchain*. Cada bloco adicional reforça a verificação do bloco anterior e, portanto, de todo o *blockchain*. Tornando o *blockchain* inviolável, fornecendo a principal força da imutabilidade. Removendo a possibilidade de adulteração por um actor malicioso e construindo um livro-razão de transacções em que você e outros membros da rede podem confiar. IBM (2018).

2.3.2. Vantagens dos Sistemas de Votação Eletrónica com *Blockchain*

A votação eletrónica traz inúmeras vantagens. Em comparação com os sistemas manuais, os sistemas eletrónicos reduzem significativamente o tempo de contagem de votos, aumentam a precisão dos resultados e permitem maior acessibilidade, especialmente para eleitores que não podem estar fisicamente presentes nos locais de votação. Cranor e Cytron (1997) apontam que os sistemas eletrónicos facilitam a participação de eleitores de diferentes localizações, permitindo que os eleitores votem remotamente, de qualquer dispositivo conectado à *internet*.

A incorporação da tecnologia *Blockchain* adiciona uma camada extra de segurança e transparência ao processo de votação. Swan (2015) argumenta que a *Blockchain*, uma estrutura descentralizada e imutável de registos, oferece uma plataforma onde cada voto pode ser auditado e verificado sem a necessidade de uma autoridade central. Isso elimina a possibilidade de adulteração de votos após a sua emissão e garante que cada voto registrado na *Blockchain* seja único e válido.

Entre as principais vantagens da *Blockchain* em sistemas eleitorais estão:

- **Transparência:** Todos os votos são registados em um livro-razão público e distribuído, acessível a qualquer parte interessada, o que dificulta a manipulação dos resultados.
- **Segurança:** A descentralização da *Blockchain* torna os sistemas eleitorais menos suscetíveis a ataques cibernéticos, já que não há um ponto único de falha. Cada voto é criptografado e registrado permanentemente, o que torna a falsificação ou exclusão de votos extremamente difícil.
- **Imutabilidade:** Uma vez que um voto é registrado na *Blockchain*, ele não pode ser alterado ou apagado, garantindo que o histórico da votação permaneça inalterado ao longo do tempo.
- **Auditabilidade:** Qualquer entidade pode auditar o sistema sem comprometer a privacidade dos eleitores, já que os dados dos votos são registados de forma anônima, mas verificável.

2.3.3. Desafios e Limitações dos Sistemas de Votação Eletrónica com *Blockchain*

Apesar das inúmeras vantagens, a implementação de sistemas de votação eletrónica com *Blockchain* apresenta desafios que precisam ser cuidadosamente considerados. Carter e Bélanger (2005) alertam que a complexidade técnica da *Blockchain* pode limitar sua adopção em larga escala, especialmente em

contextos onde a infraestrutura tecnológica é limitada ou onde o eleitorado não está familiarizado com o uso de tecnologias avançadas.

Alguns dos principais desafios incluem:

- **Escalabilidade:** À medida que o número de eleitores cresce, o tempo necessário para processar e validar cada voto na *Blockchain* pode aumentar significativamente, resultando em atrasos na apuração dos resultados.
- **Privacidade dos Eleitores:** Embora a *Blockchain* seja eficaz na manutenção da integridade dos votos, garantir a privacidade dos eleitores continua a ser uma preocupação. Zyskind et al. (2015) apontam que, embora os votos sejam registados de forma anônima, existem preocupações sobre a possibilidade de rastrear o comportamento dos eleitores por meio de métodos de análise avançada de dados.
- **Custo de Implementação:** A adoção de uma solução baseada em *Blockchain* requer investimentos substanciais em infraestrutura, treinamento de pessoal e manutenção do sistema. Isso pode ser inviável para instituições menores ou para processos eleitorais com recursos limitados.
- **Acessibilidade e Inclusão Digital:** Pratchett e Wingfield (2013) levantam preocupações sobre a inclusão digital, especialmente em contextos onde o acesso à internet ou a dispositivos digitais é limitado. A transição para sistemas eletrônicos pode excluir eleitores que não têm acesso ou conhecimento suficiente para utilizar essas plataformas.

A superação desses desafios exige um Planeamento cuidadoso e a colaboração entre autoridades eleitorais, especialistas em segurança digital e desenvolvedores de *software* para garantir que a implementação de sistemas de votação com *Blockchain* seja eficaz e acessível.

2.3.4. Aplicações da *Blockchain* em Eleições Académicas e Institucionais

A tecnologia *Blockchain* tem sido amplamente discutida como uma solução viável para resolver os problemas associados às eleições tradicionais, e suas aplicações vão além das eleições governamentais. Instituições académicas e corporativas têm começado a adotar a *Blockchain* como uma forma de garantir a segurança e a transparência em seus processos eleitorais internos.

Chavez e Manuel (2014) sugerem que, em contextos académicos a *Blockchain* pode ser uma ferramenta valiosa para garantir a integridade do processo eleitoral, evitando fraudes e aumentando a participação estudantil. Em muitos casos, os sistemas de votação tradicionais em universidades são baseados em métodos manuais, que são suscetíveis a erros e fraudes. A adoção de uma solução baseada em *Blockchain*

pode permitir que os estudantes votem remotamente, com segurança, de qualquer dispositivo, ao mesmo tempo em que garante que o processo seja auditável e transparente.

Uma aplicação típica da *Blockchain* em eleições académicas envolveria a criação de uma plataforma onde cada estudante registado na instituição teria uma carteira digital (wallet), que funcionaria como um identificador único. Tschorsch e Scheuermann (2016) descrevem que, nesse modelo, cada voto emitido seria registado na *Blockchain*, garantindo que cada estudante só pudesse votar uma vez, eliminando o risco de votos duplicados. Além disso, a contagem dos votos seria automática e auditável em tempo real, oferecendo resultados instantâneos e verificáveis.

2.3.5. Futuro dos Sistemas de Votação com *Blockchain*

O futuro dos sistemas de votação com *Blockchain* parece promissor, mas a sua adopção em larga escala depende de um maior desenvolvimento tecnológico e de uma maior confiança por parte do público e das instituições. Nakamoto (2008), em sua introdução à tecnologia *Blockchain*, previa que a descentralização e a transparência oferecidas pela *Blockchain* poderiam transformar muitas indústrias, incluindo os processos eleitorais. No entanto, para que essa visão se concretize, será necessário superar as barreiras de custo, acessibilidade e privacidade.

Nos próximos anos, é provável que vejamos um aumento na adopção de sistemas de votação eletrónica com *Blockchain* em contextos menores, como eleições académicas e empresariais, antes que a tecnologia seja amplamente utilizada em eleições governamentais. Swan (2015) destaca que a confiança do público nos sistemas de votação eletrónica precisa ser cultivada através de uma implementação gradual, que permita o teste e a validação da tecnologia em ambientes controlados.

A pesquisa em torno de novos mecanismos para melhorar a privacidade dos eleitores e a escalabilidade dos sistemas de *Blockchain* continua a ser uma área activa de desenvolvimento. Maret (2015) sugere que o avanço em tecnologias como a criptografia homomórfica e as ZK-Snarks (Zero-Knowledge Proofs) pode fornecer soluções inovadoras para os problemas actuais, permitindo que a *Blockchain* se torne uma solução viável e segura para eleições de grande escala.

Material e Métodos

Neste capítulo, serão detalhados os materiais e métodos utilizados para conduzir esta pesquisa. Será descrita a metodologia adotada para o desenvolvimento do protótipo do sistema de votação *online* baseado em *Blockchain*, bem como os métodos de recolha e análise de dados que fundamentaram o trabalho. A pesquisa foi orientada por uma abordagem exploratória e descritiva, com o objetivo de compreender os processos eleitorais actuais e propor melhorias a partir da tecnologia *Blockchain*. Este capítulo também aborda as ferramentas, linguagens de programação e tecnologias seleccionadas para o desenvolvimento do protótipo, além de justificar suas escolhas com base na revisão de literatura.

3.1 Metodologia de pesquisa

A pesquisa foi desenvolvida com base em uma abordagem qualitativa, buscando compreender os problemas e limitações do processo eleitoral actual no NEFAC-UEM e propor um sistema alternativo. O estudo incluiu a análise de documentos, entrevistas com *stakeholders* e a revisão de literatura sobre sistemas de votação e *Blockchain*. Além disso, optou-se por um estudo de caso específico, focando nas eleições do Núcleo dos Estudantes da Faculdade de Ciências, para exemplificar a aplicação prática do sistema proposto.

3.1.1. Pesquisa Quanto à Natureza

A pesquisa classifica-se como aplicada, uma vez que busca desenvolver soluções práticas para os desafios encontrados no processo eleitoral do NEFAC-UEM. O desenvolvimento de um sistema de votação *online* baseado em *Blockchain* visa resolver questões de segurança, transparência e confiabilidade nas eleições do núcleo. Essa pesquisa também é exploratória, pois investiga a viabilidade do uso da tecnologia *Blockchain* em processos eleitorais e, ao mesmo tempo, descritiva, ao analisar o processo eleitoral actual e identificar suas limitações.

3.1.2. Pesquisa Quanto à Forma de Abordagem

A abordagem utilizada foi qualitativa, priorizando a colecta de informações a partir de entrevistas com os *stakeholders* envolvidos nas eleições do NEFAC-UEM (questionário, 2024) e a análise documental. O uso de métodos qualitativos permitiu uma compreensão mais profunda dos problemas enfrentados pelo sistema actual de votação e facilitou a elaboração de uma solução tecnológica adequada. A colecta de

dados também incluiu uma análise crítica dos processos eleitorais e das ferramentas tecnológicas existentes para votação *online*.

3.1.3. Técnicas de Recolha de Dados

Foram utilizadas técnicas de recolha de dados primários e secundários. Entre os métodos primários, destacam-se as entrevistas semiestruturadas, aplicadas a líderes e membros do NEFAC-UEM (questionário, 2024). As entrevistas nos deram uma visão clara das dificuldades que as pessoas enfrentam nas eleições do núcleo e das ideias que elas têm sobre como um sistema eletrônico de votação poderia melhorar esse processo.

3.1.3.1. Entrevista

As entrevistas semiestruturadas foram utilizadas como técnica principal de colecta de dados, permitindo uma interação flexível com os participantes, como o actual presidente do núcleo. Segundo Richardson (1999), a entrevista semiestruturada é um método eficaz para explorar opiniões e atitudes, o que é essencial para compreender as preocupações dos estudantes em relação à segurança e à integridade do processo eleitoral. As entrevistas foram conduzidas com o actual presidente do NEFAC-UEM e outros membros-chave que participam do processo eleitoral, como presidentes de alguns departamentos da faculdade e estudantes (questionário, 2024). Essas entrevistas forneceram informações valiosas sobre o funcionamento actual do sistema de eleições, suas limitações, e expectativas em relação à modernização do processo. O feedback obtido foi essencial para o desenvolvimento de requisitos para o sistema de votação *online* baseado em *Blockchain*.

3.2 Metodologia de desenvolvimento

Este projecto adota a metodologia Ágil, especificamente o *framework Scrum*, por sua flexibilidade e adaptabilidade às mudanças durante o processo de desenvolvimento. Segundo Schwaber e Sutherland (2017), o *Scrum* é ideal para projectos em que os requisitos podem evoluir durante o processo de desenvolvimento, como é o caso do sistema proposto. Conforme podemos ver na Figura 5.

