UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Desenvolvimento de um Sistema de Votação Electrónica Baseado em Blockchain para o Núcleo de Estudantes de Direito da UEM

Autor:

Saiete, Luís Titos

Supervisor:

Mestre Rúben Moisés Manhiça, Eng.º

Maputo, Julho de 2025

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Desenvolvimento de um Sistema de Votação Electrónica Baseado em Blockchain para o Núcleo de Estudantes de Direito da UEM

Autor:

Saiete, Luís Titos

Supervisor:

Mestre Rúben Moisés Manhiça, Eng.º

Maputo, Julho de 2025

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

TERMO DE ENTREGA DO RELATÓRIO DE TRABALHO DE LICENCIATURA

Declaro que o estudante **Luís Titos Saiete** entregou no dia 07/07/2025, as 03 cópias do relatório do seu Trabalho de Licenciatura com referência _____, intitulado: Desenvolvimento de um Sistema de Votação Electrónica Baseado em Blockchain para o Núcleo de Estudantes de Direito da UEM.

Maputo, 07 de Julho de 2025

O Chefe da Secretaria

_____

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

DECLARAÇÃO DE HONRA

Declaro sob compromisso de honra que o presente trabalho é resultado da minha investigação e que foi concebido para ser submetido apenas para a obtenção do grau de Licenciatura em Engenharia Informática na Faculdade de Engenharia da Universidade Eduardo Mondlane.

Maputo, 07 de Julho de 2025

O Autor

_____

(Luís Titos Saiete)

Dedicatória

Dedico este trabalho à minha mãe, Fátima Biosse,
ao meu pai, Titos Saiete,
à minha esposa, Shelsia, ao meu filho, Yuken,
aos meus irmãos, Wesley e Yazmira e
à minha tia, Angelica, que luta contra o câncer
enquanto escrevo este trabalho.

Agradecimentos

A Deus, por ter permitido que eu tivesse saúde e determinação para não desanimar ao longo do curso.

Agradecer aos meus pais Titos Saiete e Fátima Biosse, por me apoiarem e me ajudarem a manter o foco no âmbito académico.

À minha esposa e ao meu filho por me permitirem manter a lâmpada do quarto acesa durante várias noites enquanto escrevia este trabalho.

Aos meus irmãos, primos e tios, por me apoiarem tanto nos bons momentos como também nos maus momentos.

Um agradecimento especial ao Eng.º Rúben Manhiça por apoiar e supervisionar a realização deste trabalho e pelo suporte na minha vida profissional.

Aos docentes do curso, aos engenheiros Délcio Chadreca, Leila Omar, Ivone Cipriano e Felizardo Munguambe e aos Mestres Vali Issufo, Sérgio Mavie, Alfredo Covele e Bhavika Rugnath, que durante esta jornada, partilharam a sua experiência e conhecimento no âmbito académico e profissional.

Ao meu mentor, Frederico Zile, que me apoiou com suas ideias desde antes de entrar na faculdade e durante esta jornada.

Ao Henrique e Ervin pelo suporte técnico na realização e revisão deste trabalho.

Ao Luis Milice, que desenhou a UI que serviu de base para a UI do protótipo desenvolvido neste trabalho.

Aos meus colegas, que representam um papel importante nesta jornada, pois sem eles, não conseguiria chegar até aqui, em especial ao Ussumane, Airo, Nunes, Muendane, Beatriz, Ana, Constâncio e Nélio que se tornaram amigos com quem partilho experiências fora do âmbito académico.

Aos meus amigos, em especial ao Imo, os meus agradecimentos pelo apoio durante esta jornada.

À team do GDSC 2021/2022, em especial ao Henrique, à Neima e ao Lourenço, por ajudarem a criar experiências que permitiram que várias pessoas (inclusive eu) pudessem aprender e partilhar muita coisa alem do que a faculdade tem para ensinar.

Epígrafe

“Não é aquele que se torna Hokage
que é reconhecido pela vila.
É aquele que é reconhecido pela vila
que se torna Hokage.” – Itachi Uchiha,
em Naruto Shippuden

Resumo

Na Universidade Eduardo Mondlane (UEM), os núcleos estudantis desempenham um papel fundamental na representação dos estudantes, sendo as suas eleições parte importante da vivência democrática no contexto académico. No entanto, esses processos eleitorais têm enfrentado desafios ligados à organização, transparência e confiança dos participantes. Diante desse cenário, este trabalho propõe o desenvolvimento de um protótipo de sistema de votação electrónica baseado em blockchain, tendo como caso de estudo o Núcleo de Estudantes de Direito da Universidade Eduardo Mondlane (NED). A proposta visa demonstrar como a tecnologia blockchain, inicialmente concebida para o setor financeiro, pode ser aplicada à modernização dos processos eleitorais, garantindo maior transparência, segurança e auditabilidade. Para atingir esse objectivo, foram definidos como objectivos descrever o processo eleitoral actual do NED, apresentar os principais conceitos e técnicas de blockchain aplicáveis à votação, e desenvolver um protótipo funcional que demonstre a viabilidade técnica e os benefícios da aplicação da blockchain em processos eleitorais. A pesquisa adoptou uma abordagem metodológica mista, combinando revisão bibliográfica e documental com entrevistas e inquéritos direcionados à comunidade estudantil do NED. O desenvolvimento do sistema seguiu o modelo em cascata e resultou numa aplicação web integrada à plataforma Ethereum, com uso de contractos inteligentes para gerir os principais eventos do processo eleitoral. Os resultados obtidos sugerem que a adopção da blockchain em contextos eleitorais pode fortalecer a integridade dos processos democráticos, mesmo em ambientes com infraestrutura limitada e baixa confiança institucional. Além disso, o trabalho abre caminho para futuras pesquisas e aprimoramentos voltados à implementação gradual de sistemas de votação electrónica baseados em tecnologias emergentes.

Palavras-chave: Blockchain, Votação Electrónica, Ethereum, contractos inteligentes.

Abstract

At Eduardo Mondlane University (UEM), the student nuclei play a fundamental role in student representation, and their elections are an important part of the democratic experience in the academic context. However, these electoral processes have been facing challenges related to organization, transparency and the trust of participants. Given this scenario, this paper proposes the development of a blockchain based electronic voting system prototype, with the Eduardo Mondlane University Law Students Nucleus (NED) as a case study. The proposal aims to demonstrate how blockchain technology, initially conceived for the financial sector, can be applied to the modernization of electoral processes, ensuring greater transparency, security and auditability. To achieve this, the goals were to describe the current electoral process at NED, present the main blockchain concepts and techniques applicable to voting, and develop a functional prototype that demonstrates the technical viability and benefits of applying blockchain to electoral processes. The research adopted a mixed methodological approach, combining a literature and document review with interviews aimed at the NED student community. The development of the system followed the cascade model and resulted in a web application integrated with the Ethereum platform, using smart contracts to manage the main events of the electoral process. The obtained results suggest that the adoption of blockchain in electoral contexts can strengthen the integrity of democratic processes, even in environments with limited infrastructure and low institutional trust. In addition, the work paves the way for future research and improvements aimed at the gradual implementation of electronic voting systems based on emerging technologies.

Keywords: Blockchain, Electronic Voting, Ethereum, smart contracts.

Índice

Lista de abreviaturas e acrónimos

ABI	Application Binary Interface
DApps	Decentralized Applications
DLT	Distributed Ledger Technology
DoS	Denial-of-Service
DRE	Direct Recording Electronic
EBP	Electronic Ballot Printers
EVM	Electronic Voting Machine
EVM	Ethereum Virtual Machine
IEBC	Independent Electoral and Boundaries Commission
International IDEA	International Institute for Democracy and Electoral Assistance
IoT	Internet of Things
KIEMS	Kenya Integrated Electoral Management System
NED	Núcleo de Estudantes de Direito
OCR	Optical character recognition
OMR	Optical Mark Recognition
P2P	Peer-to-Peer
PCOS	Precinct Count Optical Scan
PIN	Personal Identification Number
PoS	Proof of Stake
PoW	Proof of Work
SHA-256	Secure Hash Algorithm 256-bit
VVPAT	Voter-Verified Paper Audit Trail

Glossário de termos

Append-only	Tipo de estrutura de dados onde novas informações podem apenas ser adicionadas, sem a possibilidade de alterar ou remover dados previamente armazenados.
Criptografia	Conjunto de técnicas utilizadas para proteger dados, assegurando confidencialidade, autenticidade e integridade da informação.
Deploy	Processo de disponibilização de uma aplicação ou sistema em um ambiente de produção ou servidor, tornando-o acessível para os utilizadores finais. Envolve etapas como configuração do ambiente, envio dos arquivos da aplicação, e ativação dos serviços necessários para seu funcionamento.
Digest	Resumo criptográfico gerado a partir de uma entrada de dados, geralmente através de uma função hash.
Framework	Conjunto estruturado de ferramentas, bibliotecas e componentes reutilizáveis que fornece a base para o desenvolvimento de aplicações de software.
Hackers	Indivíduos com conhecimento avançado em sistemas computacionais, podendo usá-lo tanto para fins éticos quanto para atividades maliciosas, como invasão de sistemas e roubo de dados.
Hash	Função criptográfica que transforma uma entrada de qualquer tamanho em uma sequência fixa de caracteres.
Ledger	Livro-razão digital onde são armazenadas as transações de forma segura, transparente e imutável.
Middleware	Camada intermediária de software que conecta diferentes partes de um sistema.
Nós	Dispositivos ou computadores conectados a uma rede blockchain, responsáveis por validar, armazenar e propagar transações e blocos.
Peer-to-peer	Um tipo de rede em que cada computador, ou “ponto”, actua como cliente e servidor, comunicando diretamente e partilhando recursos com outros pontos sem depender de um servidor central.
Testnets	Redes de teste utilizadas para simular e experimentar funcionalidades da blockchain sem o uso de criptomoedas reais.

Timestamp	Marca temporal associada a um evento digital, como uma transação.
White paper	Documento técnico que descreve detalhadamente os objetivos, funcionamento e arquitetura de uma tecnologia ou projecto.

Lista de figuras

Lista de tabelas

Lista de tabelas

1. Capítulo I – Introdução

1.1. Contextualização

Na Universidade Eduardo Mondlane (UEM), os núcleos estudantis desempenham um papel central na representação académica e na articulação de interesses dos estudantes junto às direcções das faculdades. Esses núcleos realizam eleições periódicas para eleger os seus órgãos dirigentes, num exercício de cidadania que procura replicar, em escala académica, os princípios democráticos que regem a sociedade moçambicana. No entanto, essas eleições, como ocorre também no contexto nacional, enfrentam desafios relacionados à organização, transparência e confiança dos participantes. Casos de abstenção de eleitores e limitações logísticas são recorrentes e contribuem para o descrédito dos processos eleitorais mesmo dentro do ambiente universitário.

Em Moçambique, de forma mais ampla, o processo eleitoral é um pilar fundamental da democracia, permitindo que os cidadãos escolham seus representantes políticos e participem ativamente na construção de um futuro mais justo. No entanto, desde sempre, esse processo tem enfrentado desafios críticos que comprometem sua credibilidade. A crescente desconfiança da população, aliada a altos índices de abstenção e episódios recorrentes de fraude e violência, reflecte uma crise democrática profunda. Entre 1990 e a década de 2000, a participação eleitoral caiu drasticamente de 80% para 45% (Silva, 2016), evidenciando não apenas o desinteresse popular, mas também falhas estruturais, como recenseamento inadequado e suspeitas de manipulação nos resultados.

Diante desse cenário, a busca por soluções tecnológicas inovadoras torna-se urgente. Nesse contexto, destaca-se a tecnologia blockchain, originalmente desenvolvida para o sector financeiro, mas que hoje se expande para áreas como saúde, gestão de terras, identidade digital e, sobretudo, votação electrónica (Dong et al., 2023). Suas características únicas como a imutabilidade, transparência e descentralização, oferecem respostas concretas aos problemas de integridade e confiança que assolam os sistemas eleitorais tradicionais.

A experiência internacional comprova seu potencial. Na Estônia, a blockchain é utilizada desde 2005 em serviços públicos, incluindo votação electrónica, garantindo segurança e participação dos cidadãos (Osula, 2019). No Japão, testes em Tsukuba, em 2018, demonstraram como a tecnologia pode minimizar fraudes, permitindo que eleitores

votassem digitalmente com um cartão de identificação único (Birch, 2018). Esses casos mostram que a blockchain não apenas moderniza processos, mas também restaura a confiança nas instituições.

Para Moçambique, onde os conflitos pós-eleitorais e a deslegitimação dos resultados são frequentes, a adopção dessa tecnologia representa uma oportunidade estratégica. Este trabalho propõe o desenvolvimento de um protótipo de votação baseado em blockchain para o Núcleo de Estudantes de Direito da Universidade Eduardo Mondlane (UEM), visando criar um modelo piloto que demonstre o potencial desta tecnologia para processos eleitorais. A escolha deste contexto acadêmico permite testar a solução em um ambiente controlado, com possibilidade de replicação em outras organizações estudantis e, eventualmente, em escalas maiores.

1.2. Justificativa

O presente trabalho parte da necessidade concreta de modernizar o processo eleitoral do Núcleo de Estudantes de Direito da Universidade Eduardo Mondlane (NED), cujas eleições têm sido marcadas por desafios operacionais como filas longas, dispersão geográfica dos eleitores e dificuldades logísticas que comprometem a eficiência e a confiança no processo. Ao propor uma solução baseada em tecnologia blockchain, este projecto visa garantir maior transparência, segurança e verificabilidade dos votos, proporcionando um ambiente mais confiável e acessível para a participação dos estudantes.

Essa iniciativa local serve como um modelo piloto para validar e demonstrar a eficácia de uma solução tecnológica para processos eleitorais que pode ser replicada em contextos mais amplos. A escalabilidade da solução é uma de suas maiores virtudes: embora desenhado para o NED, o sistema poderá ser adaptado para eleições universitárias em outras faculdades, eleições estudantis nacionais e até mesmo para pleitos municipais ou gerais. Trata-se de um protótipo estratégico que oferece evidências sobre como a tecnologia pode ser utilizada para fortalecer a integridade dos processos eleitorais em Moçambique.

A nível nacional, a proposta torna-se ainda mais relevante diante do cenário recorrente de contestação eleitoral, alegações de fraude e desconfiança entre os actores políticos e a população. A introdução de mecanismos imutáveis e auditáveis de registo de votos, como os proporcionados pelo blockchain, tem o potencial de restaurar a confiança pública e promover eleições mais transparentes. Isso contribui diretamente para a consolidação da

democracia, combatendo o abstencionismo e incentivando a participação cívica, sobretudo entre os jovens.

Ao mesmo tempo, a proposta alinha Moçambique às tendências internacionais de modernização dos processos eleitorais, inspirando-se em experiências bem-sucedidas de países como a Estônia, Coreia do Sul, Quénia e Marrocos, que adoptaram soluções digitais seguras para aumentar a confiança e a eficiência nas suas eleições. O uso da tecnologia blockchain, ao garantir a integridade do voto e a possibilidade de verificação individual sem comprometer o anonimato, apresenta-se como uma resposta concreta às exigências contemporâneas por equidade, transparência e responsabilidade institucional.

Assim, a motivação deste trabalho está enraizada em um problema real e actual do contexto universitário, mas com repercussões que transcendem os muros da academia, contribuindo para o debate e a construção de alternativas tecnológicas que sirvam ao fortalecimento da democracia moçambicana.

1.3. Objetivos

1.3.1. Objetivo Geral

Propor um sistema de votação electrónica baseado em Blockchain para o Núcleo de Estudantes de Direito da UEM, que assegure a integridade, transparência e segurança do processo eleitoral, proporcionando um ambiente de votação confiável e acessível para todos os eleitores.

1.3.2. Objetivos Específicos

- Descrever o processo eleitoral actual do Núcleo de Estudantes de Direito.
- Apresentar os principais conceitos associados ao blockchain e como estes poderão ajudar na garantia da integridade e transparência do processo de votação.
- Identificar as principais técnicas de blockchain aplicáveis a sistemas de votação e sua eficácia em termos de segurança, transparência e usabilidade.
- Desenvolver e validar um protótipo funcional do sistema com base nas principais técnicas blockchain aplicáveis a sistemas de votação.

1.4. Metodologia

Marconi e Lakatos (2003, p. 83) definem o método de pesquisa como sendo "o conjunto das actividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objectivo, conhecimentos válidos e verdadeiros, traçando o caminho a ser seguido, detectando erros e auxiliando as decisões do cientista." A presente secção visa apresentar as técnicas e etapas utilizadas para alcançar o objectivo do trabalho, desde a investigação teórica até o desenvolvimento e validação do protótipo de um sistema de votação electrónica baseado em blockchain.

1.4.1. Classificação da metodologia de trabalho

Para o alcance dos objectivos estabelecidos neste trabalho, a metodologia adoptada é classificada com base nos critérios propostos por Gerhardt e Silveira (2009), que incluem: (a) a abordagem, (b) a natureza, (c) os objetivos e (d) os procedimentos. A seguir, detalha-se como o presente trabalho se enquadra em cada um desses critérios.

a) Quanto à abordagem

De acordo com Gerhardt e Silveira (2009), a pesquisa pode ser classificada em três abordagens principais: qualitativa, quantitativa ou mista. Cada uma dessas abordagens possui características distintas, que as tornam adequadas para diferentes tipos de investigação.

A pesquisa qualitativa caracteriza-se por priorizar a compreensão aprofundada de grupos sociais, organizações ou fenômenos complexos, sem focar em representatividade numérica. Nesse contexto, os pesquisadores qualitativos buscam explicar as razões subjacentes aos fenômenos sociais, explorando "o porquê das coisas" por meio de dados não-métricos, como interações simbólicas e narrativas, em vez de quantificações (Gerhardt & Silveira, 2009). Essa abordagem é particularmente útil para investigar contextos específicos, como as dinâmicas sociais e as percepções dos eleitores no processo eleitoral do Núcleo de Estudantes de Direito da UEM (NED).

b) Quanto a natureza

De acordo com Gerhardt e Silveira (2009), a pesquisa pode ser classificada quanto à natureza em básica ou aplicada. A pesquisa aplicada visa gerar conhecimentos

direcionados à solução de problemas específicos, com foco em aplicações práticas e interesses locais.

No presente trabalho, adoptou-se a pesquisa aplicada, uma vez que o objectivo principal é desenvolver uma solução prática para um problema real enfrentado pelo NED. A pesquisa aplicada é particularmente adequada para este estudo, pois busca não apenas compreender os desafios do processo eleitoral actual, mas também propor e validar uma solução tecnológica que possa ser implementada e replicada em outros contextos.

c) Quanto aos objetivos

Gil (2002) classifica as pesquisas, quanto aos objetivos, em três tipos principais: exploratórias, descritivas e explicativas.

Pesquisas exploratórias têm como objectivo proporcionar maior familiaridade com o problema, tornando-o mais explícito ou permitindo a construção de hipóteses enquanto pesquisas descritivas buscam descrever as características de uma população, fenômeno ou estabelecer relações entre variáveis.

No presente trabalho, adopta-se uma abordagem exploratória e descritiva. A fase exploratória foi essencial para familiarizar-se com o tema, investigando os conceitos teóricos relacionados à votação electrónica e à tecnologia blockchain, bem como para analisar o processo eleitoral actual do NED. Já a fase descritiva será aplicada para descrever as características do protótipo desenvolvido, estabelecendo relações entre as técnicas de blockchain e os requisitos do sistema de votação electrónica.

d) Quanto aos procedimentos

Quanto aos procedimentos, a metodologia utilizada no presente trabalho é classificada como pesquisa bibliográfica, pesquisa documental e estudo de caso.

- **Pesquisa Bibliográfica:**

Segundo Fonseca (2002), a pesquisa bibliográfica é realizada a partir do levantamento de referências teóricas já analisadas e publicadas em meios escritos e electrónicos, como livros, artigos científicos e páginas de websites. No presente trabalho, a pesquisa bibliográfica foi essencial para embasar teoricamente o estudo, permitindo a revisão de

conceitos relacionados à votação electrónica, à tecnologia blockchain e às técnicas aplicáveis ao desenvolvimento de sistemas seguros e transparentes.

- **Pesquisa Documental:**

De acordo com Gil (2002), a pesquisa documental é desenvolvida com base em materiais que não receberam tratamento analítico prévio ou que podem ser reelaborados de acordo com os objetivos da pesquisa. Neste trabalho, foram analisados documentos relacionados ao processo eleitoral do NED, como regulamentos internos, atas de reuniões e relatórios de eleições anteriores. Essa abordagem complementou o estudo de caso, fornecendo dados concretos sobre o contexto em que o protótipo será aplicado.

- **Estudo de Caso:**

De acordo com Gil (2002), o estudo de caso consiste na análise profunda e detalhada de um ou poucos objetos, com o objectivo de compreender suas características específicas. Neste trabalho, o estudo de caso foi aplicado ao processo eleitoral do NED, permitindo uma análise detalhada dos desafios e limitações do sistema actual. Essa abordagem foi fundamental para identificar as necessidades que o protótipo deve atender.

e) Técnicas de colecta de dados

Segundo Marconi e Lakatos (2003), as técnicas de coleta de dados correspondem a um conjunto de regras ou processos utilizados para reunir informações relevantes para a pesquisa. No presente trabalho, foram empregadas as seguintes técnicas:

- **Coleta Documental:**

A coleta documental consiste na obtenção de dados a partir de fontes primárias, como documentos escritos ou não escritos, pertencentes a arquivos públicos, instituições ou domicílios, além de fontes estatísticas (Marconi & Lakatos, 2003). No presente estudo, essa técnica foi utilizada para analisar documentos relacionados ao processo eleitoral do Núcleo de Estudantes de Direito da UEM, como regulamentos internos, atas de reuniões e relatórios de eleições anteriores.

- **Entrevista:**

Pode ser definida como a conversa realizada pelo pesquisador junto ao entrevistado a fim de obter informações relevantes para o objeto de estudo (Marconi & Lakatos, 2003). Neste

trabalho, a entrevista será utilizada para obter dados qualitativos junto a membros do NED, de modo a enriquecer a análise do contexto actual, identificar os principais desafios enfrentados nas eleições e validar os requisitos da solução proposta.