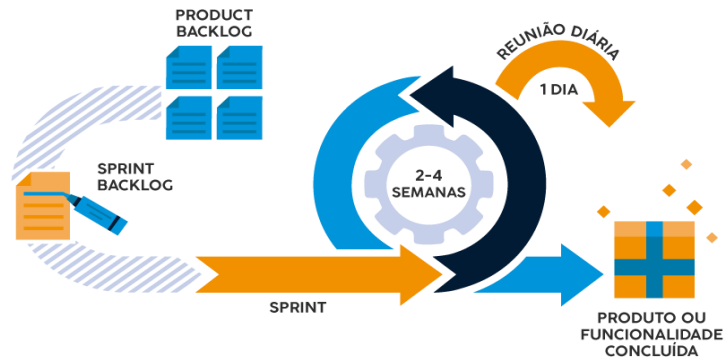


Figura 5: Funcionamento da metodologia de desenvolvimento Scrum, Somemerville (2011)

Serão utilizados os seguintes os seguintes materiais ou tecnologias de desenvolvimento:

3.2.1. Ferramentas de Desenvolvimento

O desenvolvimento de um sistema de votação *online* baseado em tecnologia *Blockchain* exigiu a utilização de uma variedade de ferramentas e tecnologias. Cada uma dessas ferramentas desempenhou um papel crucial no processo de modelagem, desenvolvimento e simulação do sistema, permitindo que a equipe abordasse os desafios de forma eficiente e eficaz. A seguir, são descritas as principais ferramentas utilizadas, bem como suas funções e importâncias dentro do projecto.

3.2.1.1. Astah

Para a modelagem do sistema, utilizamos o Astah, uma ferramenta de modelagem visual que suporta várias notações, incluindo *UML (Unified Modeling Language)*. O Astah permite a criação de diagramas de classes, casos de uso, sequência e outros, facilitando a visualização e a compreensão das interações entre os diferentes componentes do sistema. O uso de diagramas *UML* é uma prática recomendada em engenharia de *software*, pois ajuda a representar graficamente as especificações do sistema e suas interações, tornando mais fácil para os desenvolvedores e partes interessadas entenderem a estrutura e o funcionamento do sistema (Booch et al., 2007).

3.2.1.2. HTML, CSS e JavaScript

No desenvolvimento do *front-end* do sistema, utilizamos *HTML (HyperText Markup Language)*, *CSS (Cascading Style Sheets)* e *JavaScript*. O *HTML* é a linguagem padrão para a criação de páginas da *web*, permitindo estruturar o conteúdo de forma semântica. O *CSS*, por sua vez, é utilizado para estilizar e formatar a aparência visual das páginas, garantindo uma interface agradável e responsiva para o usuário. O *JavaScript* é uma linguagem de programação que permite adicionar interatividade às páginas da *web*, tornando-as dinâmicas e melhorando a experiência do utilizador Juntas, essas tecnologias formam a base

do desenvolvimento *web* moderno, permitindo que criemos interfaces de utilizador atrativas e funcionais (Duckett, 2014).

3.2.1.3. PHP e Laravel

Para o desenvolvimento do *back-end*, optou-se por PHP (*Hypertext Preprocessor*), uma linguagem de programação amplamente utilizada para desenvolvimento *web*. PHP é especialmente eficaz na criação de aplicações que interagem com base de dados e processam dados do lado do servidor. Com o objectivo de acelerar o desenvolvimento e garantir boas práticas de programação, utilizou-se o Laravel, um *framework* PHP que fornece uma estrutura robusta e um conjunto de ferramentas para facilitar o desenvolvimento de aplicações *web*. Laravel é conhecido por sua sintaxe elegante e recursos avançados, como roteamento, autenticação, e um sistema de ORM (*Object-Relational Mapping*) chamado *Eloquent*, que simplifica a interação com base de dados (Taylor, 2011).

3.2.1.4. Composer e NPM

Para gerir as dependências do projecto, utilizou-se Composer e NPM (*Node Package Manager*). O Composer é uma ferramenta de gestão de dependências para PHP que permite instalar e actualizar bibliotecas de terceiros de forma fácil e eficiente, garantindo que todas as dependências do projecto estejam sempre actualizadas e compatíveis. Já o NPM é um gestor de pacotes para JavaScript que facilita a instalação de bibliotecas e ferramentas utilizadas no desenvolvimento *front-end*, como *frameworks* e bibliotecas, contribuindo para um ambiente de desenvolvimento mais organizado e productivo (Locke, 2018).

3.2.1.5. MySQL

O sistema utiliza o MySQL, um sistema de gestão de base de dados relacional amplamente utilizado. O MySQL permite armazenar e gerir dados de forma eficiente, oferecendo suporte a consultas complexas e garantindo a integridade e segurança dos dados. A escolha do MySQL se deve à sua popularidade, facilidade de uso e integração com PHP, tornando-o uma opção ideal para o armazenamento de dados das eleições, candidatos e votos (Widenius et al., 2015).

3.2.1.6. Simulação de *Blockchain*

Para simular a funcionalidade de *Blockchain* no sistema, utilizou-se uma combinação de conceitos teóricos e ferramentas práticas. A *Blockchain* é uma tecnologia que permite o registo seguro e imutável de transacções, e sua implementação foi feita através de simulações que garantiram a integridade dos votos registados. A simulação de *Blockchain* é fundamental para assegurar que os dados dos votos sejam inalteráveis e que a transparência do processo eleitoral seja mantida. Essa tecnologia é amplamente reconhecida por sua capacidade de aumentar a segurança e a confiança em sistemas digitais (Nakamoto, 2008).

```

return new Class extends Migration
{
    /**
     * Run the migrations.
     */
    public function up(): void
    {
        Schema::create('blocks', function (Blueprint $table) {
            $table->id();
            $table->json('data');//voto na blockchain
            $table->string('hash'); // Hash do bloco
            $table->string('previous_hash'); // Hash do bloco anterior
            $table->timestamps();
        });
    }
}

```

Figura 6: Migration do Block na blockchain. Autor (2024)

Para garantir que os blocos da nossa rede *blockchain*, sejam validos e sigam um padrão aceitável na rede foi criada uma função que quando registado um voto é automaticamente criado um bloco correspondente e adicionado a *blockchain* mantendo a criptografia e garantindo a imutabilidades dos mesmos, conforme ilustra a figura 7.

```

// Dados a serem armazenados no campo 'data'
$data = [
    'eleitorId' => $eleitor->id,
    'eleicaoId' => $eleicao->id,
    'candidatoId' => $request->candidato_id
];

// Codificar os dados como JSON
$jsonData = json_encode($data);

// Criar o hash do bloco (para simplificar, vamos usar a hash do jsonData + previousHash)
$blockHash = hash('sha256', $jsonData);

// Criar um novo bloco
$block = new Block();
$block->hash = $blockHash;
$block->previous_hash = Block::latest()->first()->hash ?? 0;
$block->data = $jsonData; // Aqui os dados são armazenados em JSON
$block->save();

```

Figura 7: metodo para adição de um novo bloco na rede. Autor (2024)

3.2.1.7. Git e GitHub

Para o versionamento do código, utilizou-se Git, um sistema de controlo de versão distribuído que permite que múltiplos desenvolvedores colaborem em um projecto simultaneamente. O uso do Git facilita o rastreamento de alterações no código, a reversão a versões anteriores e a ramificação para desenvolvimento de novas funcionalidades. O GitHub é uma plataforma *online* que hospeda repositórios Git, proporcionando uma interface amigável para colaboração, revisão de código e gerenciamento de projectos. Essa combinação de Git e GitHub é uma prática padrão na indústria de software, promovendo a transparência e a organização no desenvolvimento de projectos (Chacon & Straub, 2014).

Caso de Estudo

Neste capítulo, será apresentada a organização estudada no âmbito deste trabalho de monografia, o NEFAC-UEM, e como o processo eleitoral actual está estruturado. Serão descritos o modelo actual de eleição do presidente do núcleo, identificando as limitações e desafios. Posteriormente, será proposto um novo modelo baseado em um sistema de votação *online* utilizando a tecnologia *Blockchain*, detalhando as melhorias esperadas em termos de segurança, transparência e eficiência no processo eleitoral.

4.1 Organização Estudada: NEFAC-UEM

O NEFAC é uma organização composta por estudantes e que tem como principal objectivo representar os interesses dos estudantes da faculdade, tanto no âmbito académico quanto social. Sua estrutura organizacional é composta por diferentes cargos, sendo o principal deles o presidente do núcleo, que é responsável por liderar o núcleo e zelar pelos interesses da comunidade estudantil.

4.2 Modelo Actual

4.2.1. Descrição do Fluxo de Informação no Modelo Actual

O processo eleitoral actual do NEFAC segue um modelo tradicional de votação, onde os candidatos se inscrevem para o cargo de presidente, fazem suas campanhas e, em um determinado dia, ocorre a votação presencial, na qual os estudantes comparecem para exercer seu direito de voto. Podemos constatar o este fluxo na figura 8. Esse modelo, apesar de cumprir seu propósito básico de escolha do presidente, apresenta desafios, como a falta de comunicação adequada sobre o processo eleitoral e a baixa adesão dos estudantes, conforme relatado nas respostas ao questionário.

As principais etapas do processo de eleição, conforme descritas pelos entrevistados, incluem:

- Abertura das candidaturas e inscrição dos candidatos;
- Campanhas eleitorais realizadas de forma presencial ou *online*;
- Votação presencial;
- Contagem dos votos e anúncio do vencedor.

Apesar de cumprir seu papel, este modelo apresenta limitações, como a possibilidade de fraudes, dificuldades na contagem manual dos votos e a ausência de transparência em algumas etapas do processo. Além disso, a baixa participação dos estudantes, com menos de 50% do corpo discente participando do processo, também é uma preocupação relevante.

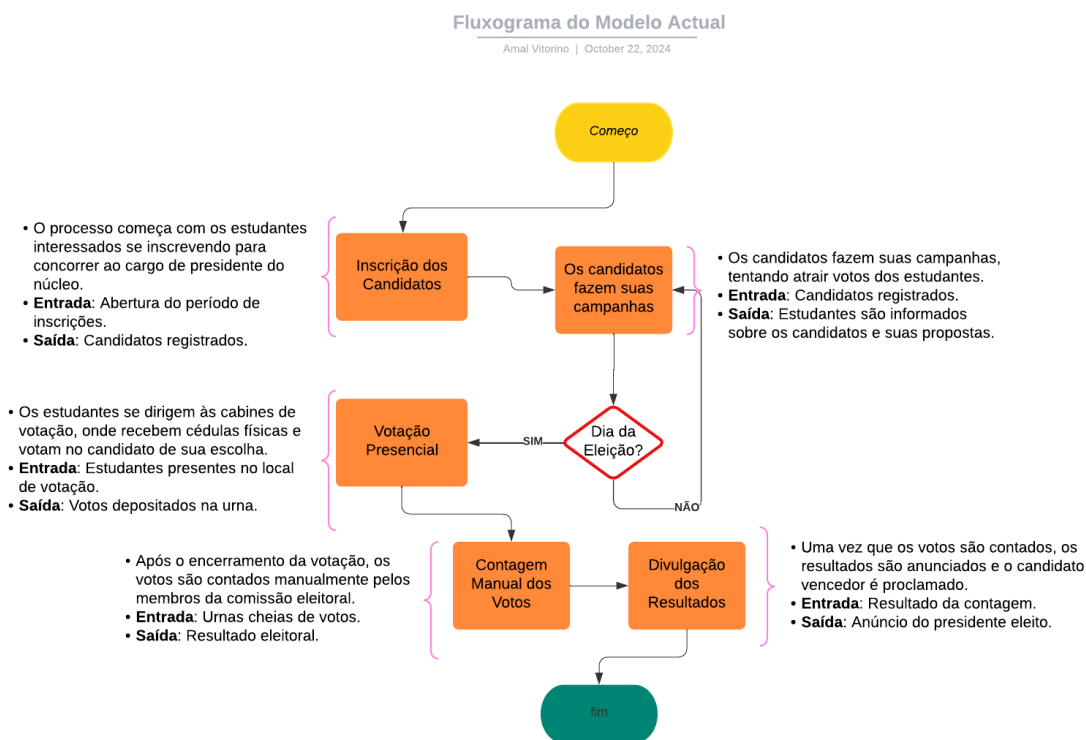


Figura 8: Modelo actual, Autor (2024)

4.3. Modelo proposto

Com base nas limitações do modelo actual, este trabalho propõe um sistema de votação *online*, utilizando a tecnologia *Blockchain*. A principal vantagem de se utilizar *Blockchain* em sistemas de votação é a segurança, garantindo que os votos não possam ser manipulados, além de aumentar a transparência e permitir auditorias eficazes.

4.3.1. Principais características do modelo proposto

- **Segurança:** *Blockchain* oferece um alto nível de segurança, impossibilitando a alteração dos votos uma vez registrados, garantindo a integridade do processo.
- **Transparência:** Todas as etapas do processo podem ser verificadas por qualquer participante, garantindo que o processo seja auditável e acessível.
- **Acessibilidade:** Com a implementação de um sistema de votação *online*, espera-se que mais estudantes participem das eleições, devido à facilidade de votar remotamente.

- **Eficiência:** A contagem de votos seria feita automaticamente pelo sistema, evitando erros humanos e acelerando o processo de divulgação dos resultados.

Esse novo modelo proposto busca solucionar os problemas de comunicação, baixa adesão e falta de transparência, criando um ambiente mais seguro e confiável para a realização das eleições.

4.3.2. Fluxo de Informação no Sistema Proposto

O fluxo de informação no sistema proposto segue os seguintes passos:

- Inscrição e verificação de candidatos;
- Autenticação dos eleitores (estudantes da faculdade) no sistema de votação;
- Votação *online*, com registo dos votos em *Blockchain*;
- Encerramento do processo de votação e contagem automática dos votos;
- Auditoria e divulgação dos resultados de forma transparente para toda a comunidade acadêmica.

Ao adotar essa nova abordagem, espera-se que o NEFAC possa superar os desafios do modelo tradicional, promovendo eleições mais seguras, participativas e transparentes.

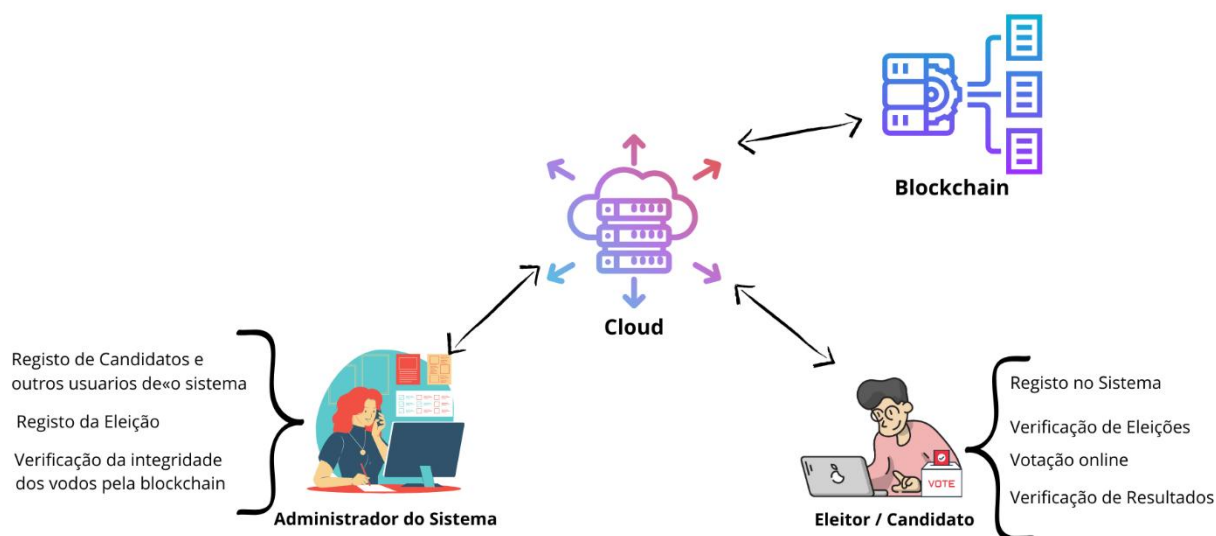


Figura 9: Modelo proposto, Autor (2024)

4.3.3. Requisitos do sistema proposto

Prioridades dos Requisitos

Alta: é um requisito de grande importância para o funcionamento do sistema, sem o qual o sistema não entra em funcionamento, esses requisitos devem ser implementados em primeiro lugar.

Média: este requisito, a sua ausência não impede o funcionamento do sistema, mas não garante o funcionamento de forma eficaz, esses requisitos podem ser implantados mesmo tendo o sistema em produção.

Baixa: este requisito não compromete as funcionalidades básicas do sistema.

4.3.3.1. Requisitos Funcionais

Os requisitos funcionais representam as capacidades essenciais que o sistema de votação *online* deve possuir para cumprir seus objetivos. Eles foram definidos com base na necessidade de garantir um processo de votação seguro, eficiente e acessível a todos os eleitores. Os principais requisitos funcionais incluem:

Tabela 1: Requisitos funcionais. Autor (2024)

ID	Requisito	Descrição	Detalhes	Prioridade
1	Autenticação de Eleitores	O sistema deve verificar a identidade dos eleitores antes que eles possam votar.	A autenticação será realizada utilizando métodos seguros, como autenticação multifactor (MFA) combinando senha, chave de segurança.	Alta
2	Emissão de Voto	O sistema deve permitir que eleitores emitam seus votos de forma segura e anônima.	Cada voto será registrado em um bloco na <i>Blockchain</i> , garantindo que ele não possa ser alterado ou excluído após a submissão.	Alta
	Contagem de Votos	O sistema deve contar os votos de forma automática e precisa, garantindo a integridade do processo.	A contagem dos votos será transparente e auditável, uma vez que toda a transacção de votos estará registada na <i>Blockchain</i> .	Alta
5	Visualização dos Resultados	O sistema deve permitir que os resultados da votação sejam visualizados em tempo real.	Os resultados poderão ser acessados por qualquer pessoa, garantindo transparência no processo eleitoral.	Média

6	Auditoria e Transparência	O sistema deve permitir a auditoria completa de todos os votos e atividades dentro da <i>Blockchain</i> .	Audidores e outras partes autorizadas poderão acessar os registros de votação, garantindo que o processo foi justo e seguro.	Alta
---	------------------------------	---	--	------

4.3.3.2. Requisitos não funcionais

Os requisitos não funcionais descrevem as qualidades que o sistema deve possuir, garantindo que ele atenda às expectativas de desempenho, segurança, escalabilidade, usabilidade e confiabilidade. Estes requisitos são fundamentais para a operação bem-sucedida do sistema em um ambiente real:

Tabela 2: Requisitos não funcionais. Autor (2024)

ID	Requisito	Descrição	Detalhes	Prioridade
1	Segurança	O sistema deve garantir a segurança dos dados dos eleitores e a integridade dos votos.	Utilização de criptografia avançada, segurança na camada de transporte (TLS/SSL), e outras medidas de segurança cibernética.	Alta
2	Escalabilidade	O sistema deve suportar um grande número de eleitores simultâneos sem perda de desempenho.	A arquitetura deve ser projectada para escalar horizontalmente, utilizando tecnologias como microserviços e balanceamento de carga.	Média
3	Desempenho	O sistema deve ter tempos de resposta rápidos para funcionalidades críticas.	Optimizações de base de dados, caching, e minimização de latência nas transacções <i>Blockchain</i> .	Alta
4	Usabilidade	O sistema deve ser fácil de usar, com uma interface intuitiva para todos os eleitores.	Design centrado no utilizador, com protótipos de alta fidelidade desenvolvidos no Figma.	Média
5	Confiabilidade	O sistema deve estar disponível e funcional durante todo o período de votação, sem falhas.	Implementação de redundância, recuperação de desastres, e monitoramento contínuo.	Alta

6	Transparência	Todo o processo de votação deve ser transparente e verificável.	Registro imutável na <i>Blockchain</i> , acessível para auditoria pública.	Alta
---	---------------	---	--	------

4.3.3.3. Funcionalidades Adicionais (opcional)

Além dos requisitos básicos, o modelo proposto inclui funcionalidades adicionais que podem ser implementadas para melhorar a experiência do usuário e a acessibilidade do sistema. Estas funcionalidades são opcionais, mas podem agregar valor significativo ao sistema:

Tabela 3: Funcionalidades adicionais (2024)

ID	Requisito	Descrição	Detalhes	Prioridade
1	Notificações de Votação	Enviar lembretes aos eleitores para votar.	Lembretes automáticos via e-mail ou SMS para os eleitores que ainda não votaram.	Baixa
2	Suporte Multilíngue	O sistema deve suportar várias línguas para atender a uma população diversa.	Interface e instruções disponíveis em múltiplos idiomas para maior acessibilidade.	Média
3	Acessibilidade	O sistema deve ser acessível para pessoas com deficiências.	Suporte para leitores de tela, navegação via teclado, e outras tecnologias assistivas para garantir inclusividade total.	Média

4.4. Modelação do modelo Proposto

4.4.1. Diagrama de Classes

Uma classe é a descrição de um conjunto de objectos que partilham os mesmos atributos, operações, relações e a mesma semântica. Uma classe corresponde a algo tangível ou a uma abstracção conceptual existente no domínio do utilizador ou no domínio do engenheiro de *software* (Silva & Videira, 2001).

O processo de modelação envolve a criação de diagramas que representam o funcionamento e o fluxo de informação no sistema, desde a interação do usuário até a finalização da votação. Nesta etapa, serão

utilizados diagramas UML (*Unified Modeling Language*) para ilustrar as interações e os principais componentes do sistema.

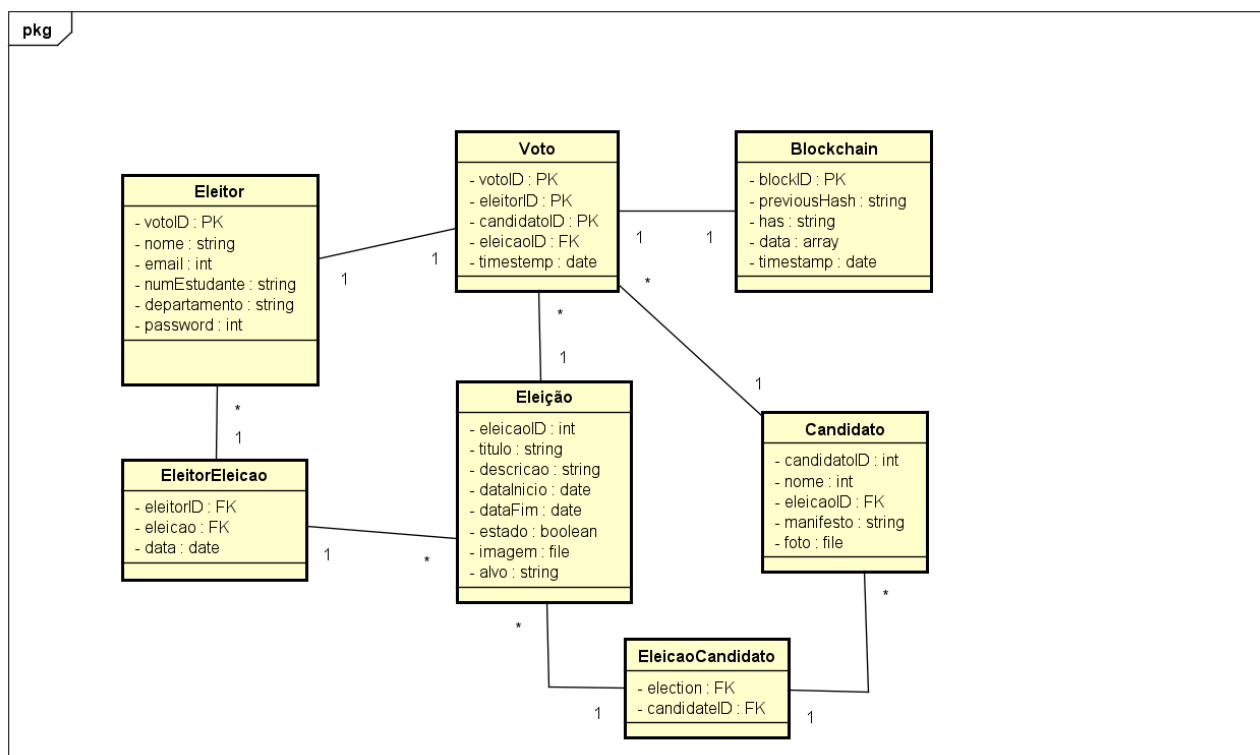


Figura 10: Diagrama de Entidade e Relacionamento DER. Autor (2024)

4.4.2. Diagramas de caso de uso

Um diagrama de casos de utilização descreve a relação entre actores e casos de utilização de um dado sistema. Este é um diagrama que permite dar uma visão global e de alto nível do sistema, sendo fundamental a definição correcta da sua fronteira. (Silva & Videira, 2001)

4.4.2.1. Diagrama de Caso de Uso Para Registo de Utilizadores

O diagrama abaixo descreve a proposta de funcionamento do registo de utilizadores no sistema proposto.