1.4.2. Metodologia de desenvolvimento do protótipo da solução proposta

O protótipo da solução proposta será desenvolvido tendo em conta as fases da metodologia de desenvolvimento de software em cascata segundo Sommerville (2011). Neste modelo, temos o encadeamento, em cascata, de forma sequencial, entre as actividades do processo de desenvolvimento de forma que uma fase não deve ser iniciada até que a fase anterior seja concluída. Desta forma, as fases que compõem a metodologia de desenvolvimento em cascata, segundo Sommerville (2011), são as seguintes:

I. Análise e definição de requisitos

Os serviços, restrições e metas do sistema são estabelecidos por meio de consulta aos usuários. Em seguida, são definidos em detalhes e funcionam como uma especificação do sistema.

II. Projecto de sistema e software

O processo de projecto de sistemas aloca os requisitos tanto para sistemas de hardware como para sistemas de software, por meio da definição de uma arquitetura geral do sistema. O projecto de software envolve identificação e descrição das abstrações fundamentais do sistema de software e seus relacionamentos.

III. Implementação e teste unitário

Durante esse estágio, o projecto do software é desenvolvido como um conjunto de programas ou unidades de programa. O teste unitário envolve a verificação de que cada unidade atenda a sua especificação.

IV. Integração e teste de sistema

As unidades individuais do programa ou programas são integradas e testadas como um sistema completo para assegurar que os requisitos do software tenham sido atendidos. Após o teste, o sistema de software é entregue ao cliente.

V. Operação e manutenção

O sistema é instalado e colocado em uso. A manutenção envolve a correção de erros que não foram descobertos em estágios iniciais do ciclo de vida, com melhora da implementação das unidades do sistema e ampliação de seus serviços em resposta às descobertas de novos requisitos.

Nota: para este trabalho, por questões de tempo, não será possível ir até a fase de Operação e manutenção, pelo que, a última fase será a de Integração e teste de sistema.

1.5. Estrutura do Trabalho

O presente trabalho está organizado em seis capítulos principais, complementados por seções de referências bibliográficas e anexos, conforme detalhado a seguir:

Capítulo I – Introdução

Apresenta o contexto da pesquisa, sua relevância acadêmica e social, os objetivos gerais e específicos, e a metodologia empregada. Esta seção estabelece o quadro teórico e prático que justifica o desenvolvimento do sistema de votação electrónica baseado em blockchain.

Capítulo II – Revisão de Literatura

Sistematiza o conhecimento científico existente sobre: (1) sistemas de votação tradicionais e electrónicos, (2) fundamentos da tecnologia blockchain e (3) aplicações de blockchain em processos eleitorais, com análise de casos internacionais.

Capítulo III – Caso de estudo

Descreve o processo eleitoral actual do NED, incluindo o fluxo de trabalho e actores envolvidos, análise crítica dos pontos fortes e limitações requisitos para a solução proposta e uma descrição geral da solução proposta.

Capítulo IV – Desenvolvimento da solução proposta

Detalha as etapas de implementação do protótipo:

1. Definição de requisitos funcionais e não-funcionais
2. Arquitetura do sistema e modelagem de dados
3. Implementação dos contratos inteligentes e interface
4. Protocolos de teste e validação

Capítulo V – Discussão dos resultados

Apresenta e discute os dados obtidos nos testes do protótipo, avaliando:

- Desempenho técnico
- Usabilidade
- Adequação aos requisitos identificados.

Capítulo VI – Considerações finais

Sintetiza as contribuições do trabalho, confronta os resultados com os objetivos iniciais e propõe direções para pesquisas futuras, incluindo possibilidades de escalabilidade para outros contextos.

Secção das Bibliografias

Lista rigorosa de todas as fontes citadas, seguindo as normas APA.

Secção dos Anexos

Inclui:

- Descrição detalhada dos casos de uso do sistema
- Diagramas técnicos completos
- Fluxogramas de processos
- Modelos de dados

- outros elementos que tenham contribuído para a concretização do trabalho.

2. Capítulo II – Revisão de Literatura

Neste capítulo, são apresentados os fundamentos teóricos que sustentam a pesquisa, com o intuito de contextualizar o problema estudado. A revisão contempla desde os conceitos relacionados ao processo de votação, suas limitações e a votação electrónica. Em seguida, são abordados os fundamentos da tecnologia blockchain, suas características, mecanismos e potencial de aplicação em sistemas de votação, de modo a fornecer a base necessária para a proposta de solução apresentada nos capítulos seguintes.

2.1. Votação

O direito ao voto, tal como é conhecido hoje, foi resultado de um longo processo de inclusão social. Nas primeiras democracias, grupos como analfabetos, negros, mulheres e indivíduos de baixa renda eram sistematicamente excluídos do processo eleitoral, seja por restrições legais ou por barreiras económicas (Rodrigues, 2008). Essa exclusão limitava a representatividade política e consolidava estruturas de poder oligárquicas.

Na contemporaneidade, a votação constitui-se como o mecanismo fundamental do Estado Liberal, permitindo que os cidadãos escolham os seus representantes governamentais através de eleições periódicas (Rodrigues, 2008). Para além do contexto político, o acto de votar assume um papel decisório mais amplo. Conforme explica Nurmi (2010), trata-se de um método de resolução de conflitos e tomada de decisões colectivas, aplicável desde escolhas governamentais até selecções em concursos ou organizações.

Moghaddam (2017) reforça essa perspectiva, definindo a votação como um processo grupal de selecção entre alternativas, cujo resultado reflecte a preferência da maioria. Seja na eleição de um presidente municipal ou de um membro do parlamento, o voto opera como instrumento de legitimação democrática.

Levando em consideração os conceitos apresentados, pode-se entender que Independentemente do contexto político, institucional ou social, a votação caracteriza-se como um mecanismo de escolha colectiva, cuja validade depende da adesão a princípios como transparência, igualdade de participação e confiabilidade nos resultados.

2.1.1. Sistemas de votação tradicionais

Os sistemas eleitorais tradicionais sofreram profundas transformações nos últimos dois séculos. Nos primórdios das democracias modernas, por volta do século XIX, os processos de votação caracterizavam-se pela ausência de registo centralizado de eleitores e pela natureza pública do sufrágio (Jones, 2003). Como detalha Jones (2003), os votantes, após prestarem juramento verbal sobre seu direito ao voto, anunciavam abertamente as suas preferências aos funcionários eleitorais, que as registavam em livros de actas, não existia qualquer mecanismo de voto secreto. Este modelo apresentava duas contradições fundamentais, conforme explica Jones (2003):

A transparência do processo permitia verificação independente da contagem, reduzindo riscos de falsificação directa de votos. Por outro lado, a exposição pública dos eleitores os tornava vulneráveis a coacção e compra de votos.

Além disso, a falta de controlo eficiente permitia que indivíduos votassem múltiplas vezes, desde que não reconhecidos pelos mesmos funcionários. A superação do voto por voz deu-se com a introdução do sistema de cédulas oficiais, marco fundamental na busca por processos eleitorais mais íntegros e acessíveis.

2.1.2. Sistema de Boletins de Voto

A revolução na tecnologia eleitoral ocorreu em 1858, quando a Austrália implementou o primeiro sistema oficial de boletins de voto impressos, contendo a lista completa de candidatos e distribuídos exclusivamente pelo governo nos locais de votação (Jones, 2003). Este modelo, descrito por Bellis (2006), opera através de três elementos-chave:

I. **Padronização**: boletins idênticos impressos com os nomes dos candidatos.
II. **Sigilo**: Marcação em cabine isolada.
III. **Segurança física**: Urnas seladas para armazenamento.

“O eleitor marca sua preferência na caixa correspondente à sua escolha, em privado, e deposita o boletim numa urna selada”, garantindo simultaneamente privacidade e rastreabilidade limitada (Bellis, 2006, secção Paper Ballots).

Vantagens e Desafios

Embora utilizado por 81% dos países, segundo o International IDEA (2023), este sistema apresenta paradoxos, como mostra a Tabela 1, baseada em Gailly et al. (2018):

Tabela 1: Vantagens e desafios dos sistemas de cédulas de Papel

Vantagens	Desafios
Simplicidade técnica	Custos logísticos elevados (transporte, impressão)
Auditabilidade física (contagem manual)	Risco de falsificação (urnas violáveis)
Acessibilidade (sem requisitos digitais)	Dificuldade para eleitores com deficiência visual

Caso de Moçambique

Em Moçambique, o sistema de boletins de voto impressos é o padrão desde 1994, porém enfrenta críticas quanto a (Brito, 2009):

- Demora na apuração, com prazos extremamente longos (15 dias para o anúncio de resultados em eleições nacionais) e que têm sido frequentemente ultrapassados.
- Suspeitas de "boletins fantasmas" em zonas rurais.

Estes desafios têm incentivado a discussão sobre o uso de tecnologias complementares, como as urnas digitais, em algumas fases do processo, embora o voto continue a ser realizado por meio de boletins de papel.

2.2. Votação Electrónica

A integração de tecnologias no processo democrático remonta ao período pós-Segunda Guerra Mundial, com a adaptação pioneira de sistemas computacionais para fins eleitorais (Vedel, 2006). Contudo, foi apenas nas últimas décadas que a votação electrónica se consolidou como paradigma distinto, definido por Wolf et al. (2011) como um sistema que utiliza tecnologias de informação e comunicação para registar, lançar ou contar votos em eleições políticas e referendos. Na prática, essa abordagem materializa-se através de (Adeshina & Ojo, 2014):

- **Dispositivos dedicados**: Máquinas de votação electrónica (EVMs - do inglês Electronic Voting Machines), usadas em países como Brasil e Índia.
- **Plataformas digitais**: Voto pela internet, implementado na Estónia desde 2005.

2.2.1. Benefícios e Limitações

Estudos destacam três vantagens principais (Adeshina & Ojo, 2014; Ayed, 2017; ODIHR, 2024):

I. **Eficiência:** Redução de 90% no tempo de apuração (comparado a boletins de papel) e minimização de erros humanos na contagem.
II. **Acessibilidade:** Facilitação do voto para populações rurais ou com mobilidade reduzida.
III. **Participação:** Sistemas de votação electrónica tornam o processo de voto mais simples e conveniente e aumentam a taxa de participação em eleições.

Apesar dos avanços, persistem desafios críticos (Statista, 2022; Wolf et al., 2011):

- **Exclusão digital**: Cerca de 4 em cada 10 pessoas em África tinham acesso à Internet até dezembro de 2021.
- Transparência e compreensão do sistema limitadas para os não especialistas.
- Risco de manipulação por pessoas com acesso privilegiado ao sistema ou por *hackers* externos.

2.2.2. Características dos Sistemas de Votação Electrónica

Segundo Wolf et al. (2011), os sistemas de votação electrónica baseiam-se em quatro pilares tecnológicos fundamentais: criptografia (proteção dos dados), aleatoriedade (ordenação na apuração), comunicação segura (transmissão dos resultados) e mecanismos de segurança (prevenção de intrusões). Esses pilares traduzem-se em funcionalidades específicas para diferentes intervenientes no processo eleitoral:

I. **Para os Eleitores**
   - **Autenticação e elegibilidade**: Os sistemas podem usar bases de dados locais ou nacionais para verificar a identidade do eleitor (via biometria, número de identificação, etc.) e impedir votos duplicados.
   - **Interface de votação**: Pode incluir urnas com tela sensível ao toque (como no Brasil), scanners ópticos (OMR) para leitura de cédulas em papel ou software para voto remoto.
   - **Acessibilidade**: Adaptações incluem leitores de tela, dispositivos Braille e interfaces com ícones para eleitores analfabetos.

II. **Para Funcionários Eleitorais**
   - **Gestão do processo**: Inclui ações como inicializar a urna (zerar contadores), encerrar a votação e emitir resultados preliminares.
   - **Transmissão segura dos resultados**: Utiliza canais criptografados para evitar a interceptação ou manipulação de dados.

Requisitos de Segurança para Sistemas de Votação Electrónica

Um sistema de votação electrónica deve atender a critérios rigorosos de segurança para garantir a integridade do processo democrático. Baseado em Cetinkaya (2008), os requisitos essenciais são:

I. **Privacidade do Eleitor:** não deve ser possível associar a identidade do eleitor ao voto registado, mesmo que indirectamente.

II. **Elegibilidade:** os eleitores qualificados devem se registar antes do dia da eleição e apenas estes podem votar.

III. **Unicidade:** apenas um voto por eleitor deve ser contado.

IV. **Imparcialidade:** resultados parciais não devem ser acessíveis nem às autoridades.

v. **Não Coercibilidade**: Nenhum coercitivo, incluindo as autoridades, deve ser capaz de extrair o valor do voto e não deve ser capaz de coagir um eleitor a votar de uma maneira específica, qualquer eleitor deve ser capaz de votar livremente.

VI. **Isenção de Recibo:** os eleitores não devem obter um recibo, nem podem construir um, que pode ser usado para provar o conteúdo de seus votos a terceiros durante a eleição e após o término da eleição.

VII. **Precisão**

- Todos os votos válidos devem ser contados corretamente.
- Nenhum voto lançado pode ser alterado, excluído, invalidado ou copiado.
- Nenhum participante, eleitor ou autoridade pode interromper ou influenciar a eleição e a contagem final adicionando votos falsos.

VIII. **Verificação Individual:** o eleitor deve poder verificar se seu voto criptografado foi contado e tabulado corretamente na contagem final.

2.2.3. Classificação dos Sistemas de Votação Electrónica

Como destacado por Wolf et al. (2011, p. 10), "não existe um sistema de votação electrónica perfeito", e a escolha deve considerar o contexto específico, ponderando vantagens e desvantagens de cada opção. Tecnicamente, os sistemas classificam-se em quatro categorias principais:

I. Máquinas de Votação Electrónica de Registo Direto (DRE - Direct recording electronic)
II. Sistemas de Reconhecimento Óptico de Marca (OMR)
III. Impressoras de Cédulas Electrónicas (EBPs - Electronic ballot printers)
IV. Sistemas de Votação pela Internet

Sistemas de Reconhecimento Óptico de Marca (OMR)

Os sistemas OMR utilizam *scanners* especializados para interpretar escolhas registadas em boletins de papel pré-formatados, combinando tecnologia digital com processos manuais. Podem ser implementados de duas formas (Wolf et al., 2011):

I. **Contagem Centralizada:** os boletins são digitalizados em centros de processamento após o encerramento da votação.
II. **Sistemas PCOS** (Precinct Count Optical Scan): a contagem ocorre na própria seção eleitoral, quando o eleitor insere a cédula na máquina.

Máquinas de Votação Electrónica de Registo Direto (DRE)

As máquinas DRE substituem os boletins físicos por interfaces digitais para registo direto dos votos em memória electrónica (Bellis, 2006). As máquinas DRE funcionam por meio de uma interface que pode incluir telas sensíveis ao toque ou botões físicos, permitindo ao eleitor selecionar os candidatos de sua preferência.

Em relação ao armazenamento, os votos são guardados na memória interna da máquina, geralmente em cartões SD ou memória flash. Conforme apontam Sepúlvida e Paiva, (2019), esse armazenamento ocorre sem o uso de criptografia, os dados dos votos são gravados de forma aleatória e não cronológica, o que torna impossível estabelecer qualquer vínculo entre o eleitor e o voto registado.

Impressoras de Boletins Eletrônicos

As Impressoras de Boletins Eletrônicos são sistemas híbridos que combinam a praticidade do voto digital com a segurança do registo físico. Funcionam como uma evolução das máquinas DRE, adicionando um comprovante em papel que pode ser auditado posteriormente (Wolf et al., 2011).

Sistemas de Votação pela Internet

Os sistemas de votação pela internet permitem que os eleitores votem remotamente usando dispositivos conectados à rede, como computadores ou smartphones. Essa modalidade tem ganhado atenção global devido à sua conveniência, mas também enfrenta desafios críticos de segurança (Wolf et al., 2011). O voto online pode ocorrer em locais com acesso controlado, de forma online com uso de qualquer dispositivo com acesso à internet, ou ainda de forma mista, combinando as duas modalidades.

2.2.4. Votação Electrónica ao Redor do Mundo

O uso de tecnologias de votação electrónica varia significativamente entre países, refletindo diferenças em infraestrutura tecnológica, confiança institucional e contexto político. Segundo o International IDEA (2023), 34 de 178 países analisados adoptaram sistemas electrónicos em eleições nacionais ou subnacionais, como demonstra a figura 1.

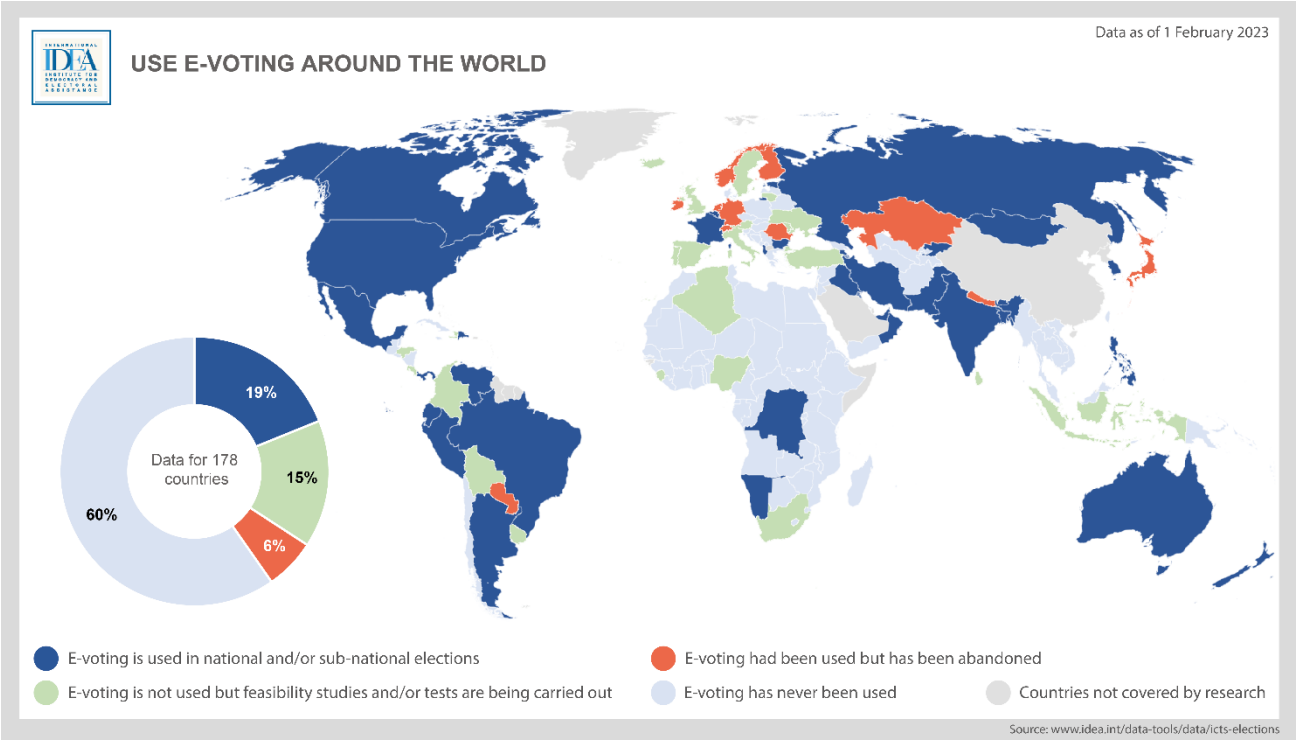


Figura 1: Mapa global da votação electrónica

Fonte: International IDEA (2023)

Em azul claro estão representados países sem adopção de voto eletrônico como é o caso da maioria da África e Alemanha, em azul escuro temos os países com uso efetivo da votação electrónica em eleições como o Brasil, Índia e Estônia e em verde, países em fase de testes, como o Canadá e Reino Unido.

Dos países que adoptaram a votação electrónica, 50% utilizam DREs (17 em 34 países). Estes países utilizam DREs com ou sem registo de auditoria em papel verificado pelo eleitor (VVPAT – do inglês voter-verified paper audit trail). 24% dos países que utilizam a votação electrónica adoptaram OMRs ou OCRs (8 em 34 países), estas tecnologias são utilizadas principalmente no hemisfério norte. Sistemas de votação pela internet foram adoptados por 41% dos países que utilizam a votação electrónica (14 em 34 países), estando alguns países a utilizar o voto pela internet para todos os eleitores do país, outros para algumas regiões e outros apenas para votação no estrangeiro (International IDEA, 2023).

2.3. Blockchain

A tecnologia Blockchain é frequentemente descrita como uma evolução das bases de dados tradicionais, operando sob o paradigma da Distributed Ledger Technology (DLT), ou tecnologia de registo distribuído. De acordo com o World Bank Group (2017), a DLT permite

que múltiplos registos de dados idênticos sejam mantidos simultaneamente por uma rede descentralizada de servidores (chamados nós). Dentro deste universo, a blockchain representa um tipo específico de DLT que utiliza técnicas criptográficas para estruturar os dados em blocos interligados e imutáveis, criando um histórico permanente e transparente de transacções.

Mais do que uma simples base de dados, a blockchain tem sido reconhecida como uma ferramenta de transacção de valores entre pares (ponto-a-ponto), eliminando a necessidade de intermediários tradicionais como bancos ou outras entidades de confiança, conforme apontado por Singhal (2018). Esta capacidade de operar sem uma autoridade central confere à tecnologia uma característica distintiva de descentralização.

Além disso, Tyagi e Bhatia (2021) destacam que uma blockchain é composta por quatro elementos principais que formam os blocos da cadeia, que por sua vez constituem um registo público, denominado ledger (nesse trabalho será adoptada a tradução para *ledger*, porém pode ser traduzido também como livro-razão), descentralizado e distribuído. Este modelo, segundo Perwej (2018), assegura que as transacções registadas na rede sejam públicas, invioláveis e irreversíveis, reforçando a confiança dos utilizadores na integridade do sistema.

2.3.1. Surgimento e história

O surgimento da tecnologia blockchain está intrinsecamente ligado à criação da Bitcoin. Em 2008, sob o pseudónimo de Satoshi Nakamoto, foi apresentado o conceito de um sistema de dinheiro electrónico descentralizado, baseado numa rede ponto-a-ponto (P2P - peer-to-peer), o qual ficaria conhecido como Bitcoin (Nakamoto, 2008). Embora inovador, o projecto de Nakamoto não surgiu num vazio: a estrutura de dados utilizada no ledger da Bitcoin foi fortemente inspirada no trabalho desenvolvido por Stuart Haber e Scott Stornetta, entre 1990 e 1997. Estes autores propuseram um sistema de *timestamping* digital de documentos, visando garantir a integridade e a autenticidade de informações ao longo do tempo, funcionando como um “notário digital” (Narayanan & Clark, 2017).