Tabela 4: Diagrama de Caso de Uso Para Registo de Usuários (2024)

CU01	Registo de usuários
Utilizadores Envolvidos	Administrador, eleitor
Condições Prévias	O sistema deve estar inicializado, e os perfis de administrador devem estar definidos previamente.
Descrição	O Administrador pode registrar e criar perfis de administradores. Fornecendo dados válidos para o efeito.
Prioridade	Alta

Relacionamento com Outros Casos	Relacionado à "Configuração da Eleição" e ao "Processo de Votação".
---------------------------------	---

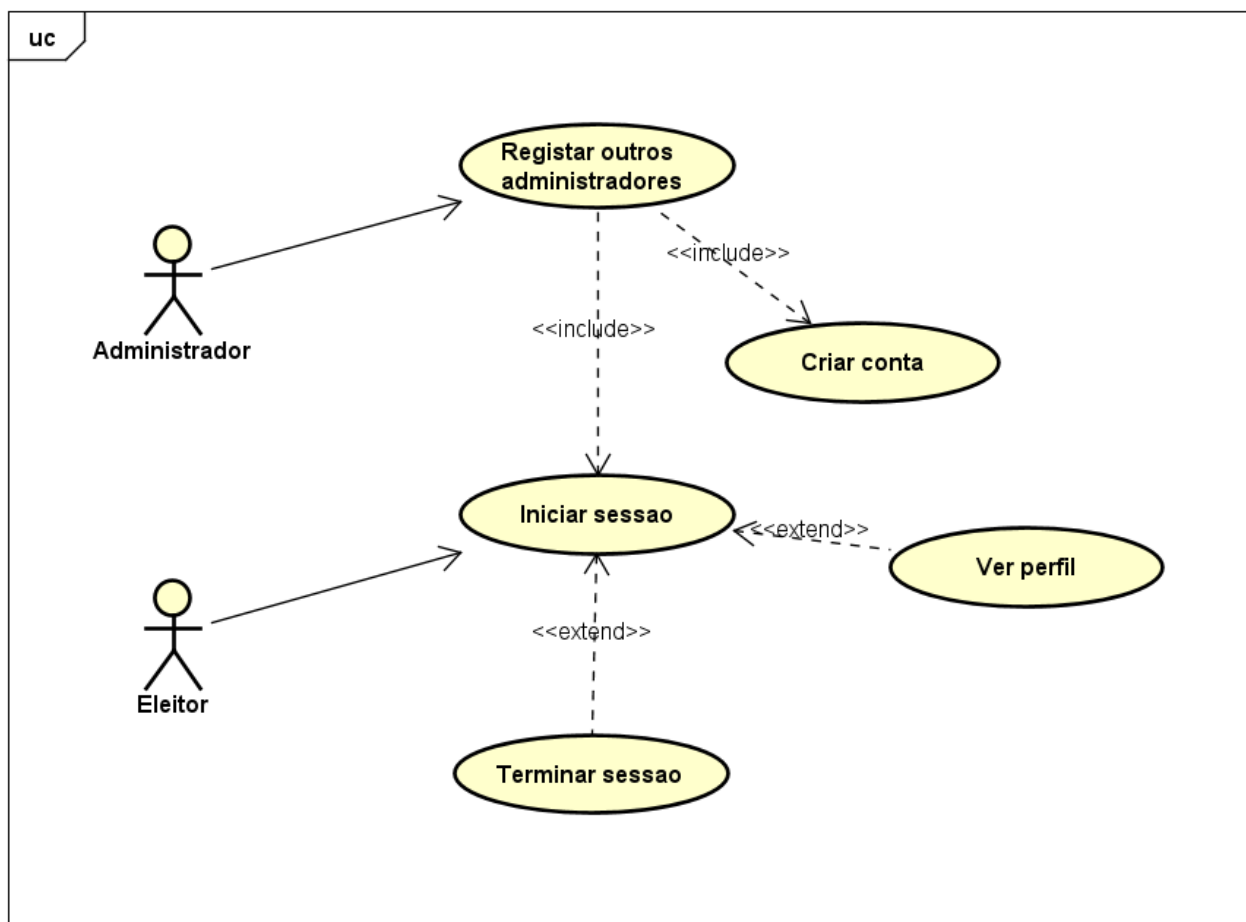


Figura 11: Diagrama de Caso de Uso Para Registo de Usuários. Autor (2024)

4.4.2.2. Diagrama de Caso de Uso Para Configuração da Eleição

O diagrama abaixo descreve a proposta de funcionamento para a configuração a eleição no sistema proposto.

Tabela 5: Diagrama de Caso de Uso Para Configuração da Eleição. Autor (2024)

CU02	Configuração da Eleição
Utilizadores	Administrador
Envolvidos	
Condições Prévias	Eleitores e administradores devem estar registados no sistema.
Descrição	O administrador define parâmetros da eleição, como datas, candidatos e critérios de elegibilidade dos eleitores, bem como o alvo da eleição.
Prioridade	Alta

Relacionamento com Outros Casos	Dependente do "Registo de Candidatos" e relacionado ao "Processo de Votação".
---------------------------------	---

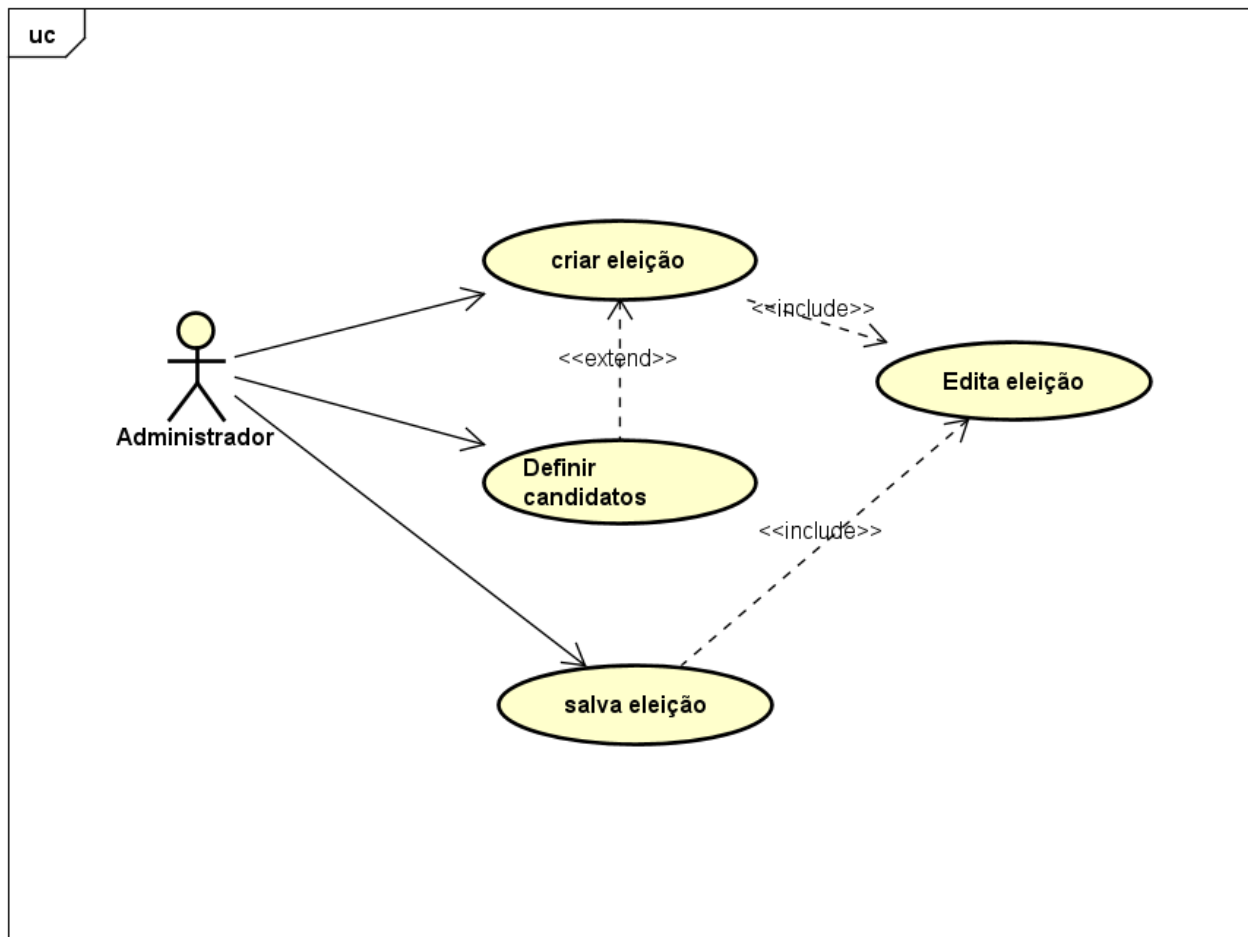


Figura 12: Diagrama de Caso de Uso Para Configuração da Eleição. Autor (2024)

4.4.2.3. Diagrama De Caso De Uso Para o Processo De Votação

O diagrama abaixo descreve a proposta de funcionamento para o processo de votação no sistema proposto.

Tabela 6: Diagrama De Caso De Uso Para o Processo De Votação. Autor (2024)

CU03	Processo de Votação
Utilizadores Envolvidos	Eleitor, administrador
Condições Prévias	A eleição deve estar configurada e activa, e o eleitor deve estar registrado e autenticado.
Descrição	

	Eleitores autenticados podem acessar o sistema para votar nos candidatos disponíveis. O sistema garante que cada eleitor vote apenas uma vez.
Prioridade	Alta
Relacionamento com Outros Casos	Relacionado ao "Autentificação" e à "Contagem e Verificação de Votos".