No modelo de Haber e Stornetta, cada novo documento era associado temporalmente ao anterior através de assinaturas digitais, formando uma cadeia de documentos que se tornava praticamente imutável sem que toda a sequência subsequente fosse alterada. A Bitcoin apropriou-se desta estrutura de cadeia cronológica, acrescentando-lhe uma camada

essencial de segurança: o mecanismo de *Proof of Work*, que introduz o conceito de validação computacional das transacções (Narayanan & Clark, 2017).

A publicação do *white paper* de Nakamoto (2008) marcou o início da implementação prática destas ideias. Em janeiro de 2009, foi minerado o primeiro bloco da Bitcoin, conhecido como bloco Génesis, dando início a uma cadeia que, até hoje, nunca sofreu interrupções. Com o crescimento contínuo da Bitcoin, a atenção voltou-se também para a tecnologia subjacente. A partir de 2015, a base tecnológica da cadeia Bitcoin passou a ser estudada de forma independente, consolidando-se sob o nome de blockchain (Malik et al., 2022).

Embora a Bitcoin continue a ser o exemplo mais reconhecido da aplicação da blockchain, a sua base tecnológica revelou-se útil para diversas outras áreas. O sucesso da Bitcoin impulsionou a exploração da blockchain em domínios como registos eletrónicos de saúde, gestão de propriedades, cadeias de abastecimento, armazenamento de dados, contratos inteligentes, Internet das Coisas (IoT) e, mais recentemente, sistemas de votação electrónica (Perwej, 2018).

No que diz respeito à sua evolução, Perwej (2018) propõe uma divisão da tecnologia blockchain em três gerações distintas.

I. A primeira geração, representada por sistemas como a Bitcoin, consistia principalmente num ledger público destinado a registar transacções financeiras assinadas criptograficamente. Nessa fase, a capacidade de suporte a transacções programáveis era bastante limitada, permitindo apenas a incorporação de pequenos fragmentos de dados auxiliares para representar ativos físicos ou digitais.
II. A segunda geração introduziu uma infraestrutura programável de uso geral, na qual o ledger público passou também a registar o resultado de operações computacionais. Este avanço permitiu a criação de aplicações mais complexas e dinâmicas, superando as restrições iniciais.
III. Por fim, a terceira geração é marcada pela introdução dos contratos inteligentes, programas que podem ser implantados e executados diretamente numa blockchain, aumentando exponencialmente as possibilidades de automação e inovação em diferentes sectores.

2.3.2. Estrutura de uma Blockchain

A blockchain é um ledger público e distribuído que regista transacções de forma segura e imutável, com base num conjunto de protocolos acordados entre os nós da rede (Perwej, 2018). Cada participante mantém uma cópia idêntica dos dados, garantindo transparência e resistência à censura. A cadeia é composta por blocos interligados, onde cada novo bloco representa uma alteração no estado partilhado da rede (Kaur et al., 2020).

Embora o funcionamento geral da blockchain envolva várias tecnologias, a sua estrutura pode ser compreendida ao analisar separadamente os seus principais componentes.

Blocos e transacções na Blockchain

Segundo Malik et al. (2022), uma transacção na blockchain é, de forma simples, uma estrutura de dados que armazena determinada informação acompanhada de um timestamp. Essa informação pode representar uma transferência de moeda, a posse de um bem, o estado de um processo ou um evento. Para que seja registada, a transacção é inicialmente transmitida à rede, onde é validada por vários nós. Depois de validada, é agrupada com outras e inserida num bloco, que será novamente transmitido para ser adicionado à cadeia (Singhal, 2018).

Conforme explicam Li et al. (2021), cada bloco é construído a partir de uma árvore de Merkle, que organiza e resume todas as transacções com funções de *hash*, e inclui também o hash do bloco anterior, formando assim uma ligação sequencial.

A estrutura de um bloco divide-se em duas partes principais: cabeçalho (header) e corpo (body) (Kaur et al., 2020). O cabeçalho inclui os seguintes campos:

- **Versão do bloco**: indica os protocolos utilizados para validação;
- **Merkle tree root hash**: representa o resumo de todas as transacções do bloco;
- **Timestamp**: marca o momento de criação do bloco;
- **nBits**: valor que define a dificuldade para validação;
- **Nonce**: um número de 4 bytes ajustado iterativamente;
- **Hash do bloco anterior**: liga o bloco actual ao anterior.

O corpo contém as transacções e um contador que indica o número total delas no bloco. A quantidade de transacções varia conforme o seu tamanho e o limite definido para o bloco.

Malik et al. (2022) destacam dois tipos principais de blocos:

I. **Bloco génese**: o primeiro da cadeia, criado uma única vez. Não possui referência a blocos anteriores e marca o início da blockchain.
II. **Bloco de transacções**: contém os dados do cabeçalho e corpo, como descrito acima, e é criado de forma contínua.

A Figura 2 ilustra como os blocos se ligam entre si, sendo que cada novo bloco carrega o hash do anterior, garantindo a continuidade e integridade da cadeia.

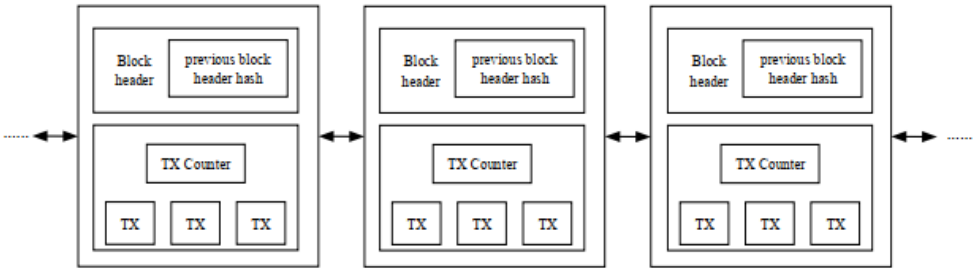


Figura 2: Cadeia de blocos

Fonte: (Li et al., 2021)

Sistema distribuído e descentralizado

Um **sistema distribuído** é composto por múltiplos computadores independentes (denominados nós), localizados em diferentes pontos da rede, que comunicam entre si e coordenam as suas ações de forma a parecerem um único sistema coeso para o utilizador final (Tanwar, 2022). Estes nós, que podem ser servidores físicos, máquinas virtuais, containers ou outros tipos de dispositivos, colaboram através da troca de mensagens.

Já um **sistema descentralizado** distingue-se por não possuir uma entidade central de controlo, todos os nós têm autoridade equivalente, funcionando de maneira autónoma e colaborativa (Singhal, 2018). Embora todos os sistemas descentralizados sejam distribuídos, nem todos os sistemas distribuídos são descentralizados. O que torna a blockchain especial é o facto de reunir ambas as características.

No contexto da blockchain, os nós não executam apenas uma parte da tarefa distribuída por um controlador central, em vez disso, os nós interessados (ou escolhidos aleatoriamente, conforme o protocolo) executam o processamento completo necessário para validar e registar uma transacção (Singhal, 2018). Este modelo cria uma rede P2P robusta e

transparente, na qual cada participante desempenha um papel na manutenção da integridade do sistema.

Criptografia

Segundo Tanenbaum e Van Steen (2017) a criptografia é uma das bases da segurança nos sistemas distribuídos, sendo essencial também para o funcionamento da blockchain. Estas técnicas são divididas em dois grandes grupos: criptografia simétrica e criptografia assimétrica.

Na **criptografia simétrica**, a mesma chave é utilizada tanto para encriptar como para desencriptar os dados. Já na **criptografia assimétrica**, são usadas duas chaves distintas, uma pública e outra privada, sendo a chave pública usada para encriptar os dados e a chave privada usada para desencriptar os dados (Lewis, 2018).

Além da encriptação, a blockchain utiliza intensivamente funções de hash criptográfico para garantir a integridade dos dados. O **hashing** consiste num processo que transforma uma entrada de qualquer tamanho (um ficheiro, texto ou imagem) numa saída de tamanho fixo, chamada *digest*. O mais importante é que uma pequena alteração na entrada, mesmo que seja um único bit, resulta numa saída completamente diferente, garantindo assim que qualquer modificação é imediatamente detetável (Yaga et al., 2019). Uma das funções de hash mais usadas nas tecnologias de blockchain é o SHA-256 (Secure Hash Algorithm 256 bits).

Tabela 2: Exemplos de entradas e saídas SHA-256 digest

Entrada	SHA-256 digest
`1`	`0x6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b`
`2`	`0xd4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35`
`Olá, mundo!`	`9583b013baa520d3a893c4270d0c67732d7ef1768eb0a13533b4e7b134d4b131`

Fonte: (Yaga et al., 2019)

Outro componente essencial da arquitetura blockchain é a assinatura digital. Trata-se de uma técnica matemática usada para validar a autenticidade e a integridade de uma mensagem, software ou documento digital. Na prática, a assinatura digital é criada encriptando o hash da mensagem com a chave privada do remetente. Qualquer pessoa com acesso à chave pública desse remetente pode verificar se a mensagem é autêntica e se não foi alterada durante a transmissão (Tanwar, 2022).

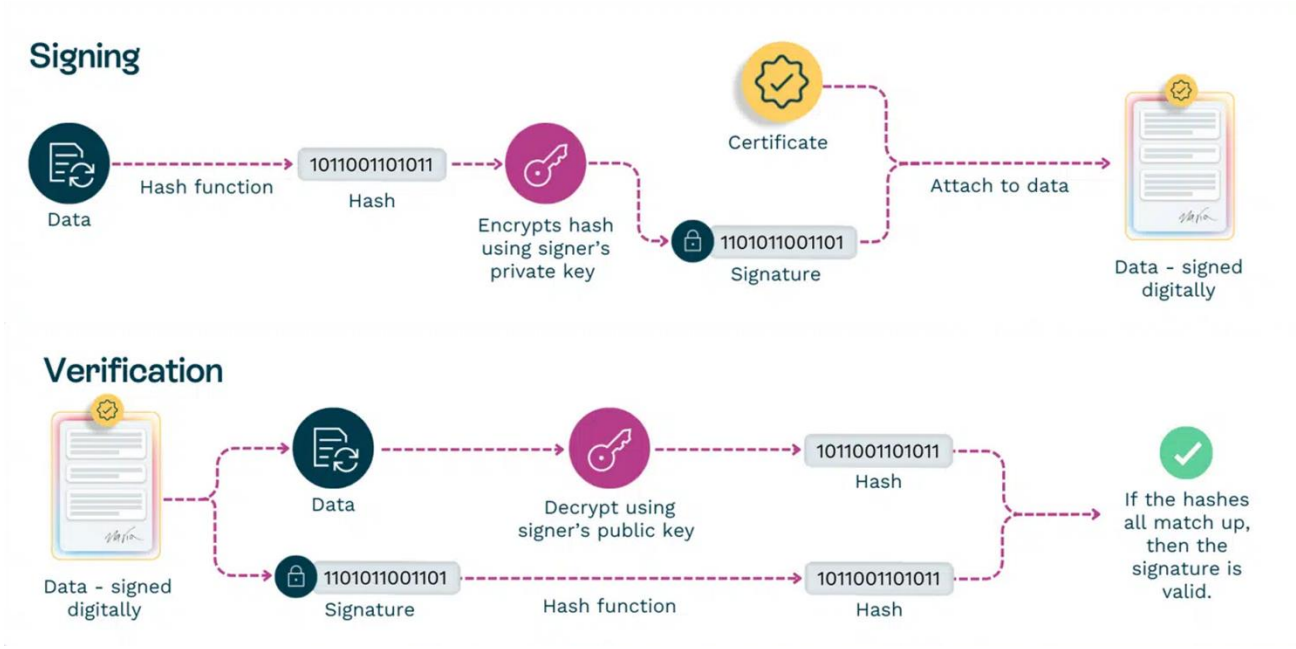


Figura 3: Assinatura digital

Fonte: (Sandford, 2024)

Árvores de Merkle

As árvores de Merkle são estruturas fundamentais para garantir a integridade e eficiência na verificação de dados dentro da blockchain. Uma árvore de Merkle é, essencialmente, uma árvore binária de hashes criptográficos. Ela é construída a partir da encriptação de pares de dados (normalmente, transacções) nas folhas da árvore. Em seguida, os valores encriptados são combinados e novamente encriptados até chegar ao topo da estrutura, formando o chamado Merkle root, ou raiz de Merkle (Singhal, 2018).

De acordo com Narayanan & Clark (2017), essa organização permite que qualquer alteração numa transacção (isto é, num dos nós folha) afete todos os hashes até à raiz, o que torna qualquer tentativa de manipulação imediatamente detetável. Assim, ao conhecer o último hash válido, é possível descarregar o restante do ledger de uma fonte não confiável e ainda assim verificar a sua integridade. Segundo Borrego (2019), essa estrutura, combinada aos ponteiros de hash, oferece um modelo de dados seguro e eficiente para rastrear todas as alterações feitas nos estados globais da blockchain.

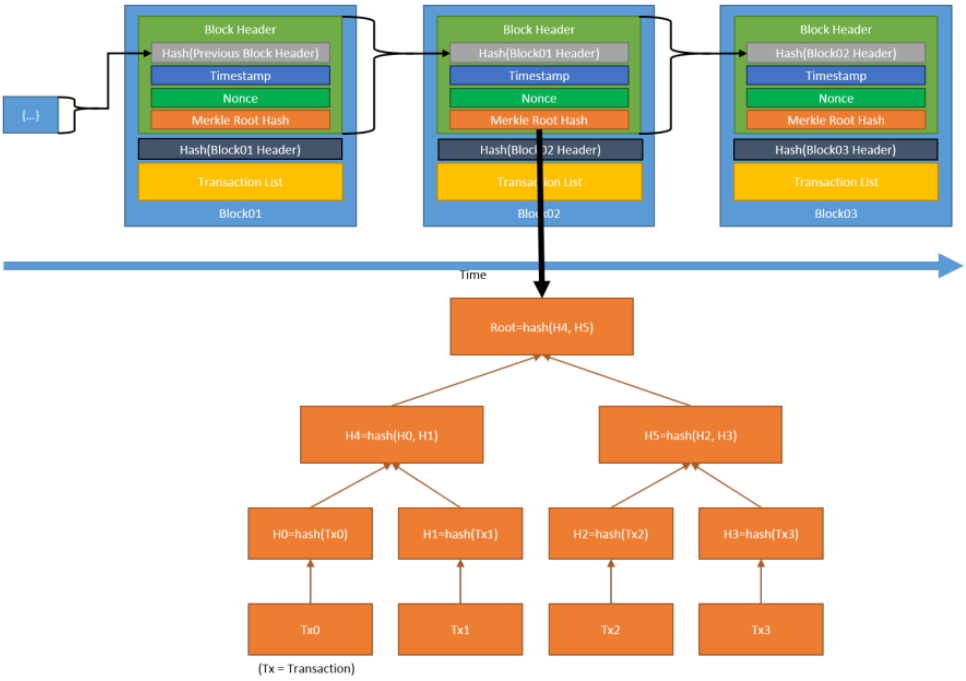


Figura 4: Transacções com Hash em uma Merkle Tree

Fonte: (Yaga et al., 2019)

Mecanismos de Consenso

Em redes blockchain, não existe um nó central responsável por garantir a consistência dos dados entre os diferentes participantes, por isso, torna-se essencial empregar protocolos que permitam que todos os nós cheguem à um acordo comum sobre o estado do ledger. Esses protocolos são conhecidos como mecanismos de consenso e constituem um dos pilares do funcionamento seguro e confiável da blockchain.

Proof of Work (PoW)

O PoW foi o primeiro algoritmo de consenso aplicado em redes blockchain, tendo sido utilizado inicialmente no Bitcoin para validar o nó que publica as transacções na rede (Nakamoto, 2008; Yaga et al., 2019).

Nesse modelo, a confiança entre os participantes é mínima ou inexistente, por isso, a validação depende da resolução de um problema computacional complexo. A dificuldade está em encontrar uma solução válida para esse problema, mas uma vez encontrada, a verificação por parte dos outros nós é rápida e simples. O objectivo é garantir que qualquer bloco proposto possa ser facilmente rejeitado caso não cumpra os requisitos do desafio, protegendo assim a rede contra tentativas de fraude (Yaga et al., 2019).

Proof of Stake (PoS)

Uma alternativa mais eficiente em termos de energia à mineração do PoW é o *Proof of Stake* (PoS). Diferente do PoW, o PoS não exige investimentos em hardware especializado, o que o torna mais acessível e sustentável (Malik et al., 2022). A lógica por trás desse modelo baseia-se no princípio de que quanto maior a participação de um utilizador no sistema, maior será seu interesse em garantir a integridade da rede. Assim, os utilizadores com maior quantidade de participação têm mais chances de serem escolhidos para validar novos blocos. As formas de selecção podem variar entre escolha aleatória, votação em múltiplas rondas ou um sistema baseado na idade das moedas, mas todas têm em comum o critério da participação como base da confiança (Yaga et al., 2019).

2.3.3. Características de uma blockchain

A tecnologia blockchain possui um conjunto de características fundamentais que a tornam especialmente atractiva para aplicações onde a segurança, confiança e rastreabilidade são essenciais. Essas características não existem de forma isolada, mas sim integradas na estrutura técnica e lógica da blockchain, reforçando mutuamente a robustez do sistema.

Segurança criptográfica

Uma das bases da segurança na blockchain é a utilização de algoritmos de hash e assinaturas digitais. Cada transacção é convertida em um valor criptográfico único por meio do algoritmo SHA-256, garantindo que qualquer alteração mínima nos dados resulte em uma modificação radical no valor do hash. Além disso, as assinaturas digitais vinculam transacções a identidades criptográficas, dificultando a falsificação ou manipulação de dados (Tanwar, 2022). Essa combinação assegura tanto a integridade como a autenticidade da informação na rede.

Imutabilidade dos dados

A estrutura da blockchain é projectada para ser *append-only*, ou seja, os dados só podem ser adicionados, nunca alterados ou removidos. Cada bloco contém o hash do bloco anterior, e qualquer tentativa de modificação mesmo que mínima invalida toda a cadeia subsequente. Essa característica torna a blockchain resistente à adulteração e garante a permanência dos registos ao longo do tempo (Kaur et al., 2020; Malik et al., 2022; Tanwar, 2022).

Transparência e auditabilidade

A transparência é assegurada pela replicação do ledger completo entre todos os nós da rede, permitindo que todos os participantes acedam e verifiquem os dados transacionais. Além disso, o código-fonte das plataformas blockchain geralmente é aberto, o que possibilita auditorias independentes. A auditabilidade é fortalecida por meio de registros com timestamp, ou seja, cada bloco é marcado com a data e hora exata da sua inclusão na cadeia, permitindo rastrear com precisão a origem e a sequência das transacções (Lewis, 2018; Malik et al., 2022).

Verificabilidade pública e individual

Na maioria das blockchains públicas, todos os dados são visíveis para todos os participantes, garantindo a verificabilidade pública. Ao mesmo tempo, cada utilizador consegue verificar individualmente a inclusão e validade das suas próprias transacções, o que confere ao sistema tanto transparência coletiva como controle individual. Esse modelo fortalece a confiança, pois qualquer pessoa pode confirmar o estado actual da rede com base em informações acessíveis a todos (Lewis, 2018; Malik et al., 2022).

Privacidade e Anonimato

Embora a blockchain seja transparente, ela também garante certo nível de anonimato. As interações entre os utilizadores ocorrem por meio de endereços gerados criptograficamente, sem necessidade de revelar identidades reais. No entanto, essa privacidade não é absoluta: como os dados são públicos e permanentes, existe a possibilidade de rastreamento das atividades caso esses endereços sejam ligados a identidades do mundo real (Kaur et al., 2020).

2.3.4. Contratos Inteligentes (Smart Contracts)

A ideia de contratos inteligentes foi inicialmente proposta por Szabo, em 1996, com o objectivo de criar contratos digitais que permitem automatizar acordos entre partes sem depender de intermediários, que sejam autoexecutáveis e sem necessidade de confiança entre as partes envolvidas. Segundo Szabo (1996), tais contratos aumentam a garantia de cumprimento ao ponto de tornar qualquer violação extremamente custosa, o que elimina incertezas nos relacionamentos contratuais.

Na prática, os contratos inteligentes são programas de software executados de forma distribuída pelos nós de uma rede blockchain. Esses programas recebem parâmetros por meio de transacções na blockchain, processam essas informações segundo um algoritmo determinístico e produzem como saída uma alteração no estado interno do contracto ou uma nova transacção na rede (De Filippi et al., 2021). O seu funcionamento pode ser descrito como auto-executável, já que não há uma entidade central encarregada de monitorar ou autorizar sua execução. Dessa forma, os resultados são visíveis, auditáveis por qualquer participante da rede e permanecem imutáveis, garantindo a integridade do sistema (Malik et al., 2022).

Quanto às plataformas que suportam contratos inteligentes, o Ethereum é actualmente a mais proeminente. Esta rede disponibiliza a linguagem Solidity, que permite desenvolver contratos complexos executados na Ethereum Virtual Machine (EVM) (De Filippi et al., 2021). Por outro lado, o Hyperledger Fabric, voltado para aplicações empresariais, suporta contratos inteligentes através do que se chama de Chaincode. Já a rede Bitcoin também possui uma linguagem de script, mas com funcionalidades mais limitadas, voltadas apenas à validação de transacções básicas (Tanwar, 2022).

2.3.5. Classificação da blockchain

À medida que mais organizações buscam adoptar a tecnologia blockchain, surgiram diferentes plataformas que se distinguem principalmente pela forma como controlam o acesso e a participação dos seus utilizadores. Nesse sentido, as blockchains podem ser classificadas como permissionadas, não-permissionadas ou híbridas, dependendo de quem pode participar das transacções e validar os blocos na rede (Li et al., 2021).

Blockchains não-permissionadas, também conhecidas como públicas, são plataformas descentralizadas em que qualquer pessoa pode participar sem a necessidade de autorização prévia. A visibilidade dos dados é pública, permitindo que qualquer utilizador verifique transacções e participe no processo de consenso. Cada nó mantém sua própria cópia da blockchain e, como todos os nós podem participar da atividade de mineração, é essencial a implementação de mecanismos de consenso robustos para garantir a segurança da rede. Além disso, esse tipo de blockchain garante o anonimato entre os participantes. Exemplos de blockchains públicas incluem Bitcoin e Ethereum (Kaur et al., 2020; Li et al., 2021; Malik et al., 2022; Yaga et al., 2019).