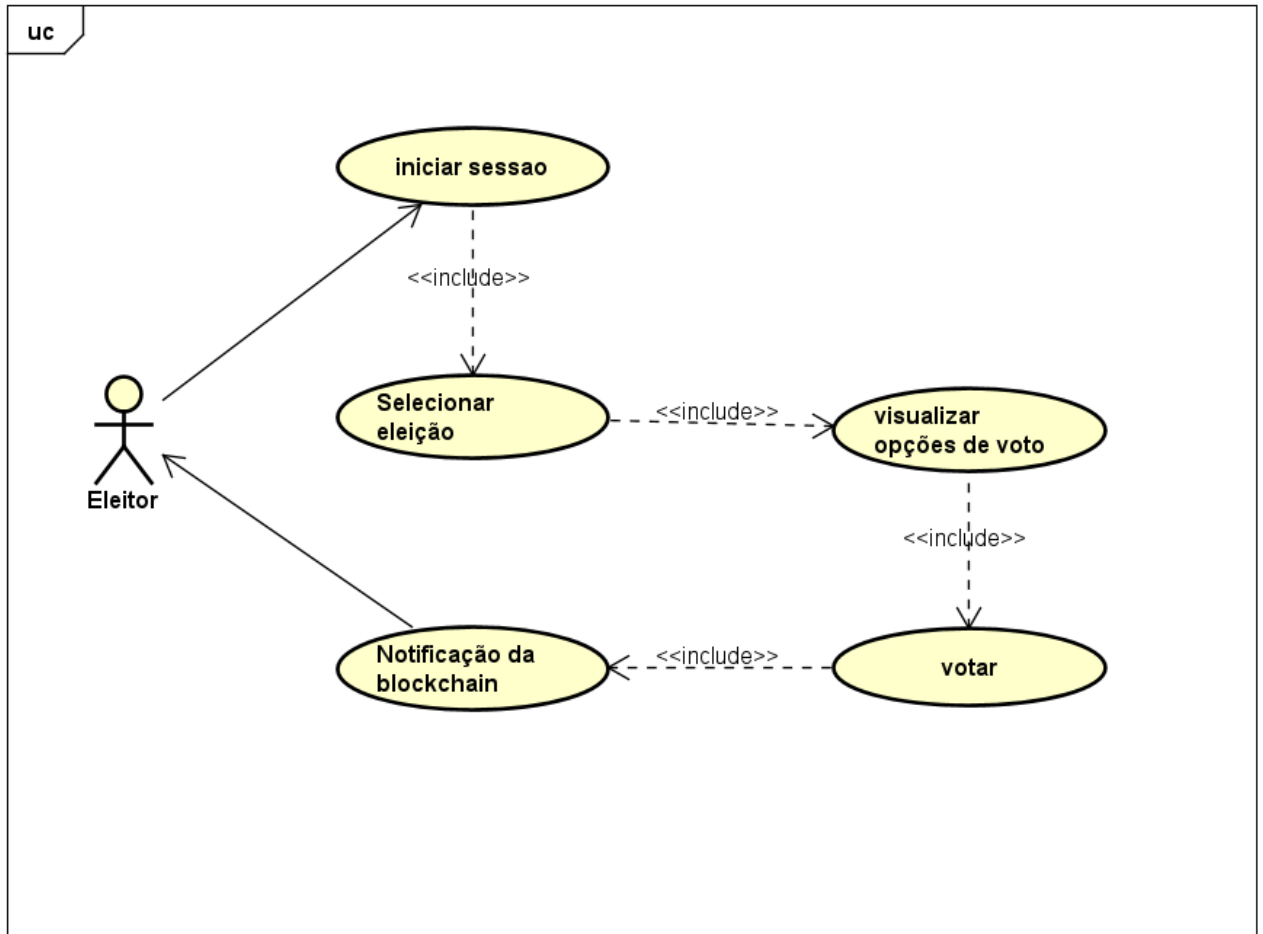


Figura 13: Diagrama De Caso De Uso Para o Processo De Votação. Autor (2024)

4.4.2.4. Diagrama de Caso de Uso para Visualização de resultados

O diagrama abaixo descreve a proposta de funcionamento para o processo de contagem e verificação de votos no sistema proposto.

Tabela 7: Diagrama de Caso de Uso para visualização resultados. Autor (2024)

CU01	Visualização Resultados
Utilizadores	Administrador, eleitor
Envolvidos	

Condições Prévias	O utilizador deve fazer o login no sistema
Descrição	O utilizador abre a tela de visualização de resultados escolhe a eleição que pretende ver os resultados e visualiza os resultados da eleição
Prioridade	Média
Relacionamento com Outros Casos	Relacionado à "Processo de votação".

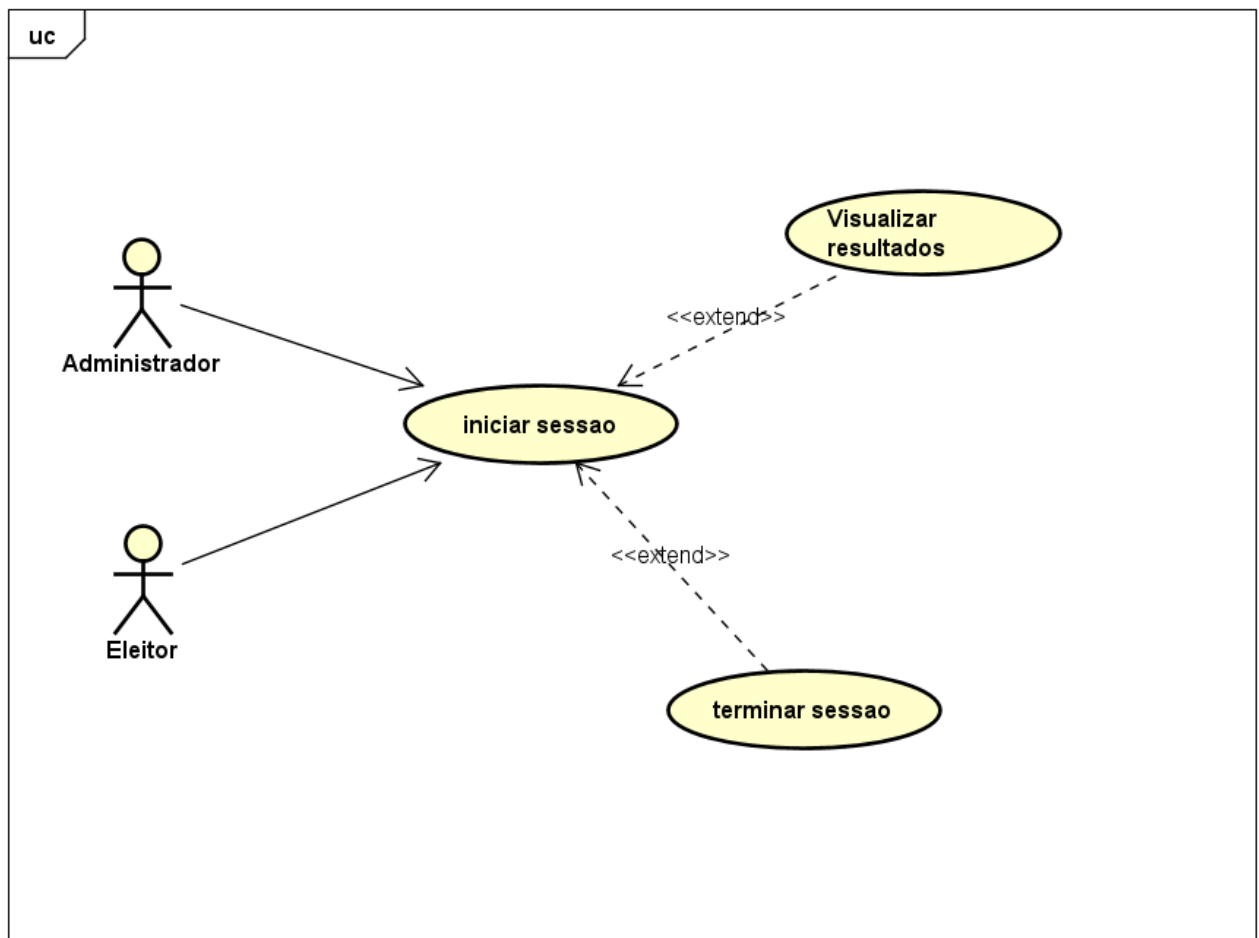


Figura 14: diagrama de Caso de Uso para Visualização de resultados. Autor (2024).

4.4.3. Diagramas de Sequência de Eventos

Um diagrama de sequência ilustra uma interação segundo uma visão temporal. Um diagrama de sequência é representado através de duas dimensões: a dimensão horizontal, que representa o conjunto de objectos intervenientes; e a dimensão vertical que representa o tempo. A apresentação destas dimensões pode ser invertida, se for conveniente. Não existe qualquer significado na ordenação horizontal dos objectos intervenientes, ou seja, na sua disposição relativa. (Silva & Videira, 2001)

4.4.3.1. Diagrama de seqüência de eventos para o registo de Administradores

O diagrama abaixo representa a seqüência de eventos durante o processo de registo de Administradores e eleitores.

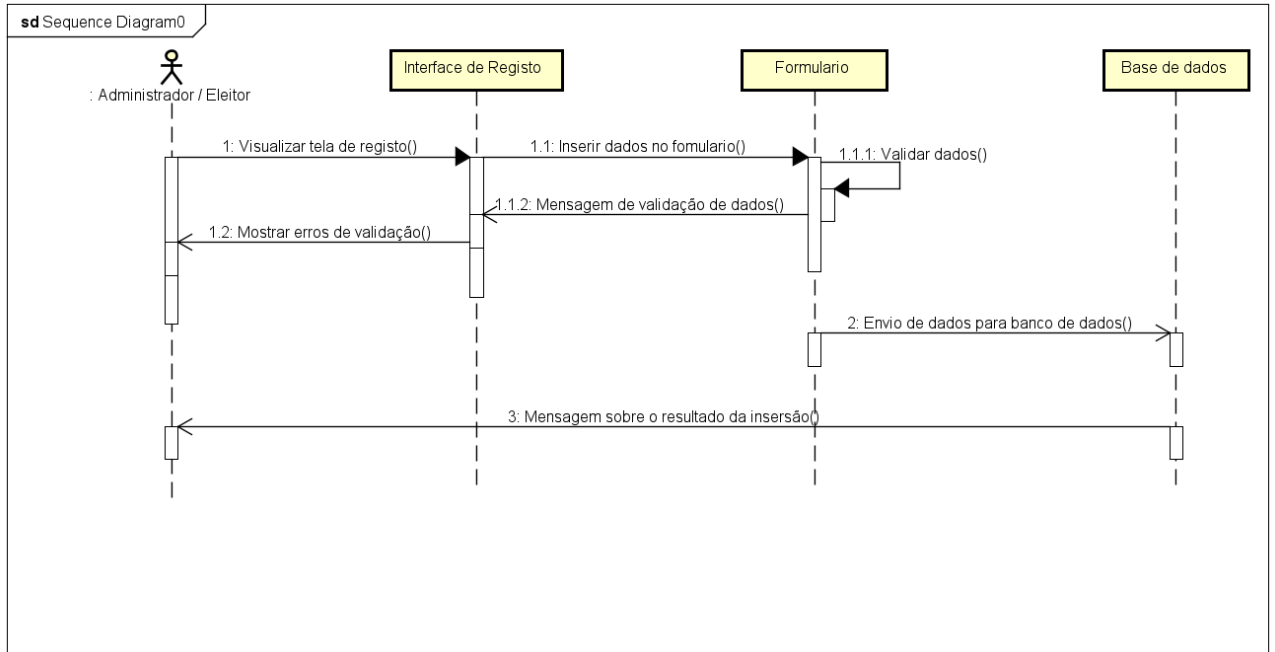


Figura 15: Diagrama de seqüência de eventos para o registo de Administradores e Eleitores, Autor (2024)

4.4.3.2. Diagrama de seqüência de eventos para a configuração de uma eleição

O diagrama abaixo representa a seqüência de eventos durante o processo de registo e configuração de uma eleição.

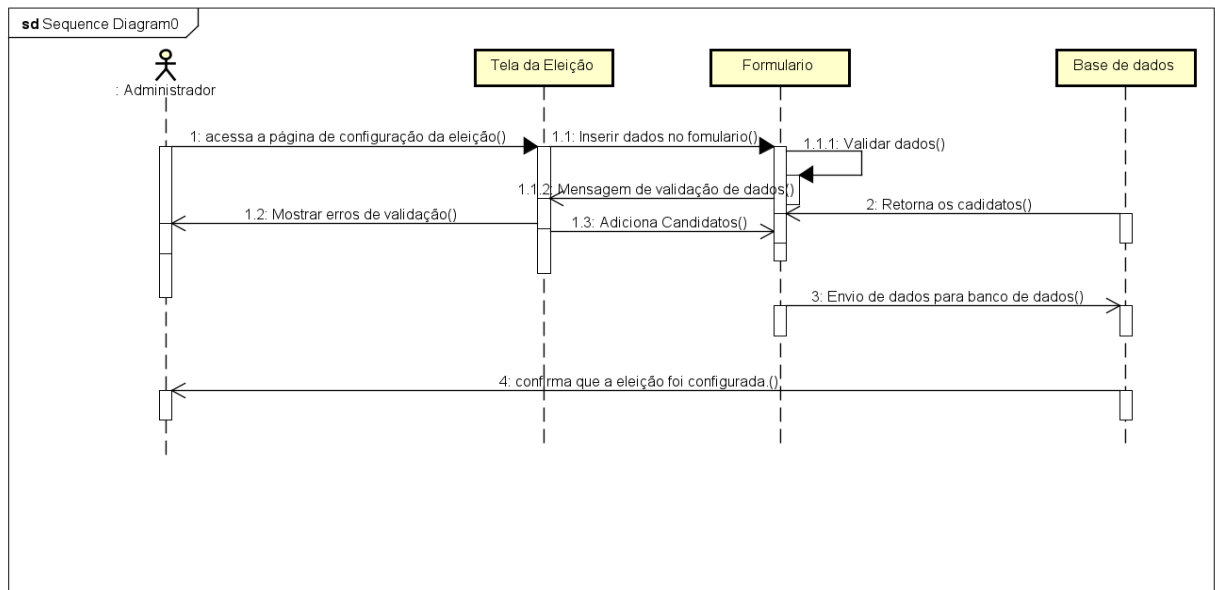


Figura 16: Diagrama de seqüência de eventos para a configuração de uma eleição, Autor (2024)

4.4.3.3. Diagrama de sequência de eventos para o processo de votação

O diagrama abaixo representa a sequência de eventos durante o processo de registo e configuração de uma eleição.

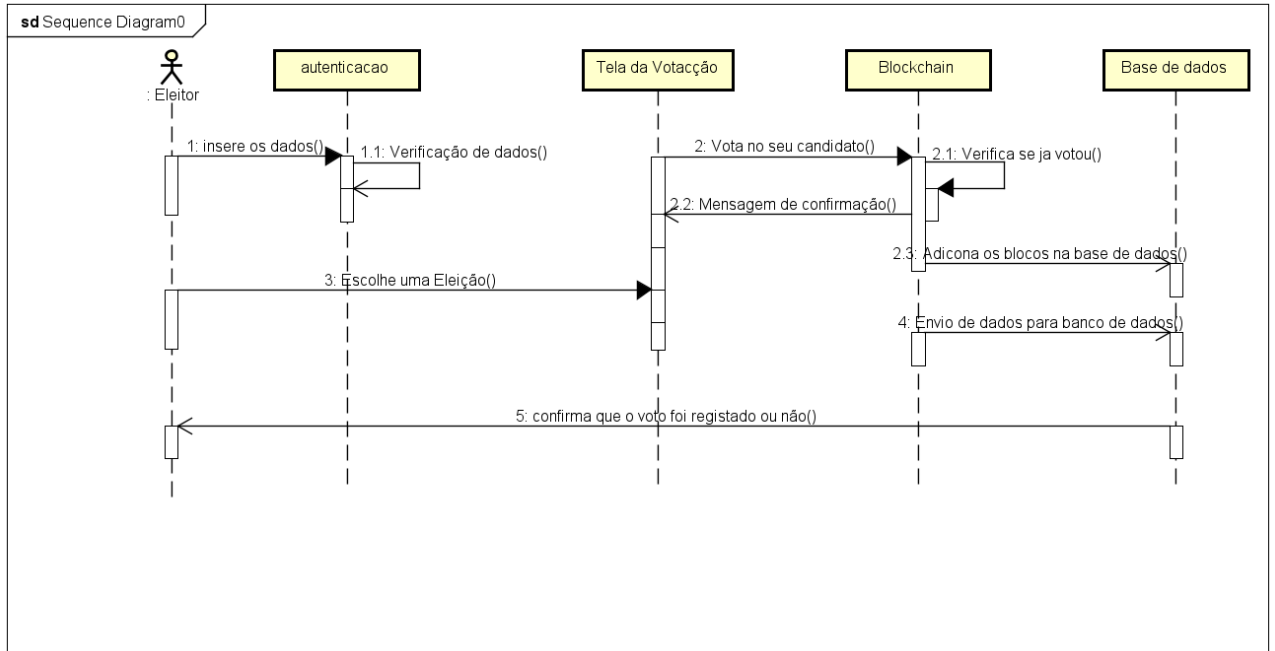


Figura 17: Diagrama de sequência de eventos para o processo de votação, Autor (2024)

4.4.3.4. Diagrama de sequência de eventos para a consulta dos resultados das eleições

O diagrama abaixo representa a sequência de eventos durante o processo de registo e configuração de uma eleição.

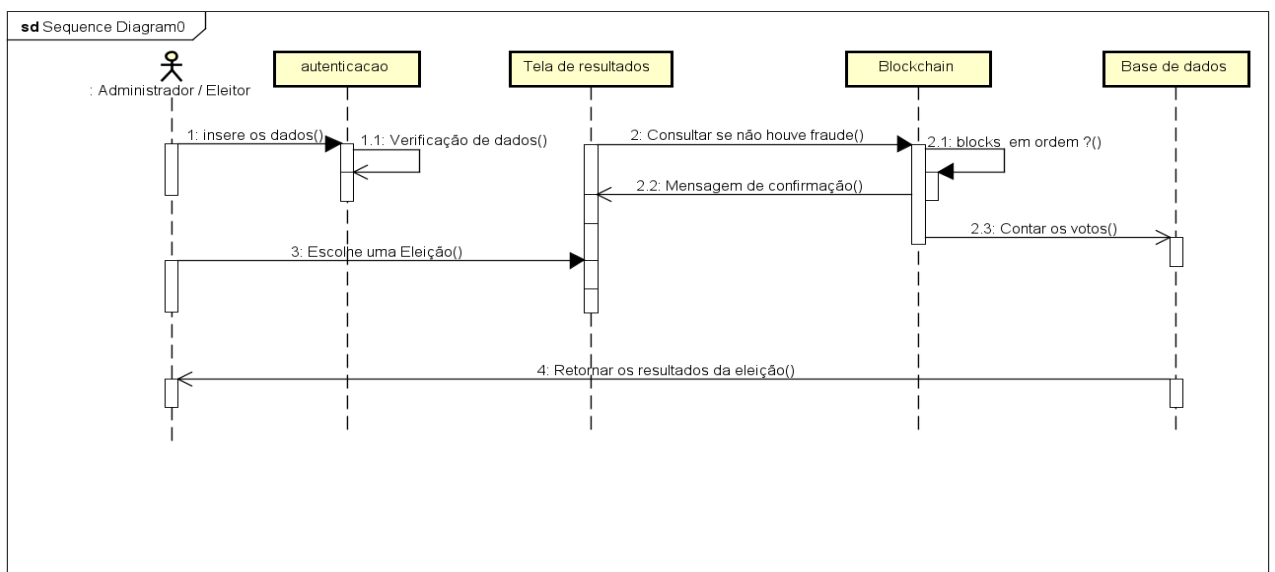


Figura 18: Diagrama de sequência de eventos para a consulta dos resultados das eleições, Autor (2024)

Conclusões e Recomendações

Neste capítulo, são apresentados as conclusões obtidas a partir do desenvolvimento do protótipo de um sistema de votação *online* baseado em tecnologia *Blockchain*. Serão discutidos os principais resultados e as implicações do projecto, além de sugestões para futuras implementações e melhorias. Conforme afirmam Creswell e Plano Clark (2011), "as conclusões não apenas resumem o que foi aprendido, mas também oferecem orientações práticas para a aplicação dos conhecimentos adquiridos." Portanto, este capítulo visa não só refletir sobre os achados da pesquisa, mas também contribuir para o aprimoramento de sistemas de votação *online*.

5.1 Conclusão

A implementação de um sistema de votação *online* baseado em tecnologia *Blockchain* representa um avanço significativo na busca por processos eleitorais mais seguros, transparentes e acessíveis. Este trabalho demonstrou que a utilização da *Blockchain* não apenas assegura a integridade dos votos, mas também promove a confiança dos eleitores no sistema eleitoral. Durante o desenvolvimento do sistema, foi possível observar a viabilidade técnica da solução proposta, evidenciando a capacidade da tecnologia de armazenar e registar dados de forma imutável e auditável, alcançando desse jeito os objetivos traçados no capítulo 1.

A pesquisa revelou que a segurança é um dos principais desafios enfrentados pelos sistemas de votação tradicionais. Casos de fraudes eleitorais, manipulação de resultados e vazamentos de dados têm gerado desconfiança nas instituições responsáveis pela condução das eleições. Nesse contexto, a utilização da tecnologia *Blockchain* oferece uma solução robusta, pois cada voto registrado se torna um bloco imutável, formando uma cadeia que não pode ser alterada sem o consenso da rede. Essa característica fortalece a integridade do processo eleitoral e proporciona maior segurança aos eleitores.

O sistema desenvolvido neste trabalho apresenta funcionalidades que facilitam o registo de eleitores, a configuração de eleições, a contagem de votos e a divulgação de resultados. A interface do sistema foi projectada para ser intuitiva, permitindo que eleitores de diferentes faixas etárias e níveis de familiaridade com tecnologia possam participar do processo eleitoral de forma tranquila e eficiente. Essa usabilidade é

fundamental para a democratização do acesso à informação e a promoção da participação cidadã, aspectos essenciais para qualquer sistema democrático.

5.1.1. Implicações da pesquisa

As implicações deste estudo vão além do desenvolvimento do sistema. Os resultados obtidos indicam que a aplicação da tecnologia *Blockchain* em sistemas de votação *online* pode contribuir significativamente para a modernização dos processos eleitorais. As organizações responsáveis pelas eleições devem considerar a adoção de tecnologias inovadoras que possam garantir a segurança e a transparência, características fundamentais para manter a legitimidade dos processos democráticos.

Além disso, a pesquisa destaca a importância de um ambiente regulatório favorável para a implementação de sistemas de votação *online*. Políticas públicas que incentivem a inovação tecnológica no setor eleitoral são essenciais para que soluções como a apresentada neste trabalho possam ser efectivamente adotadas. Os órgãos reguladores devem se engajar em discussões sobre como integrar essas tecnologias, garantindo que os direitos dos eleitores sejam preservados e que a privacidade das informações seja respeitada.

5.2 Recomendações para futuras implementações

Para que sistemas de votação *online* sejam amplamente aceitos, é necessário promover campanhas de educação e conscientização sobre a tecnologia *Blockchain* e suas vantagens. É importante desenvolver materiais educativos que expliquem de forma clara e acessível como a tecnologia funciona, destacando seus benefícios em termos de segurança, transparência e facilidade de uso. Workshops, e campanhas em mídias sociais podem ser eficazes para envolver os eleitores e garantir que eles se sintam confortáveis ao utilizar essas novas ferramentas. Embora a *Blockchain* utilize criptografia para garantir a segurança, seria recomendável adotar algoritmos de criptografia assimétrica mais robustos, como RSA ou Elliptic Curve Cryptography (ECC), para garantir que mesmo em casos de ataques futuros, os dados se mantenham invioláveis. Esses algoritmos são amplamente reconhecidos por sua resistência a ataques de força bruta e são utilizados em sistemas de segurança de alto nível.

Com o crescimento de utilizadores, o sistema de votação precisa ser capaz de lidar com um número crescente de eleitores e eleições simultâneas sem comprometer o desempenho.

5.2.1. Rede *Blockchain* Distribuída

Recomenda-se o uso de uma rede *Blockchain* distribuída, onde o armazenamento e o processamento dos blocos de transacção são distribuídos entre vários nós (servidores) para aumentar a escalabilidade. Isso pode ajudar a mitigar os problemas de desempenho que surgem quando há um grande volume de dados ou muitos eleitores participando simultaneamente.