Por outro lado, **blockchains permissionadas**, ou privadas, operam em redes centralizadas e são controladas por uma única entidade ou consórcio. Nesse modelo, nem todos os nós têm os mesmos direitos, a autoridade central define quem pode validar transacções e adicionar blocos à cadeia (Malik et al., 2022). Esse tipo de abordagem responde a preocupações comuns em ambientes corporativos e regulatórios, como a necessidade de verificação de identidade, definição de propriedade legal da cadeia de blocos e mecanismos de licenciamento (World Bank Group, 2017).

Por fim, as **blockchains híbridas** combinam elementos de blockchains públicas e privadas. Essa abordagem permite construir redes permissionadas sobre infraestruturas públicas, limitando o acesso e os papéis de cada participante, ao mesmo tempo em que mantém alguma transparência. Em alguns casos, a distinção é feita entre Blockchains públicas/privadas (referente ao acesso) e permissionadas/não-permissionadas (referente aos papéis dos participantes). Por exemplo, a plataforma Ripple é considerada uma blockchain pública permissionada, pois o acesso é aberto, mas a validação de dados é restrita a participantes autorizados. Já uma rede permissionada onde apenas um grupo

selecionado valida os dados seria classificada como uma blockchain privada permissionada (World Bank Group, 2017).

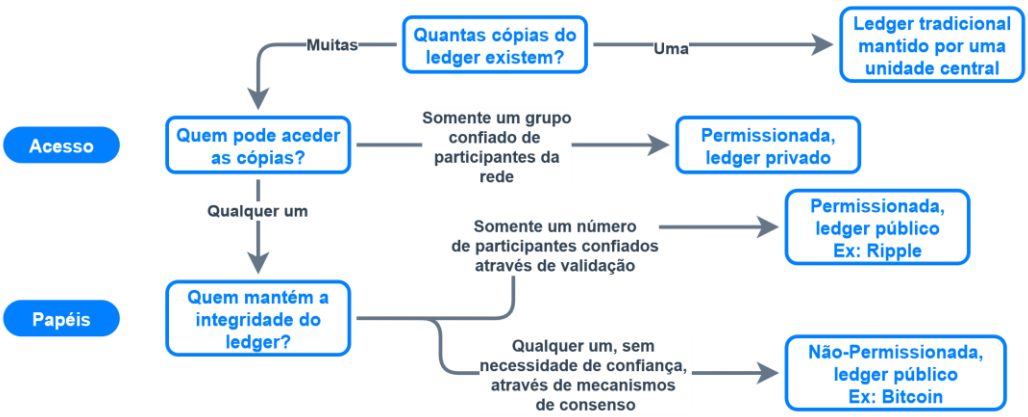


Figura 5: Classificação da Blockchain

Fonte: Adaptado de World Bank Group (2017)

2.3.6. Frameworks Blockchain

Os frameworks blockchain são soluções de software que simplificam o desenvolvimento e a implementação de aplicações baseadas em blockchain, exigindo pouca personalização. Essas plataformas geralmente incluem uma infraestrutura básica e bibliotecas prontas para acelerar o desenvolvimento, oferecendo aos programadores ferramentas essenciais para implementar contratos inteligentes, protocolos de consenso e gestão de estados distribuídos (Quasim et al., 2020).

Actualmente, existem diversas plataformas além do Bitcoin voltadas à construção de soluções blockchain. Entre as mais destacadas no cenário empresarial estão o Ethereum, Hyperledger Fabric e Corda, amplamente utilizadas em áreas como sistemas de pagamento, rastreamento da cadeia de suprimentos, registros de saúde e em aplicações de votação electrónica (Gupta & Madhur, 2018).

Ethereum

O Ethereum é uma das plataformas mais populares e versáteis do ecossistema blockchain, tendo sido projectada para permitir mais do que apenas transacções financeiras. Diferentemente do Bitcoin, que é voltado quase exclusivamente para transacções financeiras, o Ethereum foi concebido como uma máquina de estados distribuída. Os nós da rede Ethereum mantêm uma visão compartilhada do estado global, que pode ser modificado através de transacções válidas emitidas por usuários (Tikhomirov, 2017).

Uma das principais inovações do Ethereum está na possibilidade de criar contratos inteligentes, que são conjuntos de regras criptográficas que se executam automaticamente quando determinadas condições são atendidas. Essa camada abstrata permite que qualquer pessoa defina suas próprias regras de propriedade, formatos de transacção e funções de transição de estado, adaptando o uso da blockchain para as mais diversas aplicações (Vujičić et al., 2018).

Outro elemento fundamental do Ethereum é a *Ethereum Virtual Machine* (EVM), que fornece um ambiente de execução isolado e seguro para contratos inteligentes. A EVM garante que qualquer contracto inteligente seja executado de forma previsível e uniforme em todos os nós da rede, tornando possível o desenvolvimento de aplicações descentralizadas (DApps[1]) com lógica de negócios totalmente programável (Li et al., 2021). Essa flexibilidade tem sido crucial para a adopção do Ethereum em sistemas de votação electrónica, onde a verificação de votos, o anonimato e a imutabilidade são requisitos críticos.

R3 Corda

O Corda é uma plataforma de registo distribuído de código aberto desenvolvida em 2015 pelo consórcio R3, que reúne algumas das maiores instituições financeiras do mundo. Desde então, formou uma rede de parcerias com mais de 60 empresas de diferentes sectores (Gupta & Madhur, 2018).

Inicialmente projectado para facilitar o registo e o processamento de transacções financeiras, o Corda adopta um modelo P2P no qual cada nó armazena apenas os dados das transacções em que participou. Isso significa que, para reconstruir um histórico completo de auditoria, é necessário consultar múltiplos nós envolvidos na cadeia de transacções (Li et al., 2021).

Embora o Corda tenha sido criado com foco no sector bancário, seu modelo de confiança e controle de acesso também tem sido explorado em outras áreas, como cadeias de suprimentos, saúde e, mais recentemente, na administração pública e governança digital (Gupta & Madhur, 2018).

---

[1] As dApps são programas de software que funcionam numa blockchain ou numa rede peer-to-peer (P2P) de computadores, em vez de num único computador.

Hyperledger Fabric

Diferentemente das blockchains públicas como o Ethereum, o Hyperledger Fabric é uma plataforma modular e permissionada, o que significa que apenas participantes autorizados podem interagir com a rede. Ele permite a criação de contratos inteligentes, chamados *chaincodes*, e se destaca pela flexibilidade de programação, permitindo que os desenvolvedores usem linguagens comuns como Go, Java ou Node.js (Yaga et al., 2019).

Um dos aspectos mais inovadores do Fabric é sua arquitetura baseada no modelo executar-ordenar-validar, que substitui o tradicional ordenar-executar. Isso melhora a escalabilidade e permite transacções paralelas, adequando-se bem a aplicações empresariais e eleitorais em larga escala. Além disso, o Fabric não utiliza criptomoeda nativa, o que facilita a sua adopção por instituições que preferem manter controle completo sobre a gestão de identidade e regras da rede (Androulaki et al., 2018).

Tabela 3: Análise comparativa de frameworks Blockchain

Característica	Ethereum	Hyperledger Fabric	R3 Corda
Descrição da plataforma	Plataforma blockchain genérica	Plataforma blockchain modular	Plataforma de registo distribuído voltada ao sector financeiro
Governança	Desenvolvedores da comunidade Ethereum	Linux Foundation	Consórcio R3
Ledger	Público	Privado	Privado
Modo de operação	Não permissionada	Permissionada	Permissionada
Mecanismo de consenso	Proof-of-Stake	Abordagem ampla, permite múltiplos mecanismos	Consenso específico (nós notários)
Contratos inteligentes	Solidity, C/C++, LLL	Go, Java, JavaScript	Kotlin, Java
Moeda	- Ether - Tokens criados por contracto inteligente	- Sem moeda nativa - Tokens por *chaincode*	Sem moeda nativa

Fonte: (Valenta & Sandner, 2017)

Dentre os frameworks analisados, o Ethereum foi selecionado para o desenvolvimento do protótipo deste trabalho por reunir características que melhor se alinham ao contexto de um sistema de votação electrónica aberto e verificável. Diferente do Hyperledger Fabric e do Corda, que operam em ambientes permissionados e são mais voltados ao sector empresarial, o Ethereum é uma plataforma pública e descentralizada, o que facilita a implementação dos princípios de transparência, verificabilidade pública e acesso aberto ao código e às transacções, que são elementos fundamentais para garantir a confiança dos eleitores.

Adicionalmente, o Ethereum oferece suporte nativo a contratos inteligentes e possui um ecossistema maduro, com ampla documentação, ferramentas de desenvolvimento e redes de teste (testnets[2]), facilitando a construção, teste e demonstração de aplicações blockchain sem a necessidade de infraestrutura própria.

2.4. Aplicabilidade da Blockchain em Sistemas de Votação

A tecnologia blockchain tem demonstrado grande potencial para modernizar processos que exigem alta segurança, transparência e confiabilidade. Um dos campos em que sua aplicação vem ganhando destaque é em sistemas de votação electrónica. Embora o voto seja um processo de natureza política, sua execução técnica pode beneficiar-se significativamente da descentralização oferecida pela blockchain. Segundo Singhal (2018), há casos de uso em que a descentralização técnica é essencial, ainda que o controle político permaneça sob responsabilidade de governos, como é o caso do registo de propriedades, gestão de veículos e, especialmente, da votação electrónica.

Ao incorporar blockchain nos sistemas de votação, torna-se possível garantir um processo mais robusto e resistente a interferências maliciosas (Tanwar, 2022). Isso se deve, em grande parte, às propriedades fundamentais da blockchain, como a imutabilidade dos dados, a criptografia de ponta a ponta e o consenso distribuído.

De acordo com (Hardwick et al., 2018), os principais benefícios da utilização da blockchain em sistemas de votação incluem:

---

[2] Uma testnet é uma rede blockchain separada, concebida para fins de teste no âmbito da tecnologia blockchain.

- **Maior transparência**: graças ao caráter público e auditável do ledger.
- **Anonimato**: garantido através da separação entre a identidade do eleitor e seu voto.
- **Segurança e confiabilidade**: especialmente contra ataques como os de negação de serviço (DoS - Denial-of-Service).
- **Imutabilidade**: que assegura a integridade tanto do processo eleitoral quanto de cada voto individual.

2.4.1. Casos de uso da blockchain na votação

O uso de blockchain em sistemas electrónicos de votação tem ganhado destaque em diversos países e instituições como uma tentativa de tornar os processos eleitorais mais confiáveis, transparentes e resistentes a fraudes. Governos e empresas privadas vêm desenvolvendo soluções baseadas nessa tecnologia, enquanto a academia se dedica à identificação de vulnerabilidades e ao aperfeiçoamento de algoritmos que tornem os sistemas mais justos e resilientes (Vladucu et al., 2023).

Diversos países já realizaram testes ou implementações práticas da tecnologia, como Estónia, Austrália, Rússia, Noruega, Suíça, Alemanha, Serra Leoa, Quénia, Marrocos, Índia e Japão. Para ilustrar esse cenário, destacam-se a seguir alguns casos emblemáticos, tanto institucionais quanto privados.

Austrália

Em 2015, o estado de New South Wales realizou um projecto piloto de votação electrónica utilizando blockchain durante as eleições gerais estaduais. Cerca de 280 mil cidadãos participaram por meio da plataforma Scytl. O processo era baseado em autenticação com um ID e um PIN de seis dígitos. Após votar, o eleitor recebia um número de recibo com 12 dígitos, permitindo verificar posteriormente se o seu voto foi corretamente registrado no sistema (Vladucu et al., 2023; Vote Australia, 2019).

Esse modelo visava garantir transparência, auditabilidade e confiança no sistema, unindo a conveniência do voto remoto à segurança proporcionada pela infraestrutura criptográfica da blockchain.

Estónia

Pioneira no voto online, a Estónia introduziu o voto pela Internet já em 2005. O sistema estoniano é suportado por uma infraestrutura nacional de identidade digital altamente desenvolvida. Cada cidadão possui um Cartão de Identidade (ID-card) com chip criptografado, ligado a uma Infraestrutura de Chaves Públicas, obrigatória no país.

O eleitor descarrega a aplicação de votação, autentica-se com seu ID eletrónico e, se elegível, visualiza a lista de candidatos e vota. Toda a operação é registrada de forma segura e rastreável, mantendo o anonimato do voto. A experiência da Estónia é frequentemente referida como um dos modelos mais avançados de democracia digital (Heiberg et al., 2011).

Rússia

A Rússia começou a explorar a votação digital em 2014, abrangendo mais de dois milhões de utilizadores. Em 2017, residentes de Moscovo utilizaram a tecnologia blockchain para eleger membros do conselho municipal. Posteriormente, o país passou a utilizar a blockchain da plataforma Waves, que adopta um algoritmo de consenso baseado em Proof of Authority com tolerância a falhas.

Nesse sistema, contratos inteligentes armazenam as regras do processo eleitoral, as informações de registo dos eleitores e os mecanismos de verificação dos votos. Com isso, busca-se garantir integridade, auditabilidade e rapidez no apuramento dos resultados (Vakarjuk et al., 2022; Vladucu et al., 2023).

Quénia

Durante as eleições presidenciais de 2022, o Quénia implementou um sistema de votação que incorporava princípios inspirados na tecnologia blockchain, mesmo sem utilizar diretamente uma blockchain pública. A Comissão Eleitoral Independente e de Fronteiras (IEBC) utilizou o Kenya Integrated Electoral Management System (KIEMS), que combinava dispositivos biométricos para autenticação de eleitores e a transmissão electrónica segura de resultados. Cada estação de votação operava como um nó independente, onde os resultados eram digitalizados, assinados com códigos QR e enviados para os servidores centrais da IEBC. A descentralização parcial e a rastreabilidade dos dados permitiram um grau elevado de transparência, possibilitando que qualquer cidadão com acesso aos formulários digitalizados pudesse acompanhar e verificar os resultados oficiais (Kawamara & Mutawe, 2022). Segundo Kamau (2022), esta abordagem inspirada pela lógica da

blockchain ajudou a mitigar dúvidas sobre fraude e contribuiu para um processo eleitoral mais confiável.

Marrocos

Em 2024, pesquisadores marroquinos propuseram e testaram um sistema de votação electrónica baseado na blockchain Solana, com o objectivo de melhorar a transparência e a integridade das eleições no país. O sistema desenvolvido combina a Tecnologia de Ledger Distribuído Permissionado com a blockchain pública Solana, criando uma infraestrutura em múltiplas camadas que assegura que os votos sejam armazenados de forma segura, verificável, imutável e auditável. Cada voto é encriptado e assinado digitalmente antes de ser registado no ledger, o que garante tanto o anonimato quanto a auditabilidade individual (Chafiq et al., 2024). O estudo destaca a eficácia da tecnologia blockchain em mitigar fraudes eleitorais e manipulações, enfatizando a importância de um design e execução meticulosos para o sucesso da implementação.

FollowMyVote

O FollowMyVote é um software de código aberto que aplica a tecnologia blockchain para garantir a integridade e auditabilidade das eleições digitais. O sistema utiliza um par de chaves criptográficas para autenticar cada eleitor, e caso o voto seja validado, ele é armazenado na blockchain como uma transacção imutável (Follow My Vote, 2024).

O eleitor tem sua identidade verificada digitalmente e recebe uma cédula virtual para preenchimento. Após o voto, o sistema permite que o próprio eleitor verifique se seu voto foi devidamente armazenado, além de possibilitar a auditoria dos demais votos na urna (Sepúlvida & Paiva, 2019). A transparência é reforçada pelo fato de que o código-fonte está disponível publicamente, permitindo auditoria por qualquer cidadão.

Voatz

O aplicativo Voatz foi utilizado como alternativa às urnas eletrônicas nas eleições do estado da Virgínia Ocidental (EUA) em 2018, com o objectivo de promover maior eficiência, transparência e integridade ao processo eleitoral. O sistema requer que os eleitores utilizem dispositivos móveis com autenticação biométrica e reconhecimento facial, o que, apesar de aumentar a segurança, impõe restrições quanto à acessibilidade, dado que nem todos os dispositivos possuem esses recursos (Zhang et al., 2018).

Uma vez lançado, o voto é imutavelmente armazenado na blockchain do aplicativo. Após a eleição, os eleitores recebem um recibo digital assinado, contendo suas escolhas, que pode ser utilizado para verificar a correspondência com o registo na blockchain. Esse mecanismo permite a realização de auditorias pós-eleitorais, garantindo a integridade do processo.

Esses casos demonstram o potencial da blockchain como uma aliada da democracia digital, ao permitir maior auditabilidade, segurança e participação remota. No entanto, apesar dos avanços tecnológicos, os desafios relacionados à equidade no acesso, confiabilidade dos dispositivos e resistência à manipulação política ainda exigem atenção contínua de governos, desenvolvedores e da sociedade civil.

3. Capítulo III – Caso de estudo: Núcleo de Estudantes de Direito da UEM

O Núcleo dos Estudantes de Direito (NED) da Universidade Eduardo Mondlane é a organização representativa dos estudantes da Faculdade de Direito, responsável por promover a participação estudantil, defender os interesses académicos e coordenar atividades extracurriculares. A sua atuação é regulada por estatutos próprios e por um Regulamento Eleitoral, aprovado por deliberação da Comissão Eleitoral em 2012 (Regulamento Eleitoral, 2012).

3.1. Estrutura do NED

A estrutura do NED assenta num corpo diretivo eleito, cujo mandato tem a duração de dois anos. Este corpo é composto por um presidente, vice-presidente, secretário e chefes de departamentos. A existência de departamentos e representantes por turno garante a organização interna e a cobertura das diferentes áreas de atuação do núcleo, conforme confirmado pelo actual presidente do núcleo em entrevista realizada para este estudo (Agnese Arnaldo, comunicação pessoal, 5 de junho de 2025).

3.2. Processo Eleitoral no Núcleo de Estudantes de Direito da UEM

Conforme descrito pelo Regulamento Eleitoral (2012), as eleições no NED decorrem em ciclos bienais, com o objectivo de eleger a nova direção para um mandato de dois anos. O processo é conduzido pela Comissão Eleitoral (CE), órgão independente responsável por garantir a legalidade, imparcialidade e organização de todas as etapas, desde a elaboração do calendário até à tomada de posse dos eleitos.

A CE é composta por até 13 membros, assegurando representação de todas as turmas, incluindo os turnos diurno e pós-laboral, e deve incluir pelo menos um elemento com experiência em processos eleitorais anteriores. A seleção dos membros da comissão é realizada por sorteio entre os estudantes elegíveis. De acordo com o artigo 12 do Regulamento Eleitoral do NED, o processo eleitoral segue as seguintes fases principais:

I. Composição da Comissão Eleitoral;
II. Abertura e verificação das candidaturas;
III. Publicação das listas apuradas;
IV. Campanha eleitoral (com duração mínima de 10 e máxima de 20 dias úteis);
V. Votação, apuramento e publicação dos resultados;

VI. Tomada de posse dos eleitos.

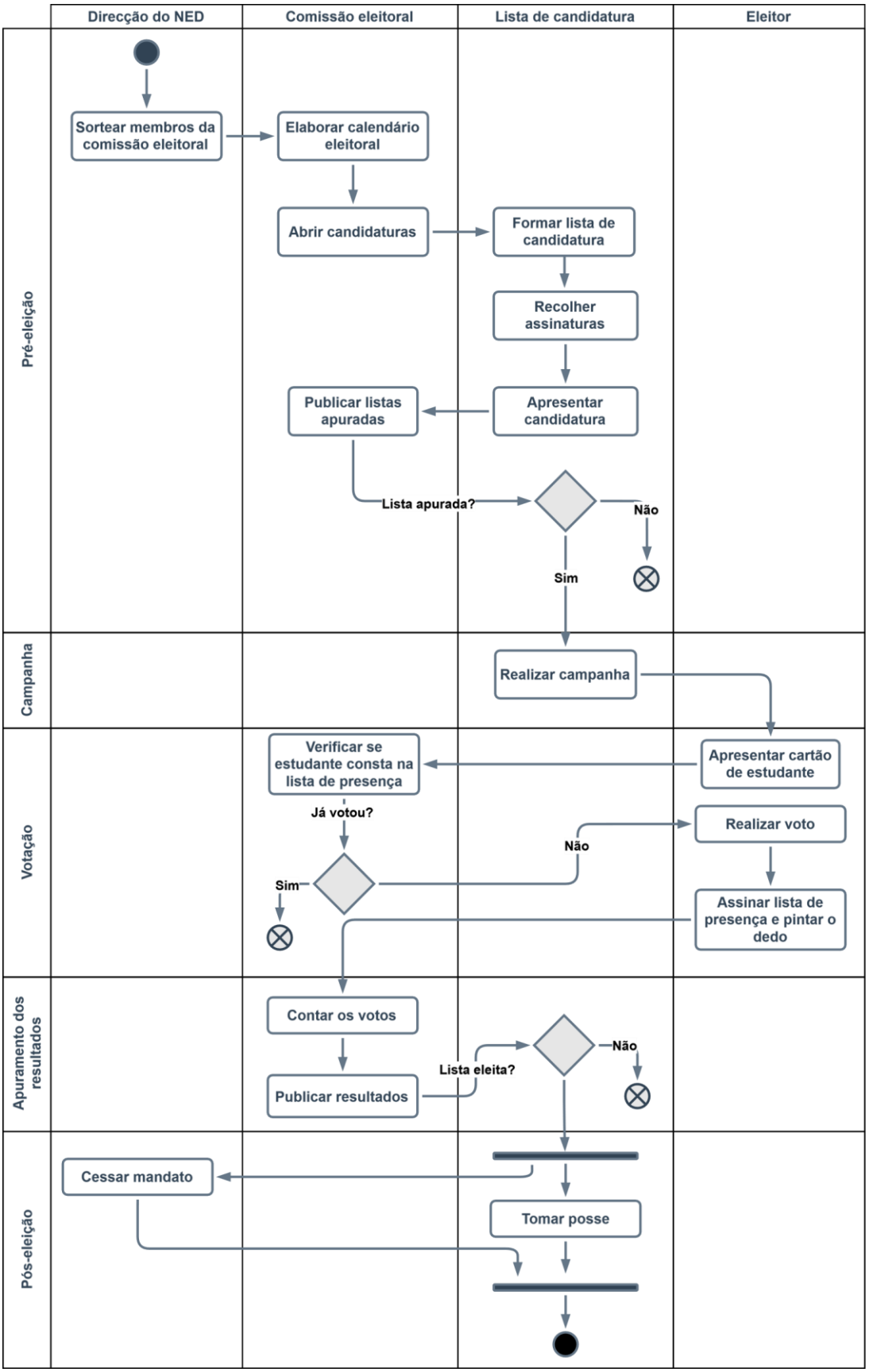


Figura 6: Processo eleitoral do NED

As listas candidatas devem apresentar uma composição completa para os cargos a preencher, um programa de ação e ser subscritas por, no mínimo, 100 estudantes. De acordo com o regulamento, apenas estudantes do 2.º e 3.º anos podem concorrer ao cargo de presidente do NED, estando excluídos estudantes do 1.º e do último ano, como forma de garantir estabilidade e continuidade na gestão.