Referências Bibliográficas

- Marconi, M. A., & Lakatos, E. M. (2003). Fundamentos de Metodologia Científica. São Paulo: Atlas.
- IBM (2018). *Blockchain* em: <https://www.ibm.com/br-pt/topics/blockchain>
- Nofer M., Gomber P., H. O. e. a. (2017). *Blockchain*. volume 59, pages 183–187.
- Gil, A. C. (2002). Métodos e Técnicas de Pesquisa Social. São Paulo: Atlas.
- Richardson, R. (1999). Qualitative Research Methods. London: Sage Publications.
- Schwaber, K., & Sutherland, J. (2017). The Scrum Guide. [Scrum.org](https://www.scrum.org/).
- Faculdade de ciencias – UEM, em: https://ciencias.uem.br/?page_id=10
- Welling, L., & Thomson, L. (2009). PHP and MySQL Web Development. Boston: Addison-Wesley.
- Stauffer, M. (2018). Laravel Up & Running. Beijing: O'Reilly Media.
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Disponível em: <https://bitcoin.org/bitcoin.pdf>
- Schoch, L. (2020). Figma: The Ultimate Guide. London: Packt Publishing.
- Silberschatz, A., Korth, H. F., & Sudarshan, S. (2011). Database System Concepts. New York: McGraw-Hill.
- Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography. Cham: Springer.
- Crampton, J. (2011). The role of *blockchain* technology in improving the security and transparency of voting systems. Journal of Information Security.
- Miller, A., & McCallum, K. (2017). End-to-end verifiable voting: A review. ACM Computing Surveys.
- Erl, T., & Puttini, R. (2016). Service-Oriented Architecture: Analysis and Design for Services and Microservices. Upper Saddle River: Prentice Hall.
- Agile Alliance. (2023). What is Agile? Agile Alliance. <https://www.agilealliance.org/agile101/what-is-agile/>
- Antunes, A. (2018). Sistemas de Votação Online: Segurança e Privacidade. Universidade de Coimbra. <https://estudogeral.sib.uc.pt/handle/10316/87500>
- Buterin, V. (2013). *A Next-Generation Smart Contract and Decentralized Application Platform*. Ethereum White Paper. <https://ethereum.org/en/whitepaper/>

Jr, L. H. L., & Batista, J. R. (2017). *Tecnologias Emergentes de *Blockchain* Aplicadas a Sistemas de Votação*. In *Revista de Tecnologias Emergentes* (Vol. 6, pp. 45-58).

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>

Ripple Labs Inc. (2014). The Ripple Protocol Consensus Algorithm. https://ripple.com/files/ripple_consensus_whitepaper.pdf

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media.

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*.

Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper. <https://ethereum.github.io/yellowpaper/paper.pdf>

Anexos

Anexo 1

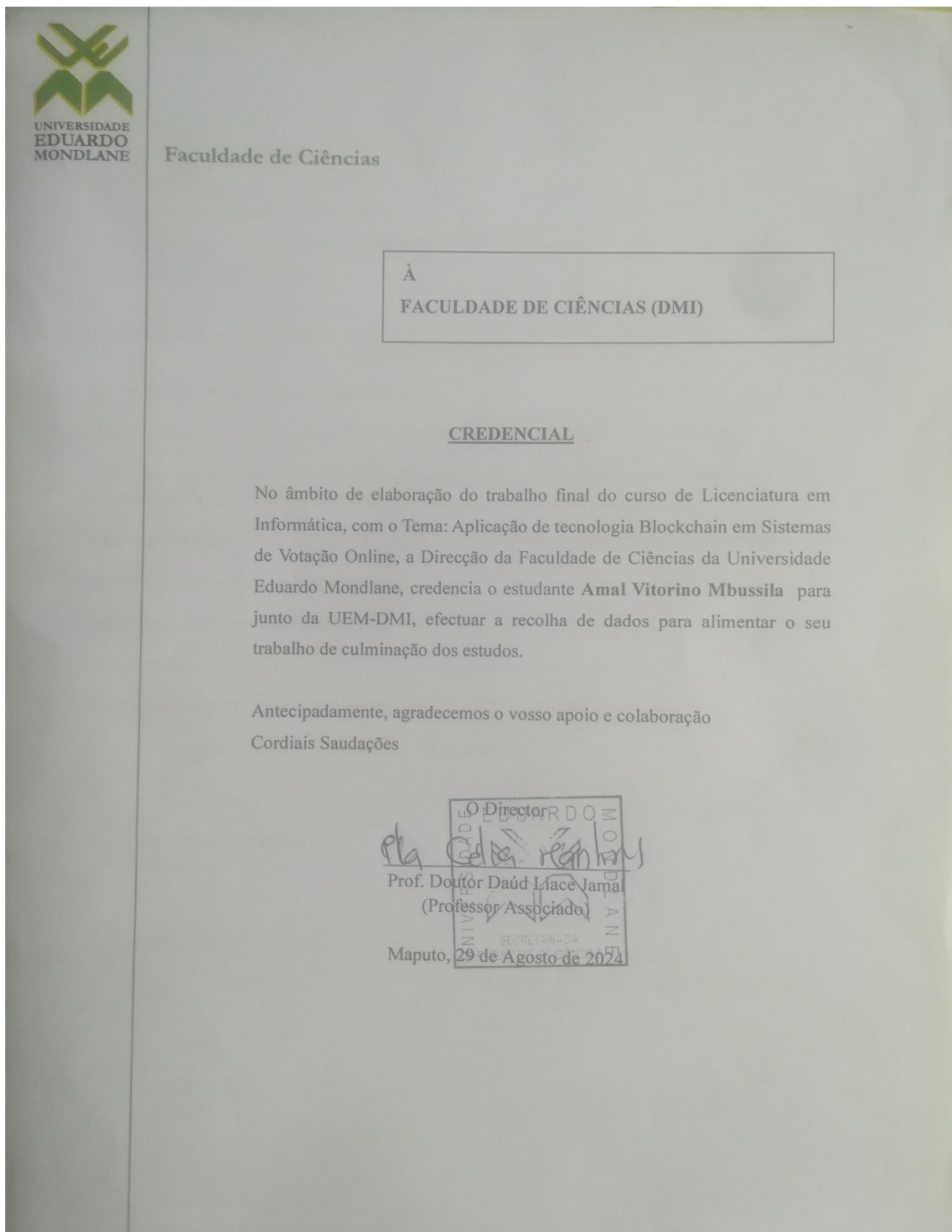


Figura 19: credencial

Apêndice 1:

Questionário de Entrevista

1. Informações Gerais

Nome: _____

Cargo Atual: _____

Período de Mandato: _____

2. Sobre o Núcleo dos Estudantes do DMI

2.2. Poderia nos dar uma breve descrição do que é o Núcleo dos Estudantes do DMI e quais são suas principais funções?

R: _____

3. Processo Eleitoral Atual

3.1. Como é organizado o processo de eleição para o presidente do núcleo? Pode descrever as etapas principais?

R: _____

3.2. Quem é responsável pela organização e supervisão das eleições?

R: _____

3.3. Quais são os critérios de elegibilidade para se candidatar a presidente do núcleo?

R: _____

3.4. Como os estudantes são informados sobre a eleição e como são realizadas as campanhas eleitorais?

R: _____

3.5. Quantos estudantes, em média, participam das eleições?

R: _____

4. Desafios e Problemas

4.1. Já houve registro de fraudes ou irregularidades durante as eleições do núcleo? Se sim, pode descrever o ocorrido?

R: _____

4.2. Quais são os principais desafios enfrentados durante a organização e a condução das eleições?

R: _____

Figura 20: questionário part1. Autor (2024)

4.3. Há alguma insatisfação entre os estudantes em relação ao processo eleitoral atual? Se sim, quais são as principais reclamações?

R: _____

5. Adoção de Tecnologias

5.1. O núcleo já considerou a adoção de tecnologias para modernizar o processo eleitoral? Se sim, quais foram discutidas?

R: _____

5.2. Como você acredita que a tecnologia poderia melhorar o processo eleitoral do núcleo?

R: _____

5.3. Você vê alguma barreira significativa para a implementação de um sistema de votação online no núcleo? Quais seriam essas barreiras?

R: _____

6. Expectativas e Recomendação

6.1. Quais são as suas expectativas em relação à modernização do processo eleitoral do núcleo?

R: _____

6.2. Você tem alguma recomendação ou sugestão para garantir que um novo sistema de votação seja aceito e eficaz entre os estudantes?

R: _____

Obrigado pela atenção!!

(Amal Vitorino Mbussila)

Figura 21: questionário part 2. Autor (2024)

Apêndices



Figura 22: página de login no mobile. Autor (2024)

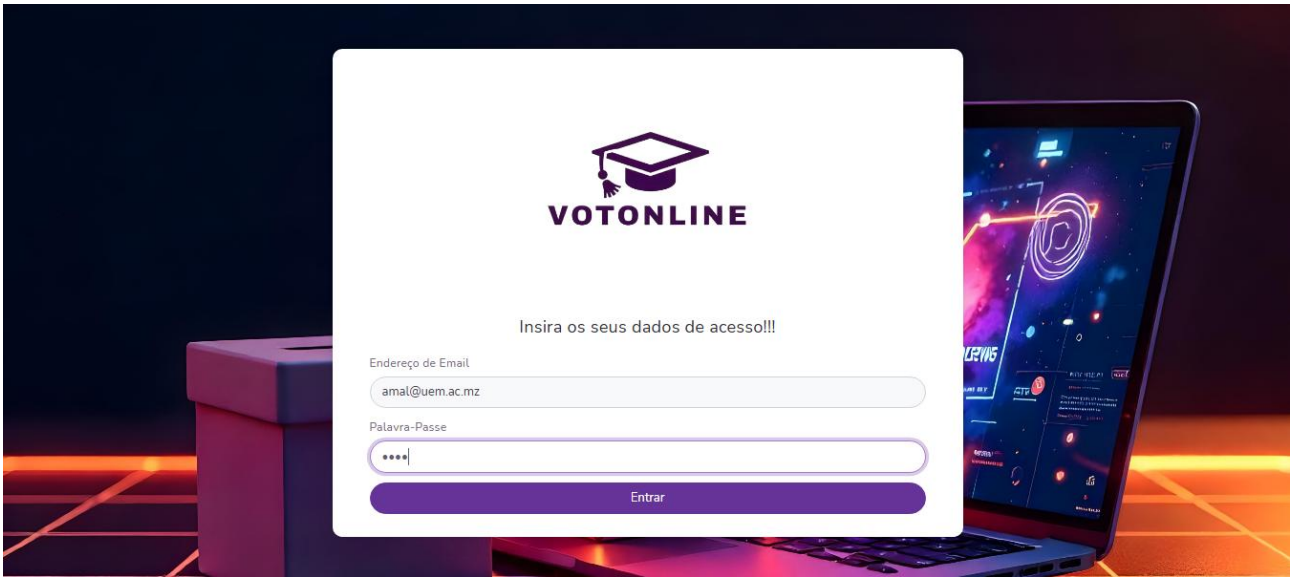



Figura 23: Página de login no computador. Autor (2024)

Registrar Novo Candidato

Nome:

Manifesto:

Imagem: arashmil.jpg

Preview: 

Lista de Candidatos

Show entries

NOME	IMAGEM	MANIFESTO	AÇÕES
Amidee	—	Me vota	<input type="button" value="Editar"/> <input type="button" value="Apagar"/>
Dadiva	—	Vou Melhrar Tudo	<input type="button" value="Editar"/> <input type="button" value="Apagar"/>

Figura 24: tela de registo do candidato. Autor (2024)

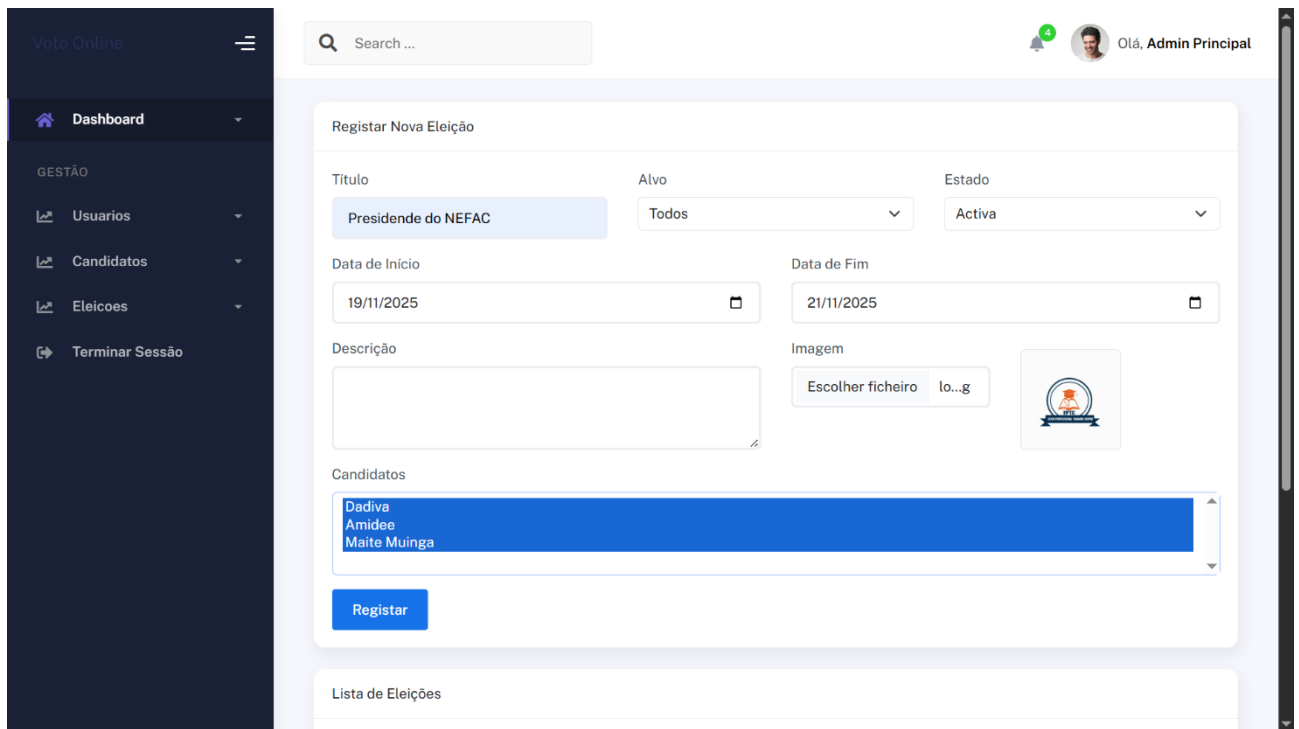


Figura 25: Tela para registo e configuração da eleição. Autor (2024)

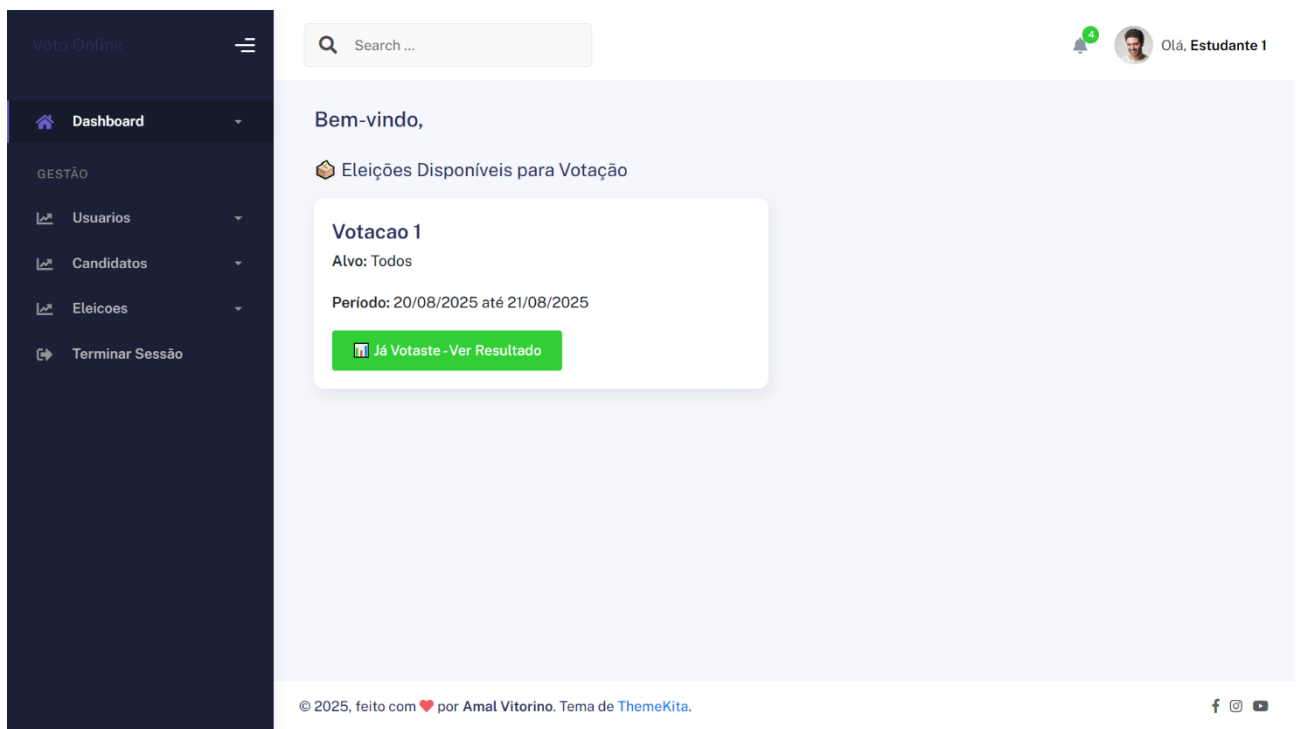


Figura 26: Tela para visualização de eleições para voto. Autor (2024)

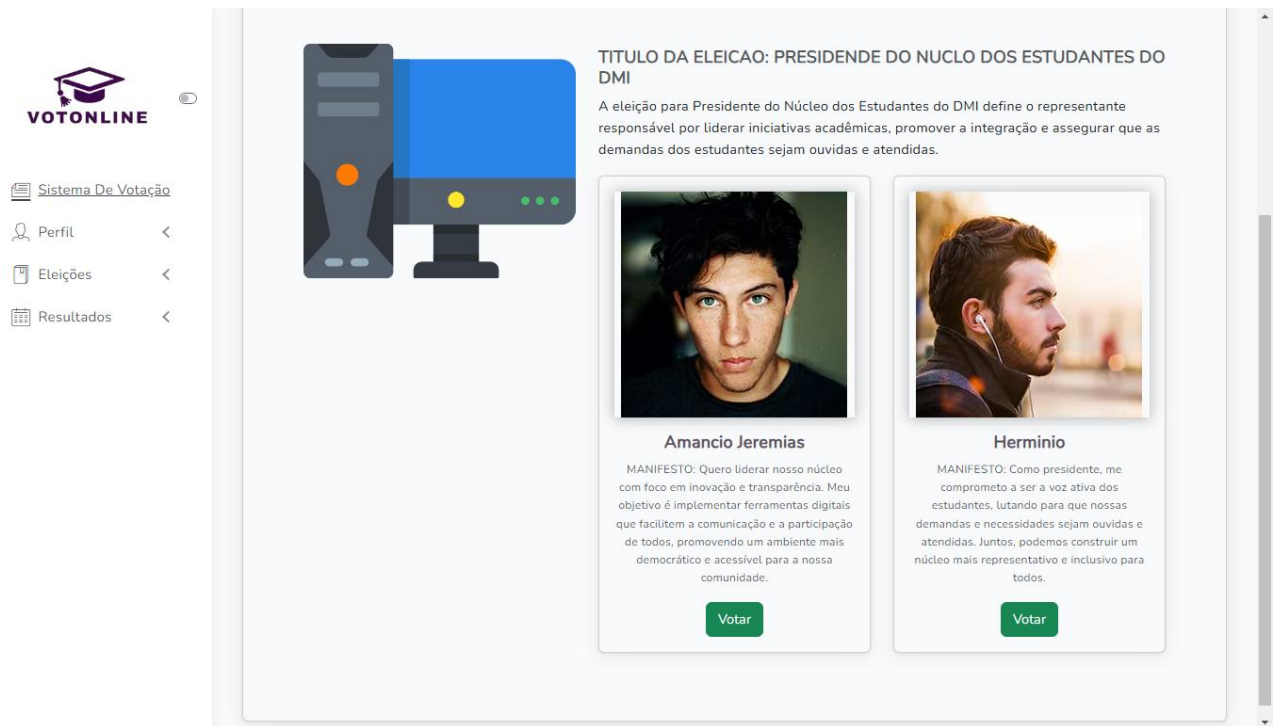


Figura 27: tela para votar no candidato escolhido. Autor (2024)

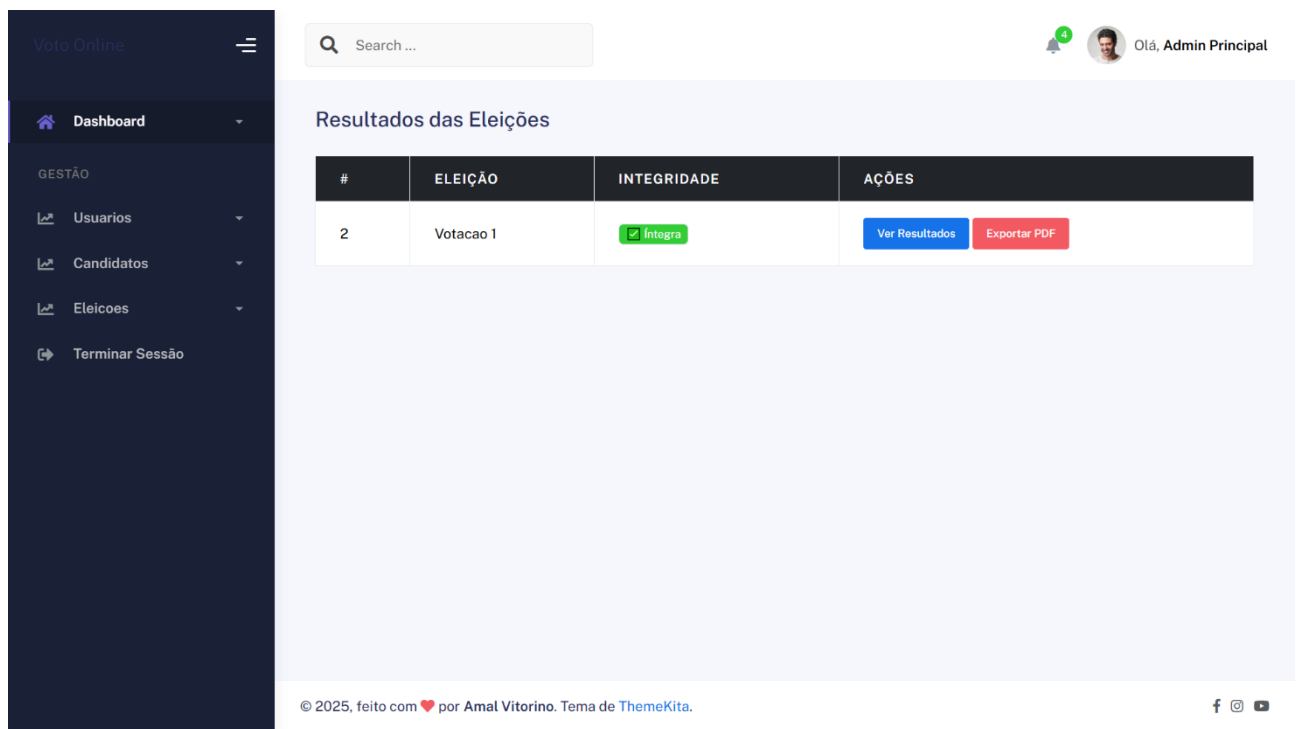


Figura 28: Tela para selecionar a eleição para ver resultados. Autor (2024)

VOTONLINE

Sistema.De.Votação

Perfil <

Eleições <

Resultados <

VotOnline - Eleições | NEFAC

Resultados da Eleição: Presidente do núcleo dos estudantes do DMI

Candidato	Manifesto	Votos
Amancio Jeremias	Quero liderar nosso núcleo com foco em inovação e transparência. Meu objetivo é implementar ferramentas digitais que facilitem a comunicação e a participação de todos, promovendo um ambiente mais democrático e acessível para a nossa comunidade.	1
Herminio	Como presidente, me comprometo a ser a voz ativa dos estudantes, lutando para que nossas demandas e necessidades sejam ouvidas e atendidas. Juntos, podemos construir um núcleo mais representativo e inclusivo para todos.	0

Figura 29: Tela para Visualizar os resultados. Autor (2024)