A votação realiza-se exclusivamente nas dependências da Faculdade de Direito, permitindo um controlo direto e rigoroso. Os eleitores devem apresentar o cartão de estudante ou, na sua ausência, o comprovativo de inscrição. Após a votação, cada eleitor assina a lista de presença e pinta o dedo, como forma de autenticação. O regulamento ainda prevê o credenciamento de observadores eleitorais, a presença de delegados de lista e a publicação dos resultados finais por edital.

3.2.1. Desafios e Limitações do Processo Actual

Apesar da estrutura normativa clara e da organização do processo, o modelo eleitoral actualmente praticado pelo NED enfrenta limitações que afetam diretamente a sua eficácia e inclusividade. Os principais desafios identificados são:

- **Falta de participação**: A votação ocorre de forma presencial e exclusivamente em um único dia letivo, o que resulta em longas filas e conflitos com atividades académicas, como aulas e avaliações. A situação agrava-se no caso dos estudantes do turno pós-laboral e daquelas turmas que frequentam aulas fora da Faculdade de Direito, como na Faculdade de Medicina ou no campus central da UEM, o que leva a elevados níveis de abstenção.
- **Perceção de imparcialidade comprometida**: Embora não existam registos formais de fraude, o ambiente de familiaridade entre estudantes e membros da Comissão Eleitoral pode gerar desconfiança quanto à neutralidade do processo, sobretudo em situações de competição acirrada entre listas.
- **Ausência de mecanismos de feedback**: Após o término das eleições, não há um processo estruturado para recolher opiniões e sugestões dos eleitores. Isso impede que a Comissão Eleitoral e o núcleo em geral identifiquem pontos de melhoria com base na experiência dos próprios estudantes.

- **Restrição física da votação**: A limitação da votação a um único espaço físico e período temporal compromete a acessibilidade e a flexibilidade do processo, dificultando a participação daqueles com impedimentos logísticos.

3.3. Solução proposta para o processo eleitoral

Como resposta aos desafios identificados no processo eleitoral actual do NED, propõe-se a implementação de um sistema de votação electrónica que auxilie a Comissão Eleitoral na gestão de todo o processo, ao mesmo tempo que ofereça aos eleitores uma experiência mais acessível, segura e transparente. O sistema visa manter os princípios de transparência, imparcialidade e controlo estabelecidos pelo regulamento do NED, mas com ganhos substanciais em eficiência, rastreabilidade e participação. A utilização do sistema está dividida em duas fases principais, conforme ilustrado nos diagramas seguintes.

Fase 1: Preparação

Após a constituição da Comissão Eleitoral e a validação das candidaturas, os dados das listas aprovadas e dos eleitores aptos são registados na aplicação. Esta etapa visa assegurar que apenas os estudantes elegíveis possam participar na votação.

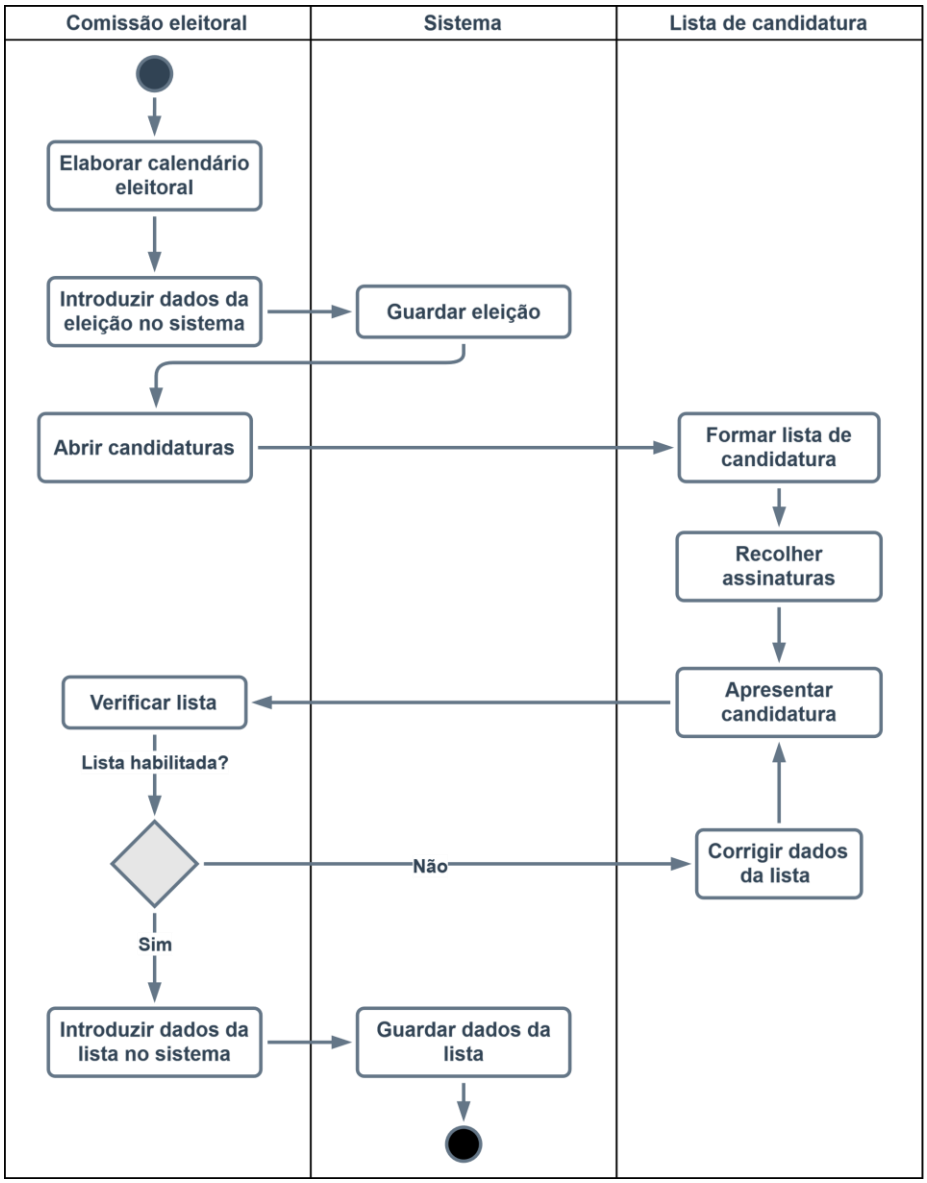


Figura 7: Processo eleitoral proposto - Fase 1

Fase 2: Votação e resultados

No dia da eleição, os eleitores autenticam-se no sistema e registam o seu voto. Ao encerrar o período de votação, o sistema realiza automaticamente a contagem dos votos e publica os resultados finais, que podem ser auditados por todas as partes interessadas.

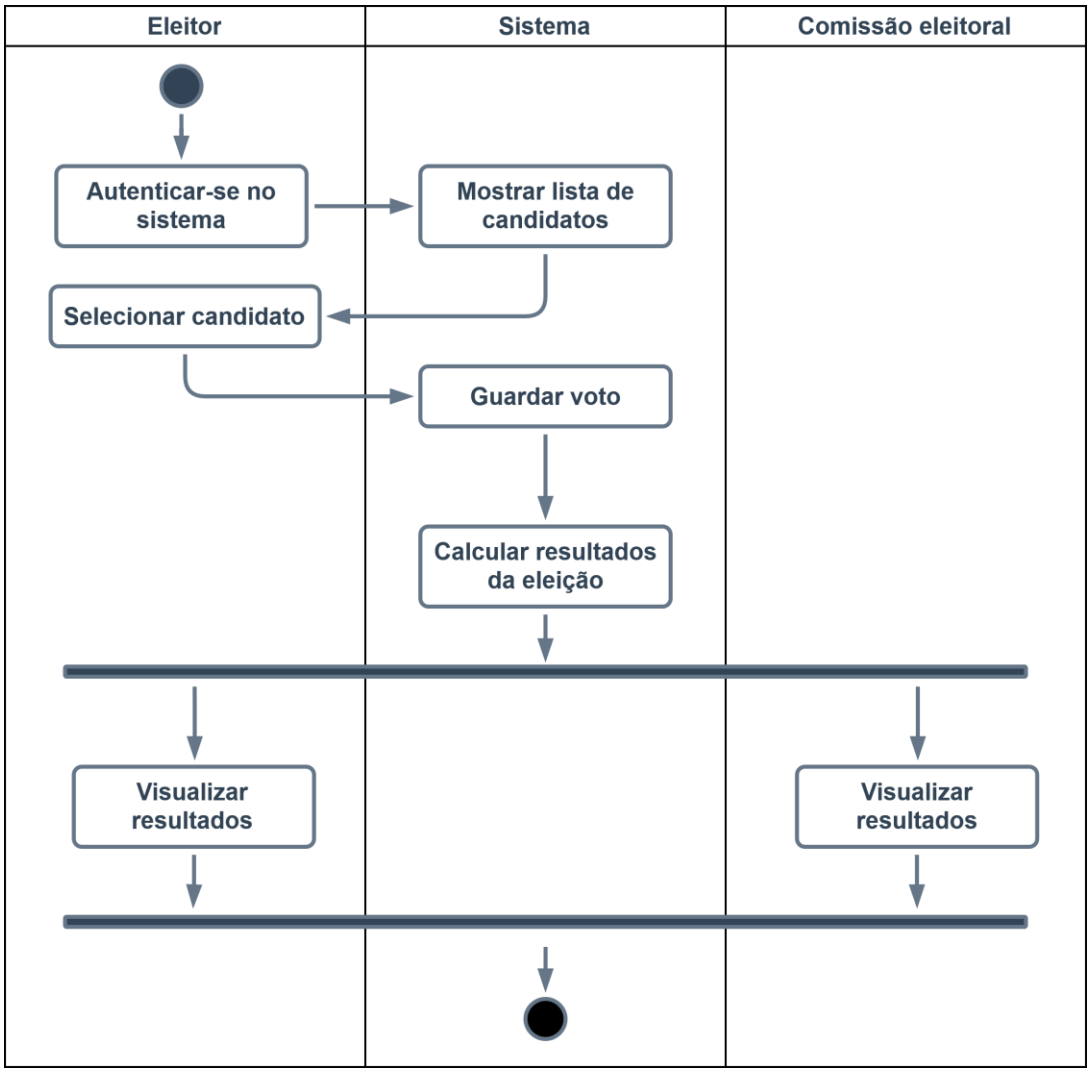


Figura 8: Processo eleitoral proposto - Fase 2

Arquitetura Técnica da Solução

A infraestrutura da solução baseia-se na plataforma Ethereum, escolhida por oferecer características adequadas a sistemas de votação electrónica, como descentralização, imutabilidade dos dados, auditabilidade pública e suporte a contratos inteligentes.

O sistema será composto por uma aplicação web com uma interface simples e acessível, permitindo aos utilizadores finais realizar operações como o registo de eleitores e a submissão de votos. Essa interface estará conectada aos contractos inteligentes implementados na blockchain Ethereum.

Os contractos inteligentes serão responsáveis por assegurar o cumprimento das regras do processo eleitoral, incluindo a verificação da elegibilidade dos eleitores, a garantia de voto único por eleitor e a contagem automatizada dos votos. Todos os votos serão registados

como transações imutáveis na blockchain, assegurando a integridade, verificabilidade e total transparência do processo.

4. Capítulo IV - Desenvolvimento da solução proposta

Este capítulo descreve o processo de construção da solução de votação eletrônica baseada em blockchain, partindo dos requisitos levantados até à implementação do protótipo funcional. A abordagem adotada segue as etapas do modelo em cascata, conforme apresentado no Capítulo I. A proposta tem como objectivo garantir segurança, transparência e verificabilidade no processo eleitoral, utilizando a tecnologia Ethereum como base para o armazenamento e validação dos votos.

4.1. Análise e definição de Requisitos

De acordo com Sommerville (2011), os requisitos de um sistema consistem nas descrições sobre o que o sistema deve fazer, os serviços que deve oferecer e as restrições que limitam o seu funcionamento. Esses requisitos podem ser organizados em duas categorias principais: requisitos funcionais e requisitos não funcionais.

Para esta pesquisa, os requisitos foram classificados com base em níveis de prioridade, utilizando os seguintes critérios:

- **Essencial**: requisito sem o qual o sistema não cumpre seu propósito. É considerado indispensável e deve ser implementado já na primeira versão funcional do software.
- **Importante**: requisito que agrega valor ao sistema e aprimora suas funcionalidades principais, mas cuja ausência não inviabiliza o funcionamento essencial.
- **Desejável**: requisito opcional que melhora a experiência do usuário ou a eficiência do sistema, mas que pode ser adiado ou até mesmo não implementado, sem comprometer a operação básica da solução.

4.1.1. Requisitos Funcionais

Conforme definido por Sommerville (2011), os requisitos funcionais descrevem os comportamentos e funcionalidades específicas que o sistema deve oferecer, como a forma de resposta a determinadas entradas e o comportamento esperado em diferentes cenários de uso. Em alguns casos, também podem incluir limitações explícitas sobre o que o sistema não deve permitir.

A Tabela 4 apresenta os requisitos funcionais identificados para o sistema proposto:

Tabela 4: Requisitos funcionais

Referência	Requisito	Descrição	Prioridade
RF01	Cadastro de eleitores	O sistema deve permitir o cadastro dos eleitores elegíveis, feito pela comissão eleitoral.	Essencial
RF02	Autenticação de utilizadores	O sistema deve permitir que os utilizadores se autentiquem para permitir acesso ao processo de votação.	Essencial
RF03	Cadastro de eleições	A comissão eleitoral deve poder criar novas eleições.	Essencial
RF04	Cadastro de candidatos	O sistema deve permitir o registo de candidatos para cada eleição.	Essencial
RF05	Registo de voto	O sistema deve permitir que o eleitor vote apenas uma vez e registar o voto na blockchain.	Essencial
RF07	Consolidar resultados	O sistema deve calcular automaticamente os resultados da eleição após o encerramento.	Essencial
RF08	Visualizar resultados	O sistema deve permitir que os resultados da eleição sejam visualizados publicamente.	Essencial
RF09	Auditoria Pública	O sistema deve permitir auditoria das transacções de votação diretamente na blockchain.	Importante

4.1.2. Requisitos Não Funcionais

De acordo com Sommerville (2011), os requisitos não funcionais dizem respeito às restrições e qualidades gerais que o sistema deve apresentar, independentemente das funcionalidades específicas. Eles incluem características como desempenho, segurança, usabilidade, confiabilidade, escalabilidade, entre outras. Embora não descrevam

diretamente os serviços oferecidos, são fundamentais para garantir que o sistema funcione de maneira eficiente, segura e com boa experiência para os utilizadores.

Tabela 5: Requisitos não funcionais

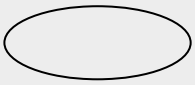
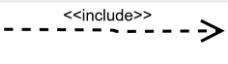
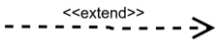
Referência	Requisito	Descrição	Prioridade
RNF01	Segurança	O sistema deve garantir a proteção contra fraudes, acesso não autorizado e alteração dos dados de votação.	Essencial
RNF02	Disponibilidade	O sistema deve estar disponível durante todo o período eleitoral, sem interrupções críticas.	Essencial
RNF03	Desempenho	O sistema deve registar e validar votos em tempo razoável, com baixa latência.	Importante
RNF04	Usabilidade	A interface do sistema deve ser simples e intuitiva, permitindo que os utilizadores votem com facilidade.	Importante
RNF05	Escalabilidade	O sistema deve ser capaz de lidar com um número crescente de utilizadores e votos sem comprometer o desempenho.	Desejável
RNF06	Auditabilidade	O sistema deve permitir a auditoria dos votos registados de forma transparente e verificável.	Essencial

4.1.3. Diagrama de Casos de Uso

Segundo Stadzisz (2002), o modelo de casos de uso serve como um instrumento para descrição das intenções ou requisitos para um sistema computacional. Conforme descreve Sommerville (2011), um caso de uso identifica os actores envolvidos em uma interacção e dá nome ao tipo de interacção . Essa é, então, suplementada por informações adicionais que descrevem a interacção com o sistema.

Os casos de uso de um projecto de software são descritos na linguagem UML através de Diagramas de Casos de Uso. Estes diagramas utilizam como primitivas Actores, Casos de Uso e Relacionamentos (Stadzisz, 2002).

Tabela 6: Elementos do diagrama de casos de uso

Elemento	Anotação	Descrição
Actor		Actores são representações de entidades externas, mas que interagem com o sistema durante sua execução.
Caso de uso		Descrição dos serviços a serem oferecidos pelo sistema.
Associação		Indica uma interacção entre o actor e o caso de uso.
Inclusão		É uma relação estrutural através da qual um caso de uso insere em seu interior um outro caso de uso.
Extensão		É uma relação estrutural entre dois casos de uso através da qual um caso de uso maior é estendido por um caso de uso menor.

Fonte: Stadzisz (2002)

O diagrama de casos de uso apresentado a seguir resume graficamente as interações fundamentais do sistema proposto, servindo como base para a compreensão dos requisitos funcionais e para o posterior projecto e implementação da solução.

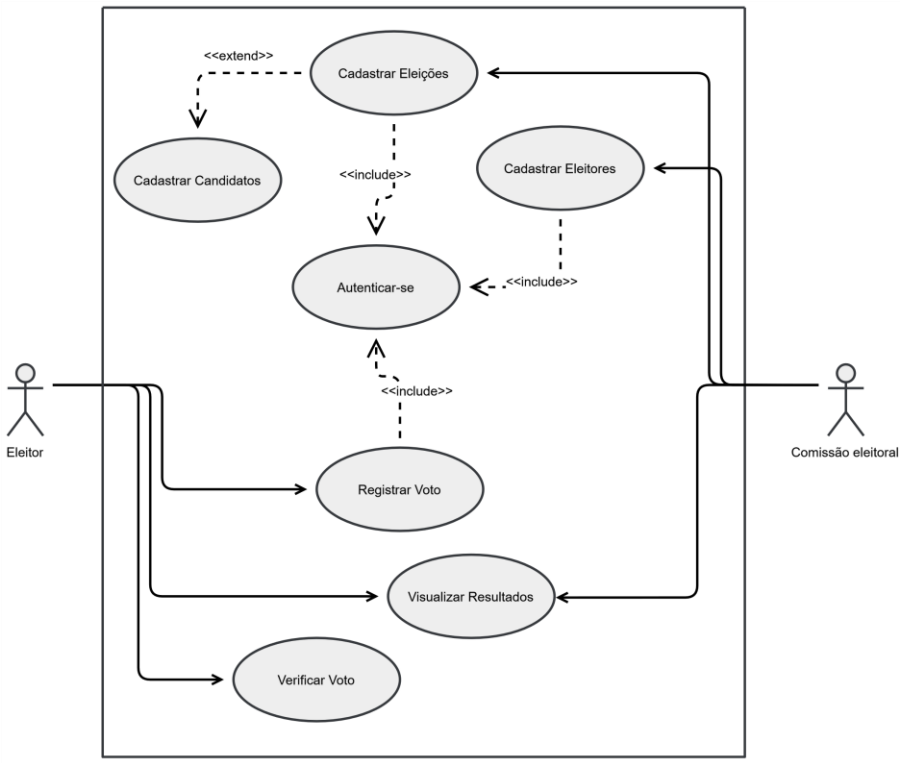


Figura 9: Diagrama de casos de uso

4.2. Projecto de Sistema e software

Segundo Mall (2019), a fase de projecto tem como objectivo transformar os requisitos do sistema em uma estrutura organizada e adequada para implementação em uma linguagem de programação. Para Sommerville (2011), é nesta fase onde identificam-se e definem-se as principais abstrações do sistema, bem como os relacionamentos entre elas, estabelecendo assim a arquitetura que orientará todo o desenvolvimento.

Nesta seção, será apresentada a arquitetura do sistema proposto, incluindo a organização dos seus principais componentes, a estrutura de comunicação entre eles e os fluxos operacionais esperados. Serão utilizados diagramas ilustrativos para apoiar a compreensão da estrutura técnica e do funcionamento geral da solução.

4.2.1. Arquitetura do sistema

De acordo com Tremblay (2001), a arquitetura de software consiste na descrição dos subsistemas e componentes de um sistema, bem como dos relacionamentos existentes entre eles. Nesta secção, o autor apresenta os principais componentes da arquitetura proposta para a solução de votação electrónica baseada em blockchain, com cinco

componentes principais: Interface do Utilizador, Middleware, servidor, autenticação e a Blockchain.

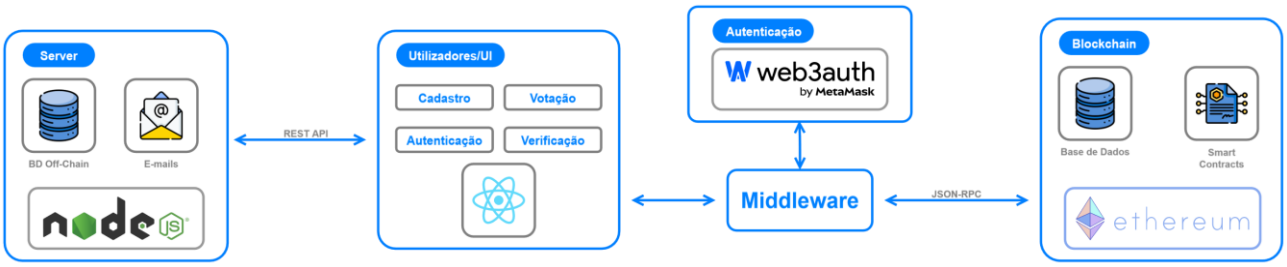


Figura 10: Arquitetura do sistema

Interface do utilizador

Esta camada corresponde à interface gráfica com a qual o utilizador interage diretamente. Por meio dela, os eleitores podem realizar operações como autenticação, acesso à cédula eleitoral, lançamento do voto e consulta dos resultados. A interface é concebida para ser simples, intuitiva, responsiva e acessível via navegador web.

Middleware

A camada de middleware actua como intermediária entre a interface do utilizador e a blockchain. É responsável por processar as solicitações do frontend, comunicar-se com os contratos inteligentes e garantir que apenas ações válidas sejam transmitidas à blockchain.

Autenticação

Esta camada é responsável por gerir todo o processo de autenticação dos utilizadores, assegurando uma experiência de acesso simplificada e segura. Utiliza uma abordagem que abstrai o uso direto do endereço da carteira blockchain, permitindo que os utilizadores se autentiquem por meio de mecanismos familiares (como email) enquanto, por trás dos panos, associa-se de forma segura um endereço de carteira ao utilizador. Isso reduz a complexidade técnica para o eleitor e mantém a integridade do processo de identificação.

Servidor

A camada de servidor é responsável por armazenar e processar informações sensíveis que não devem ser gravadas na blockchain, como dados pessoais dos eleitores. Essa separação visa garantir a privacidade dos utilizadores e evitar que seja possível, a partir dos dados públicos da blockchain, estabelecer uma ligação entre o endereço da carteira e a identidade do eleitor, preservando assim o anonimato do voto. Além disso, esta camada

também inclui serviços complementares, como o servidor de email, utilizado para enviar notificações e códigos de verificação aos utilizadores durante o processo de autenticação.

Blockchain

A camada blockchain é o núcleo de persistência e validação do sistema. É nela que os contractos inteligentes são armazenados e executados, e onde ficam registadas de forma imutável todas as transacções correspondentes aos votos.

Os contratos inteligentes implementam a lógica central da eleição. Neles estão definidos os processos de registo de eleitores e candidatos, a gestão das fases da eleição (início, votação e encerramento), o armazenamento dos votos e o cálculo automático dos resultados. Esses contratos são executados de forma descentralizada e garantem que todas as regras da eleição sejam cumpridas sem intervenção manual. Através da blockchain, garante-se a transparência, segurança e verificabilidade pública do processo eleitoral.

4.2.2. Modelagem de dados

A modelagem de dados tem como objectivo representar de forma estruturada os principais elementos do sistema e suas relações. Embora a solução proposta utilize contractos inteligentes em uma blockchain (que não segue o modelo relacional tradicional), é importante definir as entidades principais envolvidas no processo eleitoral, bem como os seus atributos e vínculos lógicos. Esta modelagem serve de base para a implementação dos contractos inteligentes, da base de dados off-chain e das regras de negócio do sistema.

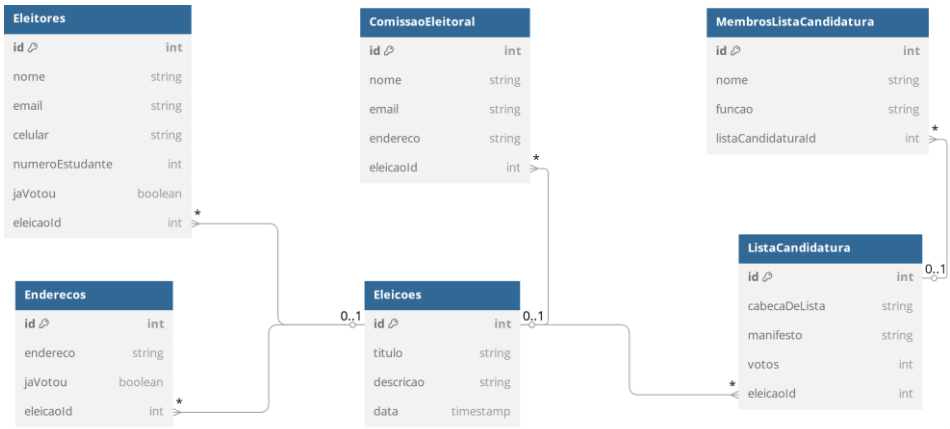


Figura 11: Modelo de dados

4.2.3. Design da interface do utilizador

O design da interface do utilizador tem como objectivo garantir uma interacção simples, intuitiva e segura com o sistema de votação. Para este trabalho, foram definidos os principais ecrãs que suportam as funcionalidades essenciais tanto para os eleitores quanto para os membros da comissão eleitoral.

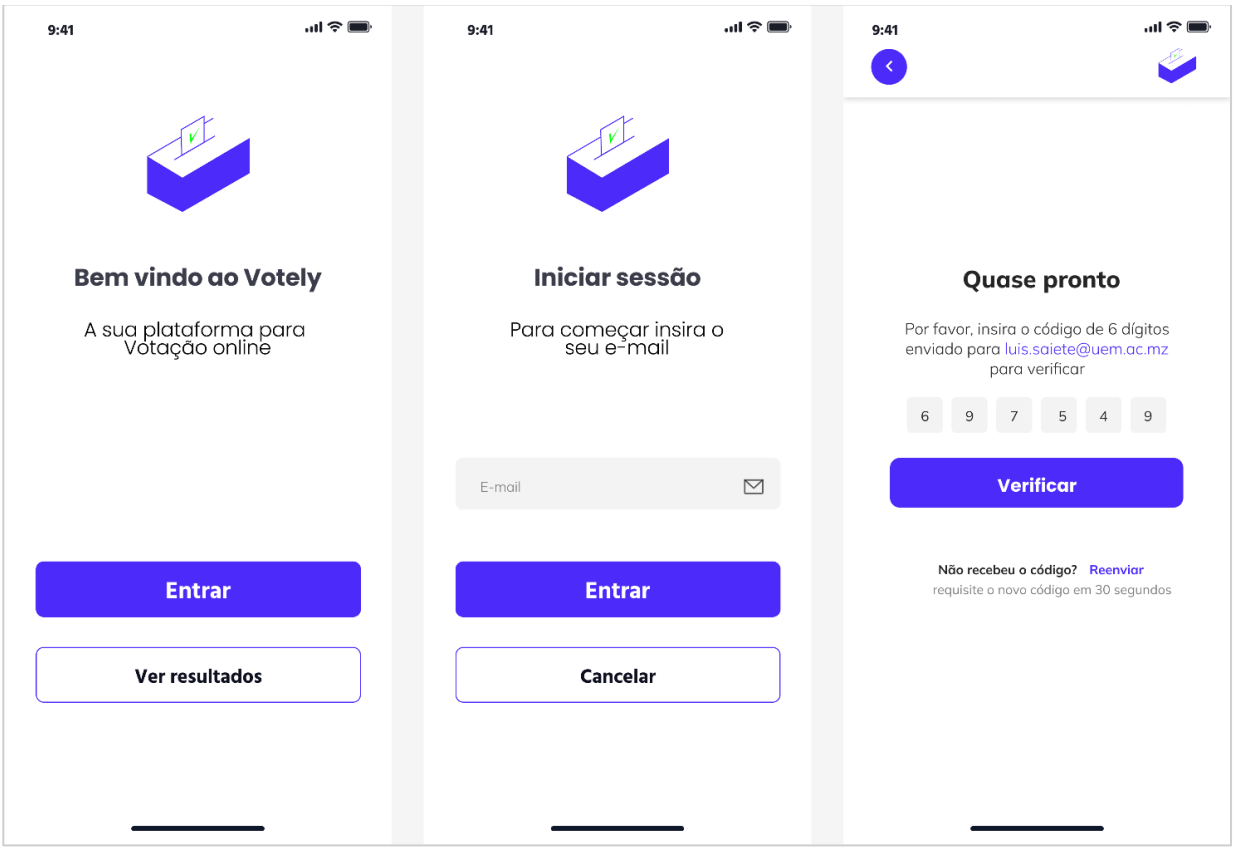


Figura 12: Telas para autenticação de utilizadores

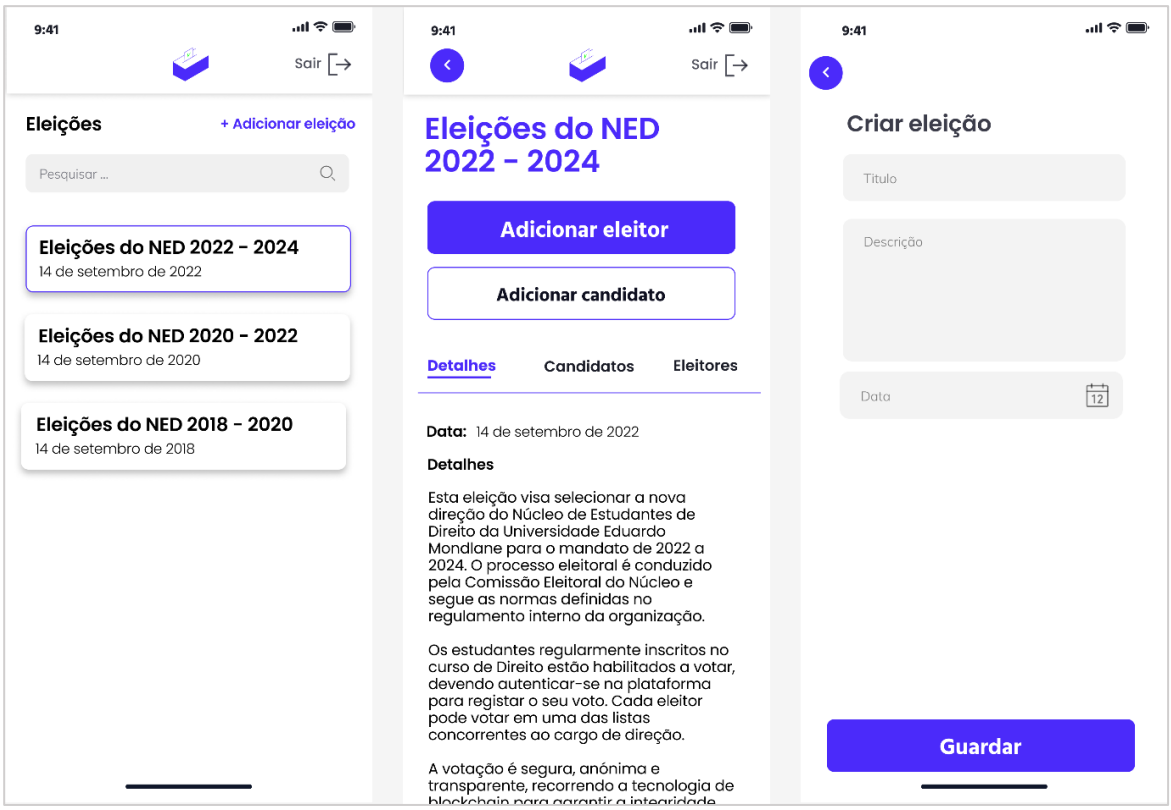


Figura 13: Telas para gestão de eleições

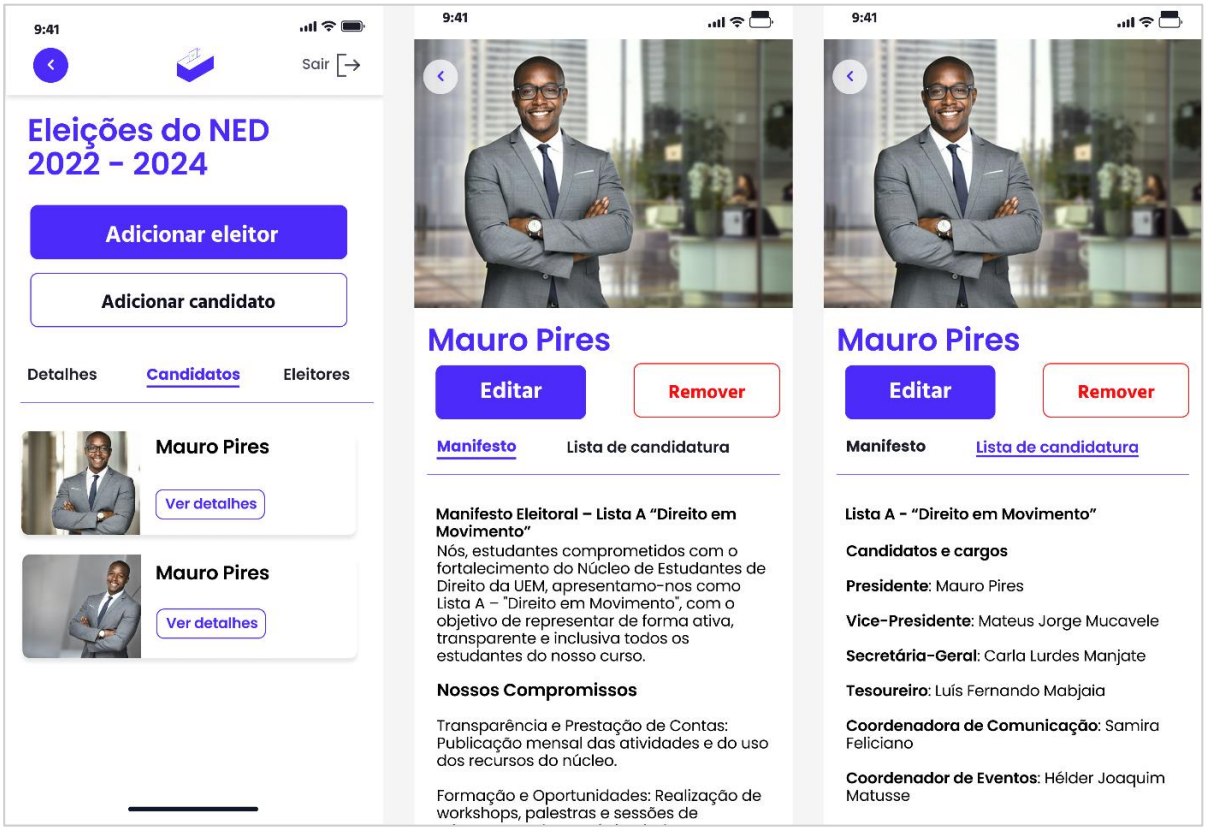


Figura 14: Telas para gestão de candidatos

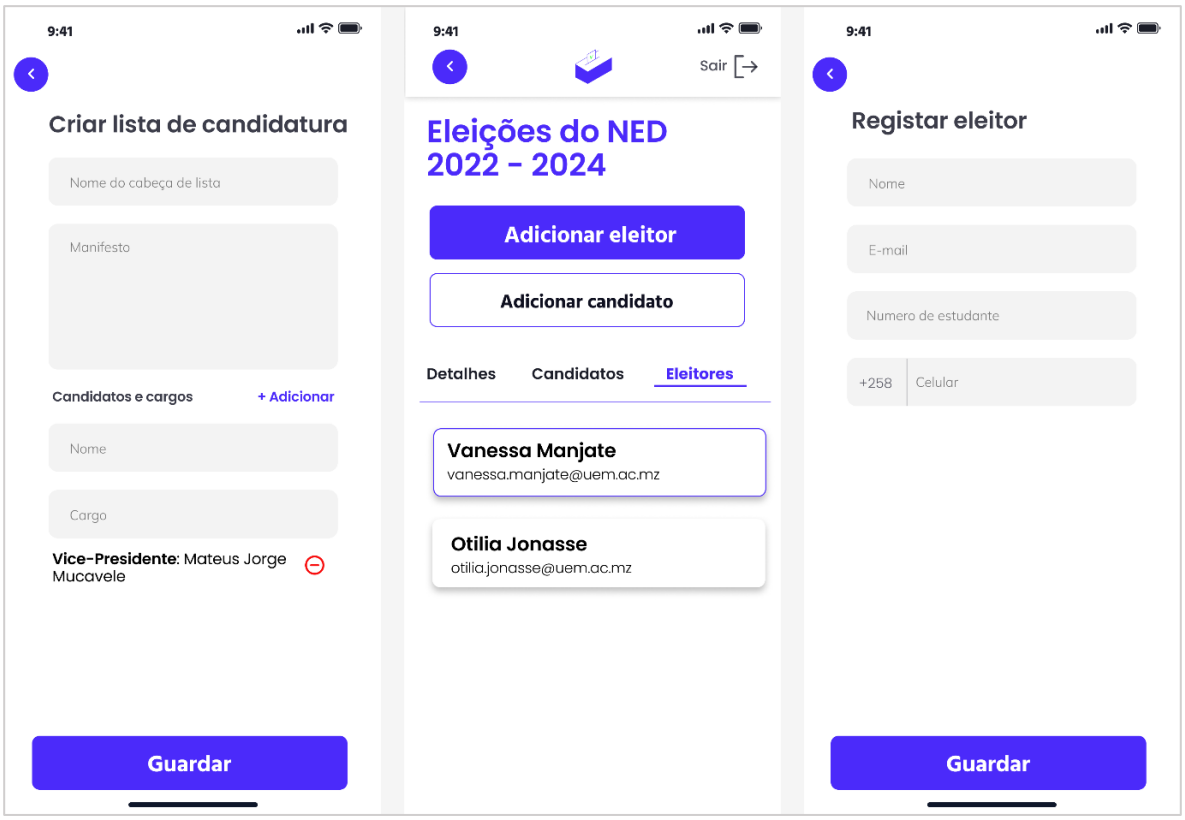


Figura 15: Telas para registo de candidatos e eleitores

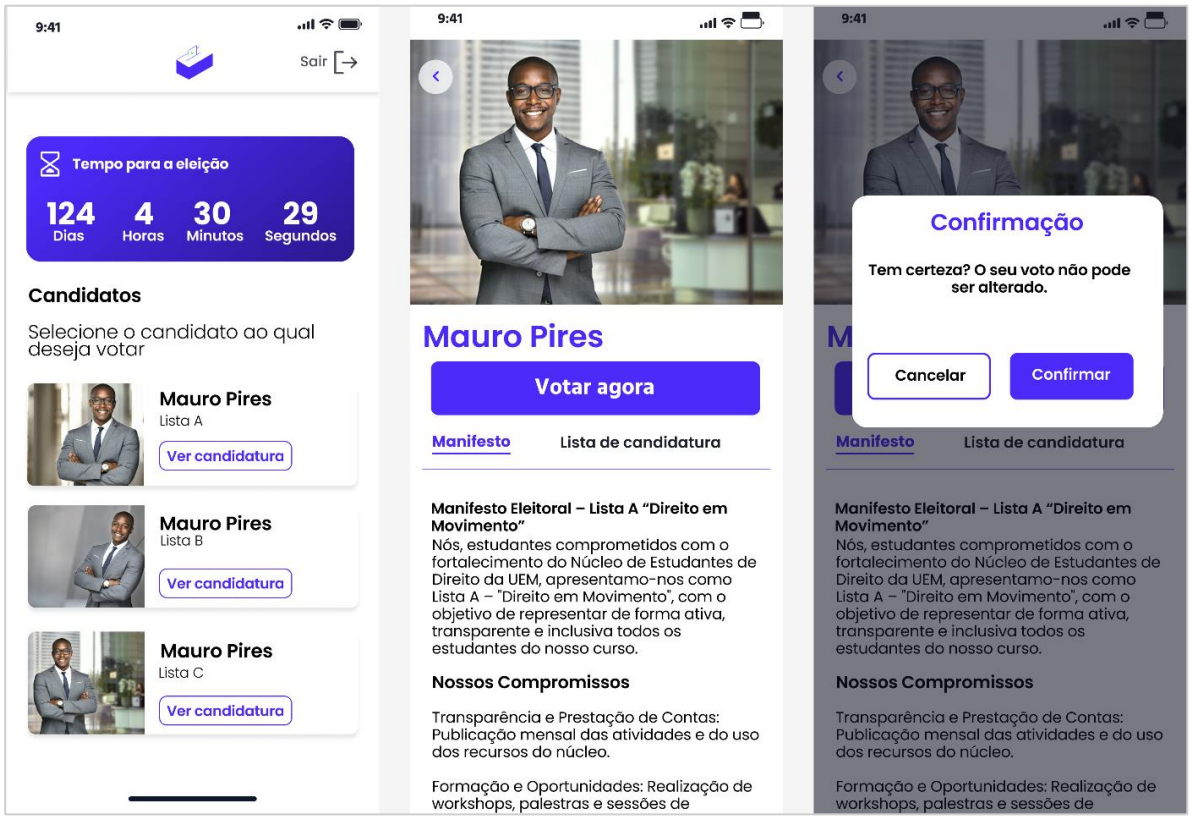


Figura 16: Telas para registo de voto

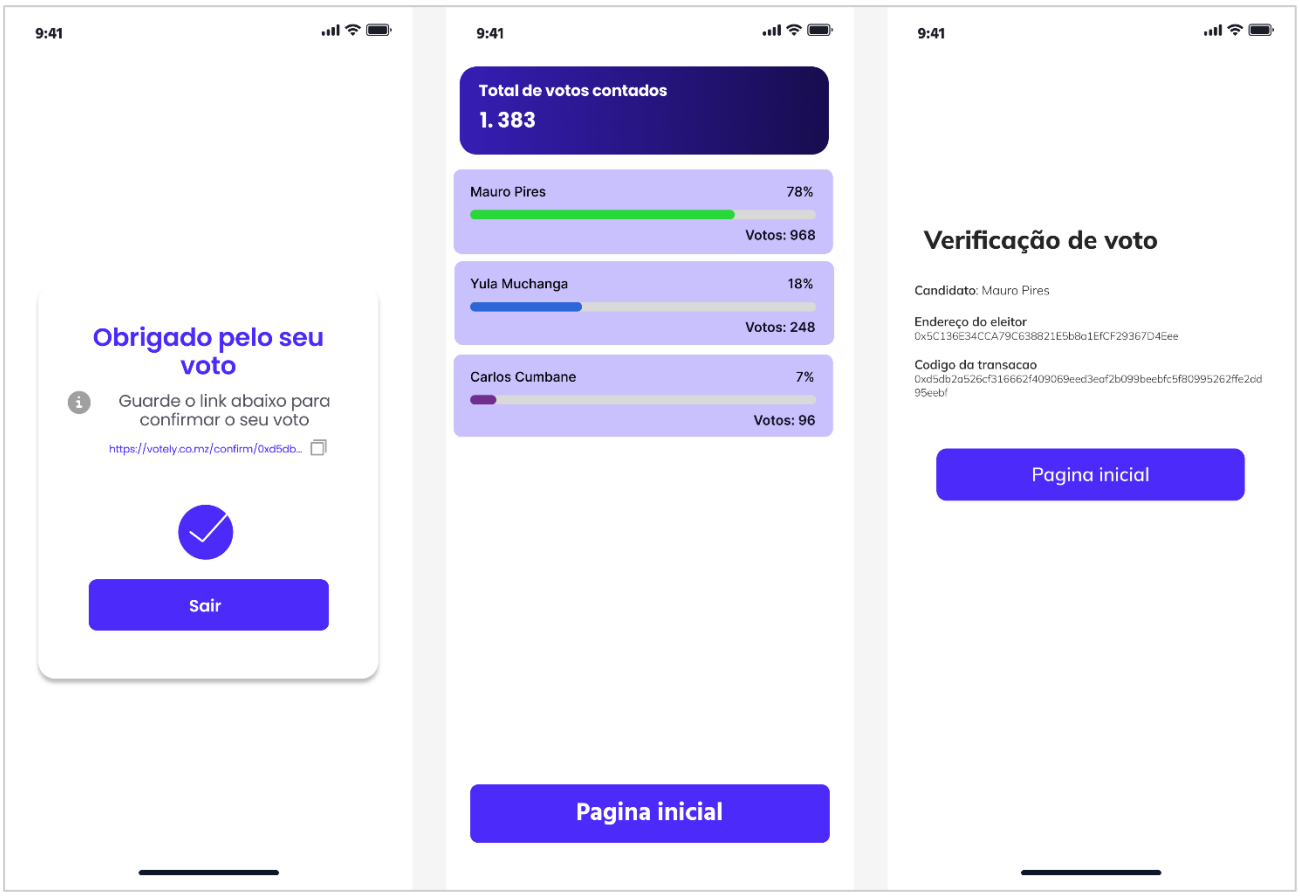


Figura 17: Telas para verificação de resultados

4.3. Implementação e teste unitário

Segundo Sommerville (2011), o estágio de implementação do desenvolvimento de software é o processo de conversão de uma especificação do sistema em um sistema executável. Neste estágio estão envolvidos processos de projecto e programação de software.

4.3.1. Tecnologias Utilizadas

Para a implementação da solução proposta, recorreu-se a um conjunto de tecnologias modernas que, em conjunto, permitem garantir a construção de um sistema de votação electrónica descentralizado, seguro e funcional.

- **Blockchain**: Ethereum é a plataforma blockchain escolhida para o desenvolvimento e execução dos contractos inteligentes. Suporta um ambiente descentralizado, imutável e programável através da Ethereum Virtual Machine (EVM).
- **Contractos inteligentes**: Solidity é a linguagem nativa da plataforma Ethereum, que permite o desenvolvimento de lógica de negócios diretamente na blockchain. Esta

será a linguagem de programação utilizada para a criação dos contractos inteligentes.

- **Frontend**: Para o desenvolvimento da interface do utilizador será utilizada a biblioteca JavaScript ReactJS.
- **Servidor**: Para o desenvolvimento do servidor off-chain sera usada a plataforma Node.js.
- **Autenticação**: Para a logica da autenticação sera usada a biblioteca Web3Auth
- **Ethers.js**: Biblioteca JavaScript utilizada para interacção entre o frontend da aplicação e os contratos inteligentes na blockchain. Permite enviar transacções, ler dados e escutar eventos.
- **Ganache**: Será utilizada como rede de teste (testnet) para simular a execução do sistema em ambiente blockchain sem custos financeiros reais. Isso irá facilitar a validação do comportamento dos contratos inteligentes antes da publicação em rede principal.

Este conjunto de ferramentas permitiu o desenvolvimento eficiente de uma solução que alia os princípios da descentralização com a praticidade de uma aplicação web moderna.

4.3.2. Configuração da Rede Blockchain

Para efeitos de desenvolvimento e testes da solução proposta, optou-se por utilizar uma rede blockchain local. Esta abordagem permite maior controlo sobre os dados, facilita a realização de testes repetitivos, reduz o tempo de desenvolvimento e elimina custos associados a transacções reais.

Ambiente de desenvolvimento

Os testes do protótipo desenvolvido na presente pesquisa foram feitos computador portátil da marca Acer, modelo TravelMate P214, com processador Intel Core i5-1135G7 @2.40GHz, 24GB de memoria e sistema operativo Windows 11.

Rede Ethereum

A rede blockchain local foi configurada com o Ganache, uma ferramenta amplamente utilizada no ecossistema Ethereum para criar blockchains locais. O Ganache simula uma rede Ethereum, disponibilizando contas com saldo fictício e permitindo a visualização e o controlo completo sobre os blocos e transacções.

Após a instalação do Ganache, foi iniciada uma nova instância da rede, que forneceu:

- Um conjunto de contas Ethereum com chaves privadas e saldo pré-definido em ETH fictício.
- Um RPC Server local (http://127.0.0.1:7545) para interacção com a rede.

Esta configuração permitiu o deploy local dos contratos inteligentes, bem como a interacção com a aplicação frontend de forma rápida e sem necessidade de depender de uma testnet pública.

4.3.3. Implementação dos Contratos Inteligentes

Os contratos inteligentes representam o núcleo lógico do sistema de votação proposto, sendo responsáveis pela execução automática e transparente das regras do processo eleitoral. Foram desenvolvidos em Solidity e implementados na plataforma Ethereum, utilizando o ambiente de desenvolvimento Hardhat para compilar, testar e fazer o deploy dos contractos na rede. Para começar são escritas as funções e todo o código que contem as configurações do contracto inteligente e faz-se o deploy, após o deploy é retornado o endereço do contracto na rede e é gerado um JSON denominado ABI (Application Binary Interface), que contem a descrição das funções e objectos presentes no contracto inteligente, essas informações são necessárias para a conexão com o frontend.

4.3.4. Autenticação

A implementação da autenticação será realizada através da integração com o Web3Auth, uma solução que simplifica o acesso a aplicações descentralizadas ao permitir a autenticação com credenciais familiares ao utilizador, nesse caso sera usado o email institucional. Ao invés de exigir que o eleitor interaja diretamente com carteiras digitais tradicionais, o Web3Auth permite que uma carteira blockchain seja criada e gerida de forma segura a partir dessas credenciais. A integração será feita no frontend, utilizando o Web3Auth SDK para inicializar o fluxo de login, gerar e recuperar a chave privada do utilizador, e estabelecer a conexão com a carteira associada.

4.3.5. Integração da Interface do Utilizador com a Plataforma de Blockchain

A integração entre os contratos inteligentes e a interface do utilizador permite que os utilizadores interajam com a blockchain de forma amigável, sem necessidade de compreender os detalhes técnicos subjacentes.

Através do Ethers.js, foi possível estabelecer a ligação entre a aplicação frontend e os contratos inteligentes previamente desenvolvidos e implantados na blockchain.

O processo inicia-se com a conexão ao provedor Ethereum.

Em seguida, a aplicação instancia o contracto inteligente através do seu endereço de implantação e do ABI, o qual define as funções públicas acessíveis do contracto.

Uma vez estabelecida essa instância, a interface gráfica permite executar, de forma transparente ao utilizador, várias ações definidas nos contratos inteligentes, como o registo de eleitores, a submissão de votos e a visualização dos resultados da eleição.

5. Capítulo VI – Considerações finais

Este Capítulo aborda as conclusões sobre o alcance dos objectivos do trabalho, os principais desafios enfrentados durante a pesquisa e recomendações para futuras melhorias e expansões do sistema de votação electrónica desenvolvido com base na tecnologia blockchain.

5.1. Conclusões

O presente trabalho teve como objectivo propor e desenvolver um sistema de votação eletrônica baseado na tecnologia blockchain, com foco na transparência, segurança e verificabilidade do processo eleitoral. A motivação partiu da constatação de fragilidades nos modelos tradicionais de votação, tanto em contextos nacionais quanto em contextos mais específicos, como o das eleições estudantis, onde ainda predominam métodos manuais, suscetíveis a erros e desconfiança.

Ao longo do estudo, foi possível perceber o potencial transformador da blockchain na modernização de processos eleitorais. Sua natureza descentralizada, aliada à imutabilidade dos registos e à capacidade de auditabilidade pública e individual, oferece um cenário promissor para a construção de sistemas mais confiáveis e transparentes. Neste sentido, a aplicação prática da tecnologia no contexto do Núcleo de Estudantes de Direito da UEM não apenas permite melhorias significativas na gestão das eleições estudantis, como também serve como base experimental para eventuais aplicações em cenários mais amplos.

Entre os principais resultados alcançados, destacam-se a análise detalhada das técnicas de blockchain aplicáveis a sistemas de votação, a seleção e justificação do uso da plataforma Ethereum, o desenvolvimento de uma arquitetura de sistema em camadas, e a implementação de um protótipo funcional com contratos inteligentes integrados à uma interface web. O sistema proposto atende aos requisitos essenciais levantados, permitindo o cadastro de eleições, eleitores e candidatos, o lançamento e verificação de votos, bem como a visualização segura dos resultados.

Este trabalho demonstrou que a utilização de tecnologias emergentes como a blockchain pode contribuir de forma relevante para a integridade e modernização de processos democráticos, mesmo em contextos com limitações de infraestrutura ou baixa confiança nas

instituições. Ao mesmo tempo, abre espaço para futuras investigações e melhorias, tanto no campo técnico quanto na adaptação institucional de soluções digitais para votação.

5.2. Constrangimentos

Durante a realização deste trabalho, foram identificados os seguintes constrangimentos e limitações:

- Conhecimento técnico inicial: A necessidade de adquirir conhecimentos técnicos sobre blockchain, Solidity e ferramentas do ecossistema durante a própria execução do trabalho representou um desafio adicional, que exigiu um processo intensivo de autoaprendizagem.
- Acesso limitado a dados reais: Não foi possível obter actas, relatórios ou documentos oficiais sobre eleições passadas no Núcleo de Estudantes de Direito, o que dificultou uma análise mais detalhada e baseada em evidências históricas. Além disso, o núcleo nunca realizou inquéritos para aferir o nível de confiança dos estudantes nos processos eleitorais, limitando a compreensão do grau de aceitação ou rejeição da comunidade estudantil em relação ao sistema tradicional.

5.3. Recomendações

Com base nos resultados obtidos e nas observações feitas durante o desenvolvimento deste trabalho, apresentam-se as seguintes recomendações:

- Sugere-se que o protótipo desenvolvido seja testado em uma eleição real do Núcleo de Estudantes de Direito da UEM, a fim de avaliar seu desempenho com utilizadores reais, em ambiente controlado e com acompanhamento técnico.
- Para garantir uma transição segura e gradual, recomenda-se que o sistema de votação eletrônica baseado em blockchain seja inicialmente implementado em paralelo com o método tradicional de votação. Essa abordagem permitirá comparações diretas entre os dois métodos, identificação de melhorias e aumento da confiança dos participantes.
- Caso o sistema venha a ser considerado para contextos maiores, recomenda-se a realização de testes de carga e simulações para avaliar sua escalabilidade e estabilidade em ambientes com elevado número de utilizadores.

Referências Bibliográficas

Adeshina, S. A., & Ojo, A. (2014). Design Imperatives for E-Voting as a Sociotechnical System. *2014 11th International Conference on Electronics, Computer and Computation (ICECCO)*, 1–4. https://ieeexplore.ieee.org/abstract/document/6997569/

Agnese Arnaldo. (2025, junho 5). *Entrevista aberta ao presidente do NED* [In-person].

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., & others. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. *Proceedings of the thirteenth EuroSys conference*, 1–15.

Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, *9*(3), 01–09.

Bellis, M. (2006). *The History of Voting Machines—History of the Voting System Standards Program*. https://theinventors.org/library/weekly/aa111300b.htm

Birch, J. (2018, junho 9). *Blockchain e eleições: A experiência japonesa, suíça e norte-americana*. https://br.cointelegraph.com/news/blockchain-and-elections-the-japanese-swiss-and-american-experience

Borrego, T. A. (2019). *Tecnologia Blockchain-Potencial de Aplicação no Âmbito dos Processos de Negócio das Cadeias de Abastecimento* [Master's Thesis]. Universidade do Porto (Portugal).

Brito, L. de. (2009). Sobre a Transparência Eleitoral. *IESE - Instituto de Estudos Sociais e Económicos*, *20*, 2.

Cetinkaya, O. (2008). Analysis of security requirements for cryptographic voting protocols. *2008 Third International Conference on Availability, Reliability and Security*, 1451–1456. https://ieeexplore.ieee.org/abstract/document/4529515/

Chafiq, T., Azmi, R., & Mohammed, O. (2024). Blockchain-based electronic voting systems: A case study in Morocco. *International Journal of Intelligent Networks*, *5*.

De Filippi, P., Wray, C., & Sileno, G. (2021). Smart contracts. *Internet Policy Review*, *10*(2), 1–9.

Dong, S., Abbas, K., Li, M., & Kamruzzaman, J. (2023). Blockchain technology and application: An overview. *PeerJ Computer Science*, *9*, e1705.

Follow My Vote. (2024). Blockchain Voting: The End To End Process. *Follow My Vote*. https://followmyvote.com/blockchain-voting-the-end-to-end-process/

Fonseca, J. J. S. (2002). *Metodologia Da Pesquisa Científica*. João José Saraiva da Fonseca. https://books.google.co.mz/books?hl=en&lr=&id=oB5x2SChpSEC&oi=fnd&pg=PA4&dq=Fonseca+-+Metodologia+da+pesquisa+cient%C3%ADfica+pdf+&ots=OSSV-xejn-&sig=uEHjBeVnvkOh0Dn5SxMCykyt4M4&redir_esc=y#v=onepage&q&f=false

Gailly, N., Jovanovic, P., Ford, B., Lukasiewicz, J., & Gammar, L. (2018). Agora: Bringing our voting systems into the 21st century. *Agora Voting, White Paper*, 41.

Gerhardt, T. E., & Silveira, D. T. (2009). *Métodos de pesquisa*. Editora da UFRGS.

Gil, A. C. (2002). *Como Elaborar Projetos De Pesquisa* (4.ª ed.). Atlas.

Gupta, S., & Madhur, M. (2018). HFS top 10 enterprise blockchain services 2018. *Cambridge, MA (available at https://us. nttdata. com/en/-/media/assets/reports/digital-blockchain-hfs-top-10-enterprise-blockchain-services-report. pdf)*.

Hardwick, F. S., Gioulis, A., Akram, R. N., & Markantonakis, K. (2018). E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1561–1567.

Heiberg, S., Laud, P., & Willemson, J. (2011). The application of i-voting for Estonian parliamentary elections of 2011. *International Conference on E-Voting and Identity*, 208–223. https://link.springer.com/chapter/10.1007/978-3-642-32747-6_13

International IDEA. (2023, junho 2). *Use of E-Voting Around the World*. International IDEA. https://www.idea.int/news-media/multimedia-reports/use-e-voting-around-world

Jones, D. W. (2003). *Illustrated Voting Machine History*. A Brief Illustrated History of Voting. https://homepage.cs.uiowa.edu/~jones/voting/pictures/#ballota

Kamau, R. (2022, agosto 11). *Kenyan Electoral Board Designs A Transparent Voting System That Mirrors The Bitcoin Blockchain*. https://www.forbes.com/sites/rufaskamau/2022/08/11/bitcoin-blockchain-inspires-kenyan-electoral-board-to-implement-a-transparent-voting-system/

Kaur, A., Nayyar, A., & Singh, P. (2020). Blockchain: A path to the future. *Cryptocurrencies and Blockchain technology applications*, 25–42.

Kawamara, E., & Mutawe, P. (2022). *Blockchain as a Tool for Election Validity*. JEPA. https://www.jepaafrica.com/insights/blockchain-as-a-tool-for-election-validity

Lewis, A. (2018). *The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology That Powers Them* (1st ed). Mango Media.

Li, X., Wang, X., Kong, T., Zheng, J., & Luo, M. (2021). From bitcoin to solana–innovating blockchain towards enterprise applications. *International Conference on Blockchain*, 74–100.

Malik, L., Arora, S., Shrawankar, U., & Deshpande, V. (Eds.). (2022). *Blockchain for smart systems: Computing technologies and applications* (First edition). Chapman & Hall\CRC Press.

Mall, R. (2019). *Fundamentals of software engineering* (Fifth edition). PHI Learning Private Limited.

Marconi, M. de A., & Lakatos, E. M. (2003). *Fundamentos de metodologia científica* (5.ª ed.). EDITORA ATLAS.

Moghaddam, F. M. (Ed.). (2017). Voting, History of. Em *The SAGE Encyclopedia of Political Behavior* (1.ª ed., p. 898). SAGE Publications, Inc. https://sk.sagepub.com/reference/the-sage-encyclopedia-of-political-behavior/i11859.xml

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, *4*(2), 15.

Narayanan, A., & Clark, J. (2017). Bitcoin's Academic Pedigree: The concept of cryptocurrencies is built from forgotten ideas in research literature. *Queue*, *15*(4), 20–49.

Nurmi, H. (2010). Voting systems for social choice. Em *Handbook of Group Decision and Negotiation* (pp. 167–182). Springer.

ODIHR (Ed.). (2024). *Handbook for the observation of information and communication technologies (ICT) in elections*. OSCE ODIHR.

Osula, A.-M. (2019). *Blockchain in Estonia & Project Priviledge H2020*. https://northsearegion.eu/media/11757/20191217-guardtime.pdf

Perwej, Y. (2018). A pervasive review of Blockchain technology and its potential applications. *Open Science Journal of Electrical and Electronic Engineering (OSJEEE), New York, USA*, *5*(4), 30–43.

Quasim, M. T., Khan, M. A., Algarni, F., Alharthy, A., & Alshmrani, G. M. M. (2020). Blockchain frameworks. *Decentralised Internet of Things: A Blockchain Perspective*, 75–89.

Regulamento Eleitoral, Pub. L. No. 001/CE/2012, 001 001/CE/2012 (2012).

Rodrigues, D. F. (2008). *Sistemas De Votação: Análise, Opções E Possibilidades* [Universidade do Legislativo Brasileiro]. http://www2.senado.leg.br/bdsf/handle/id/161569

Sandford, L. (2024, novembro 8). *What is digital signature? Your guide in 2025*. Oneflow. https://oneflow.com/digital-signatures/

Sepúlvida, F. R., & Paiva, C. E. (2019). *Um estudo sobre o uso da tecnologia Blockchain para votação eletrônica*. http://ric-cps.eastus2.cloudapp.azure.com/handle/123456789/5066

Silva, C. R. da. (2016). As eleições e a democracia moçambicana. *OBSERVARE. Universidade Autónoma de Lisboa*. https://repositorio.grupoautonoma.pt/server/api/core/bitstreams/3e8c5af7-f10f-49f0-a885-2320808e9695/content

Singhal, B. (com Dhameja, G., & Panda, P. S.). (2018). *Beginning Blockchain: A beginner's guide to building Blockchain solutions*. Apress.

Sommerville, I. (2011). *Engenharia de software* (9.ª ed.). Pearson Education.

Stadzisz, P. C. (2002). Projeto de Software usando a UML. *Curitiba: CEFET*.

Statista. (2022). *Africa: Internet penetration 2022*. Statista. https://www.statista.com/statistics/1176654/internet-penetration-rate-africa-compared-to-global-average/

Szabo, N. (1996). Smart contracts: Building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought,(16)*, *18*(2), 28.

Tanenbaum, A. S., & Van Steen, M. (2017). *Distributed systems*. CreateSpace Independent Publishing Platform.

Tanwar, S. (2022). *Blockchain Technology: From Theory to Practice* (1st ed. 2022). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-1488-1

Tikhomirov, S. (2017). Ethereum: State of knowledge and research perspectives. *International symposium on foundations and practice of security*, 206–221.

Tremblay, G. (2001). Software Design. *SWEBOK*, 35.

Tyagi, S. S., & Bhatia, S. (Eds.). (2021). *Blockchain for business: How it works and creates value*. Wiley-Scrivener.

Vakarjuk, J., Snetkov, N., & Willemson, J. (2022). Russian federal remote E-voting scheme of 2021–protocol description and analysis. *Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference*, 29–35.

Valenta, M., & Sandner, P. (2017). Comparison of ethereum, hyperledger fabric and corda. *Frankfurt School Blockchain Center*, *8*, 1–8.

Vedel, T. (2006). The idea of electronic democracy: Origins, visions and questions. *Parliamentary Affairs*, *59*(2), 226–235.

Vladucu, M.-V., Dong, Z., Medina, J., & Rojas-Cessa, R. (2023). E-Voting Meets Blockchain: A Survey. *IEEE Access*, *11*, 23293–23308. https://doi.org/10.1109/ACCESS.2023.3253682

Vote Australia. (2019). *Blockchain Voting*. Vote Australia. https://www.voteaustralia.org.au/blockchain_voting

Vujičić, D., Jagodić, D., & Ran\djić, S. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. *2018 17th international symposium infoteh-jahorina (infoteh)*, 1–6.

Wolf, P., Nackerdien, R., & Tuccinardi, D. (com International Institute for Democracy and Electoral Assistance). (2011). *Introducing electronic voting: Essential considerations*. International Institute for Democracy and Electoral Assistance.

World Bank Group. (2017). *Distributed ledger technology (DLT) and blockchain*. World Bank Group Washington, DC.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

Zhang, J., Young, A., & Verhulst, S. (2018). *Addressing Voting Inefficiencies Resulting from Identity Challenges with Blockchain*. GovLab.

Anexos

Anexo 1: Regulamento Eleitoral do NED

O presente anexo contém uma seleção dos artigos mais relevantes do Regulamento Eleitoral do Núcleo dos Estudantes de Direito da Universidade Eduardo Mondlane (NED). Este extrato foi elaborado com o objectivo de apoiar a análise apresentada no Capítulo III deste trabalho, centrada na estrutura, funcionamento e desafios do processo eleitoral do NED. O regulamento completo encontra-se disponível junto à Comissão Eleitoral do NED e poderá ser consultado para fins complementares, caso necessário.

Deliberação nº 001/CE/2012

Os Estatutos da Associação Núcleo dos Estudantes de Direito-NED conferem a cada um dos seus membros o direito de eleger e ser eleito aos diversos órgãos existentes.

Tendo em atenção que os estatutos sofreram uma profunda revisão que passou a incluir a Comissão Eleitoral na lista dos órgãos do NED, mostra-se pertinente a necessidade de adequar os procedimentos eleitorais aos novos Estatutos.

É aprovado o Regulamento Eleitoral do NED, anexo à presente Deliberação e que dele faz parte integrante.

Aprovado pela Comissão Eleitoral, aos 18 de Junho de 2012. Promulgado em 26 de Junho de 2012.

CAPÍTULO I - Princípios Fundamentais

Artigo 1 - Âmbito

1. O presente regulamento contém as normas a que devem obedecer o processo eleitoral e as eleições para o corpo directivo da Associação Núcleo dos Estudantes de Direito-NED, doravante designado NED.

2. Vincula todos os estudantes da Faculdade de Direito da UEM e aplica-se, com as devidas adaptações, a todos os órgãos do NED.

Artigo 2 - Princípio electivo

1. O corpo directivo do NED é eleito com base em sufrágio universal, igual e directo.

2. Os órgãos do NED são eleitos em escrutínio secreto e por um período de dois anos.

3. Nenhum associado pode estar representado em mais de um órgão electivo.

4. O voto pode ser exercido presencialmente ou por procuração legal válida.

Artigo 3 - Capacidade eleitoral activa

Cada membro do NED no pleno gozo dos seus direitos tem direito a um voto.

Artigo 4 - Capacidade eleitoral passiva

1. Pode ser eleito qualquer associado sem dívidas e em pleno gozo dos direitos associativos.

2. Não podem candidatar-se à presidência os estudantes do último ano.

3. Estudantes com infrações disciplinares ativas não podem candidatar-se.

CAPÍTULO II - Organização do Processo Eleitoral

Artigo 5 - Tutela jurisdicional e administração

Compete à Comissão Eleitoral (CE) a verificação da validade dos atos do processo eleitoral e sua administração.

Artigo 6 - Calendário Eleitoral

1. A CE elabora o calendário eleitoral e submete à Direcção Geral do NED para aprovação.

2. O silêncio da Direcção por 48h equivale à aprovação tácita.

Artigo 7 - Noção da Comissão Eleitoral

A CE é responsável por toda a organização e fiscalização do processo eleitoral.

Artigo 8 - Natureza

A CE é independente da Direcção Geral do NED e da Faculdade. Nenhum membro pode ser candidato ou apoiante de lista.

Artigo 9 - Competências da CE

Incluem: elaborar o calendário, gerir candidaturas, fiscalizar campanhas, controlar votação e contagem de votos, publicar resultados, etc.

Artigo 10 - Mandato

O mandato dos membros da CE termina com a composição da nova comissão, salvo impedimentos legais ou disciplinares.

CAPÍTULO III - Processo Eleitoral

Artigo 12 - Fases do Processo Eleitoral

a. Composição da CE; b. Abertura de candidaturas; c. Verificação e publicação das listas; d. Campanha eleitoral; e. Votação; f. Apuramento e publicação; g. Tomada de posse.

Artigo 13 - Composição da Comissão Eleitoral

Composta por até 13 membros, com representação de cada turma, secretários e representantes do conselho de chefes de turma.

Artigos 17 a 19 - Candidaturas

Definem o processo de submissão, subscritores exigidos, composição mínima das listas e critérios de aceitação.

Artigos 23 a 29 - Campanha e Propaganda

Definem o tempo, os meios, os limites e as proibições quanto à campanha e propaganda.

Artigos 30 a 39 - Votação

Regulam local, horário, credenciais, autenticação de eleitores, fluxo de votação e sigilo do voto.

CAPÍTULO VI - Apuramento e Resultados

Artigos 41 a 49

Definem quem pode presenciar a contagem, como ocorre a apuração, recontagem, publicação e critérios de vitória.

CAPÍTULO IV - Infrações e Sanções

Artigo 51 - Infrações eleitorais

Proíbem condutas como voto duplo, coerção, propaganda irregular e quebra do sigilo.

Artigo 52 - Sanções

Prevêem desde advertência verbal até desqualificação da lista e perda do direito de voto.

Anexo 2: Guião de entrevista

Entrevista aberta ao presidente do NED.

1. Como está estruturado o Núcleo dos Estudantes de Direito?

R: O núcleo possui uma estrutura bem definida, composta por um Presidente, Vice-Presidente, Secretário, Chefes de Departamentos e representantes distribuídos por diversas áreas.

2. Como é organizado o processo eleitoral no NED?

R: As eleições ocorrem a cada dois anos, seguindo um regulamento próprio. O processo envolve a criação de um calendário eleitoral, a formação da Comissão Eleitoral, a abertura e validação de candidaturas, o período de campanha (máximo de 20 dias), o dia da votação e a publicação dos resultados no mesmo dia.

3. Quem compõe a Comissão Eleitoral e como é formada?

R: A Comissão Eleitoral pode ter até 13 membros, incluindo representantes de todas as turmas e turnos. É obrigatória a presença de pelo menos um membro com experiência em eleições anteriores. Nenhum membro pode ter ligação com as listas candidatas.

4. Quais são os critérios para apresentação de candidaturas?

R: Podem integrar uma lista estudantes de qualquer ano, mas só estudantes do 2º e 3º anos podem candidatar-se à presidência. Os candidatos devem apresentar documentação como cartão de estudante, comprovativo de inscrição e não ter histórico de fraudes na instituição.

5. Quem tem direito a votar?

R: Todos os estudantes da Faculdade de Direito da UEM. No momento da votação, devem apresentar o cartão de estudante ou comprovativo de inscrição.

6. Como é controlado o processo de votação para evitar votos duplicados?

R: Cada votante assina uma lista de presença e pinta o dedo após votar. Isso permite evitar que alguém vote mais de uma vez.

7. Que desafios são enfrentados durante o processo eleitoral?

R: Um dos principais desafios é a pré-campanha feita por candidatos antes da abertura oficial do período de campanha, o que pode levar à desqualificação. Além disso, há dificuldades logísticas devido à realização da votação em dias letivos e à dispersão das turmas, incluindo estudantes que assistem aulas no campus central e na Faculdade de Medicina. Isso gera longas filas e impede que muitos estudantes participem.

8. Houve casos de fraude nas eleições anteriores?

R: Não houve registos de fraudes diretas, mas já ocorreram tentativas de sabotagem entre listas. A proximidade entre os estudantes pode levantar suspeitas de parcialidade.

9. Considera que a tecnologia pode melhorar o processo eleitoral no NED?

R: Sim. Um sistema de votação electrónica poderia reduzir filas e aumentar a participação, especialmente se permitir voto remoto. No entanto, é essencial que o sistema seja gerido por uma entidade neutra, externa ao núcleo, garantindo imparcialidade.

10. Que funcionalidades considera essenciais num sistema de votação electrónica?

R: Autenticação segura do eleitor, controle contra votos duplicados, acessibilidade por telemóvel e funcionamento limitado ao horário oficial de votação. O sistema também deve ser auditável e supervisionado pela Comissão Eleitoral.

Anexo 3: Descrição dos casos de uso

O sistema é composto por sete (7) casos de uso, sendo apresentadas as suas especificações a seguir.

CU01. Cadastrar Eleições

Tabela A3 – 1: CU01. Cadastrar Eleições

Nome	Cadastrar Eleições
Descrição	Permite ao membro da comissão eleitoral criar uma nova eleição, definindo os seus parâmetros básicos como título, descrição e data da votação.
Actor	Membro da comissão eleitoral
Pré-condições	O membro da comissão eleitoral deve estar autenticado no sistema.
Pós-condições	Uma nova eleição é registada no sistema e armazenada na blockchain, ficando visível para os utilizadores.
Fluxo principal de eventos	
Actor	Actividades
Comissão eleitoral	Aceder à interface de criação de eleições.
Comissão eleitoral	Preencher os dados da eleição (título, descrição, datas).
Comissão eleitoral	Submeter o formulário.
Sistema	Enviar os dados da eleição ao contractos inteligente.
Sistema	Registar a eleição na blockchain.
Sistema	Confirmar o sucesso da operação ao membro da comissão eleitoral.
Excepções	
Caso os campos obrigatórios não sejam preenchidos, o sistema apresenta um alerta e impede o envio.	
Caso haja falha na conexão com a blockchain, a eleição não é registada e uma mensagem de erro é apresentada.	

CU02. Cadastrar Eleitores

Tabela A3 – 2: CU02. Cadastrar Eleitores

Nome	Cadastrar Eleitores
Descrição	Permite ao membro da comissão eleitoral registar os eleitores que estarão habilitados a votar em uma determinada eleição. O registo é feito associando o endereço da carteira digital do eleitor ao sistema.
Actor	Membro da comissão eleitoral, eleitor
Pré-condições	O membro da comissão eleitoral deve estar autenticado no sistema. Deve existir uma eleição previamente criada.
Pós-condições	O endereço do eleitor é adicionado à lista de eleitores habilitados.
Fluxo principal de eventos	
Actor	Actividades
Comissão eleitoral	Aceder à interface de gestão das eleições.
Comissão eleitoral	Selecionar a eleição para a qual deseja registar eleitores.
Comissão eleitoral	Introduz os dados do eleitor (nome, email institucional, número de telefone, número de estudante).
Sistema	Verificar se não existe eleitor com mesmo e-mail ou número de estudante
Sistema	Guardar os dados do eleitor
Sistema	Enviar e-mail com link de conclusão da inscrição para o eleitor.
Eleitor	Aceder ao link enviado por e-mail.
Sistema	Enviar código de confirmação para o e-mail do eleitor
Eleitor	Introduzir código de confirmação
Sistema	Gerar e armazenar o endereço no contracto inteligente como um eleitor válido.
Sistema	Confirmar o sucesso da operação ao eleitor.
Excepções	
Se tiver um eleitor com o mesmo e-mail ou número de estudante já registado, o sistema impede duplicação.	

CU03. Cadastrar Candidatos

Tabela A3 – 3: CU03. Cadastrar Candidatos

Nome	Cadastrar Candidatos
Descrição	Permite ao membro da comissão eleitoral registar os candidatos que irão concorrer nas eleições, vinculando seus dados ao sistema por meio de um identificador, nome e detalhes da lista de candidatura.
Actor	Membro da comissão eleitoral
Pré-condições	O membro da comissão eleitoral deve estar autenticado no sistema. A eleição deve estar no estado de preparação (ainda não iniciada).
Pós-condições	O candidato é adicionado à lista oficial de candidatos da eleição, com seu identificador armazenado no contracto inteligente.
Fluxo principal de eventos	
Actor	Actividades
Comissão eleitoral	Aceder à interface de gestão das eleições.
Comissão eleitoral	Selecionar a eleição para a qual deseja registar o candidato.
Comissão eleitoral	Inserir os dados do candidato (nome e detalhes da lista de candidatura).
Sistema	validar os dados.
Sistema	Armazenar os dados do candidato no contracto inteligente.
Sistema	Confirmar o sucesso da operação ao membro da comissão eleitoral.
Excepções	
Se os dados estiverem incompletos ou inválidos, o sistema rejeita o registo.	

CU04. Registar Voto

Tabela A3 – 4: CU04. Registar Voto

Nome	Registar Voto
Descrição	Permite ao eleitor autenticado submeter o seu voto para um dos candidatos disponíveis na eleição em curso. O voto é registado como uma transacção imutável na blockchain.
Actor	Eleitor
Pré-condições	O eleitor deve estar autenticado no sistema. A eleição deve estar no estado de votação. O eleitor deve estar registado na lista de eleitores elegíveis. O eleitor ainda não deve ter votado.
Pós-condições	O voto do eleitor é registado na blockchain e torna-se parte permanente da eleição.
Fluxo principal de eventos	
Actor	Actividades
Eleitor	Aceder à interface de votação.
Sistema	Verificar a elegibilidade do eleitor e se já existe um voto anterior registado para este eleitor.
Eleitor	Selecionar o candidato pretendido.
Eleitor	Submeter a escolha.
Sistema	Registar o voto na blockchain.
Sistema	Confirmar o sucesso da operação ao eleitor e fornecer o hash da transacção.
Sistema	Terminar a sessão do eleitor no sistema.
Excepções	
Se o eleitor já tiver votado, o sistema impede a nova tentativa e informa que o voto já foi registado.	
Se a eleição estiver encerrada ou ainda não tiver iniciado, o sistema rejeita a tentativa de votação.	
Problemas de conexão com a blockchain podem causar falhas no registo do voto, sendo exibida uma mensagem de erro ao utilizador.	

CU05. Visualizar Resultados

Tabela A3 – 5: CU05. Visualizar Resultados

Nome	Visualizar Resultados
Descrição	Permite aos utilizadores acederem ao resultado da eleição após o encerramento do período de votação. Os resultados são calculados e disponibilizados através do contracto inteligente e armazenados de forma transparente na blockchain.
Actor	Utilizador (Membro da comissão eleitoral ou Eleitor)
Pré-condições	A eleição deve estar encerrada. O contracto inteligente deve ter executado o processo de contagem de votos.
Pós-condições	O utilizador visualiza a lista de candidatos com a respetiva contagem de votos recebidos.
Fluxo principal de eventos	
Actor	Actividades
Utilizador	Aceder à interface de resultados.
Sistema	Consultar o contracto inteligente na blockchain.
Sistema	Buscar e exibir na interface os resultados da eleição.
Excepções	
Se a eleição ainda estiver em andamento, o sistema exibe uma mensagem indicando que os resultados ainda não estão disponíveis.	
Caso haja falha na comunicação com a blockchain, é exibida uma mensagem de erro ao utilizador.	

CU06. Autenticar Utilizador

Tabela A3 – 6: Autenticar utilizador

Nome	Autenticar Utilizador
Descrição	Permite que o utilizador se identifique no sistema para realizar ações protegidas, como votar ou gerir eleições. A autenticação é feita por meio de um código de confirmação enviado para o email do utilizador.
Actor	Utilizador (Membro da comissão eleitoral ou Eleitor)
Pré-condições	

Pós-condições	O utilizador é autenticado e o sistema reconhece seu endereço Ethereum como válido.
Fluxo principal de eventos	
Actor	Actividades
Utilizador	Aceder à aplicação.
Utilizador	Clicar em "Entrar".
Utilizador	Introduzir e-mail institucional no campo “E-mail”
Sistema	Enviar PIN de 6 dígitos de confirmação para o email do utilizador.
Utilizador	Introduzir PIN enviado para o seu e-mail.
Sistema	Realizar conexão com endereço do utilizador e atribuir permissões.
Excepções	
Caso o utilizador falhe o PIN, o acesso é cancelado.	
Se o endereço não estiver registado como eleitor ou membro da comissão eleitoral, o sistema bloqueia o acesso às funcionalidades restritas.	

Anexo 4: Diagramas de Sequência

Diagrama de sequência do caso de uso “Cadastrar eleições”

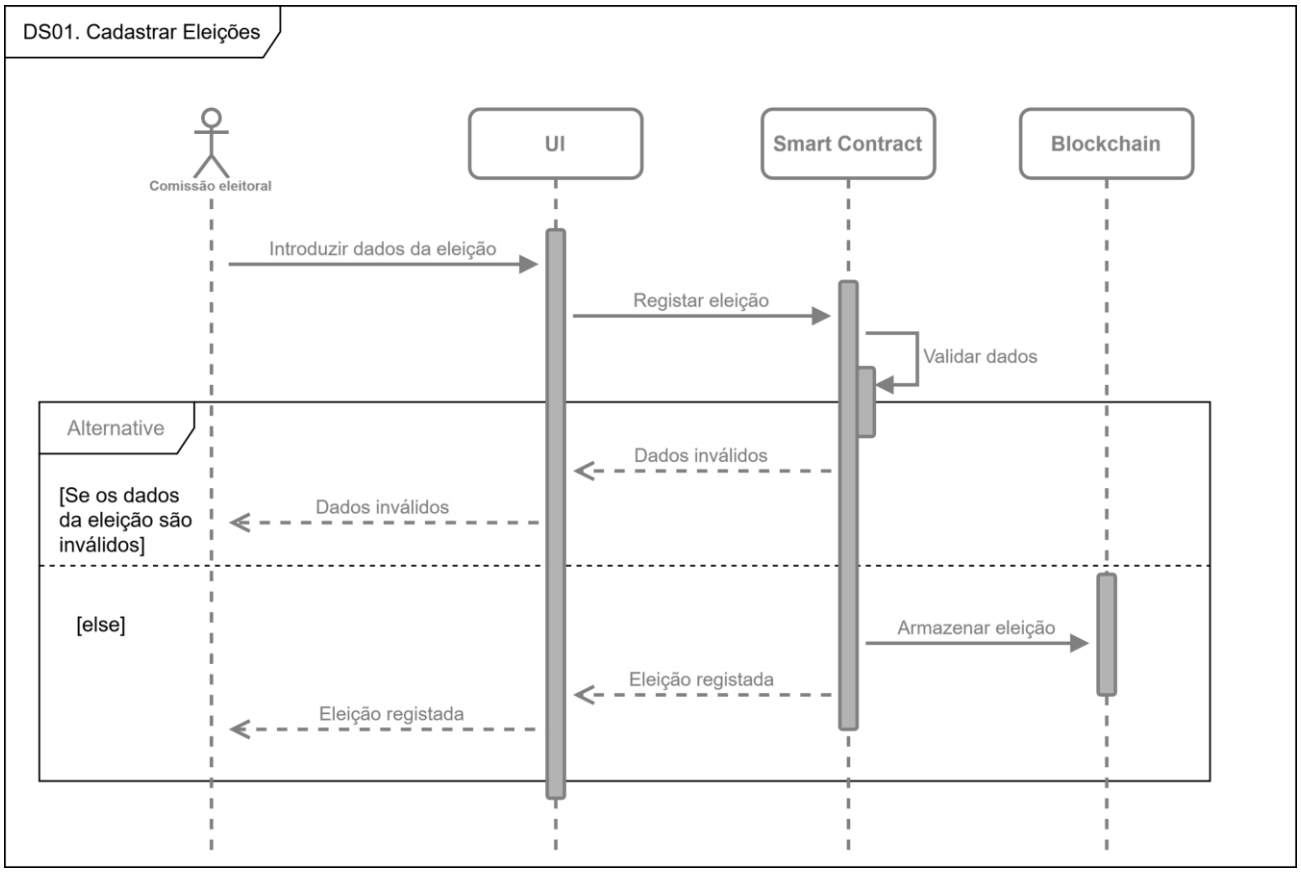


Figura A4 – 1: DS01. Cadastrar eleições

Diagrama de sequência do caso de uso “Cadastrar candidatos”

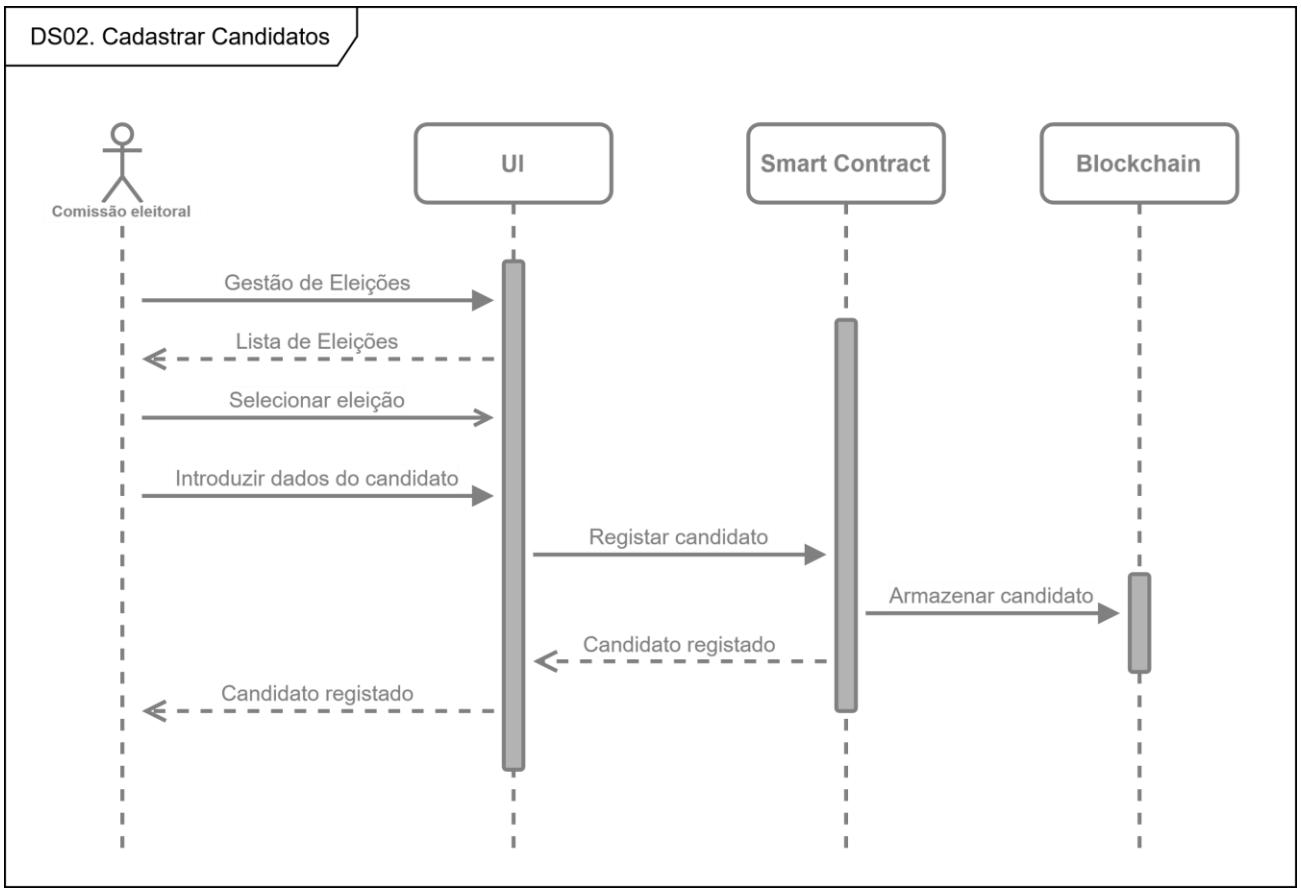


Figura A4 – 2: DS02. Cadastrar candidatos

Diagrama de sequência do caso de uso “Cadastrar eleitor”

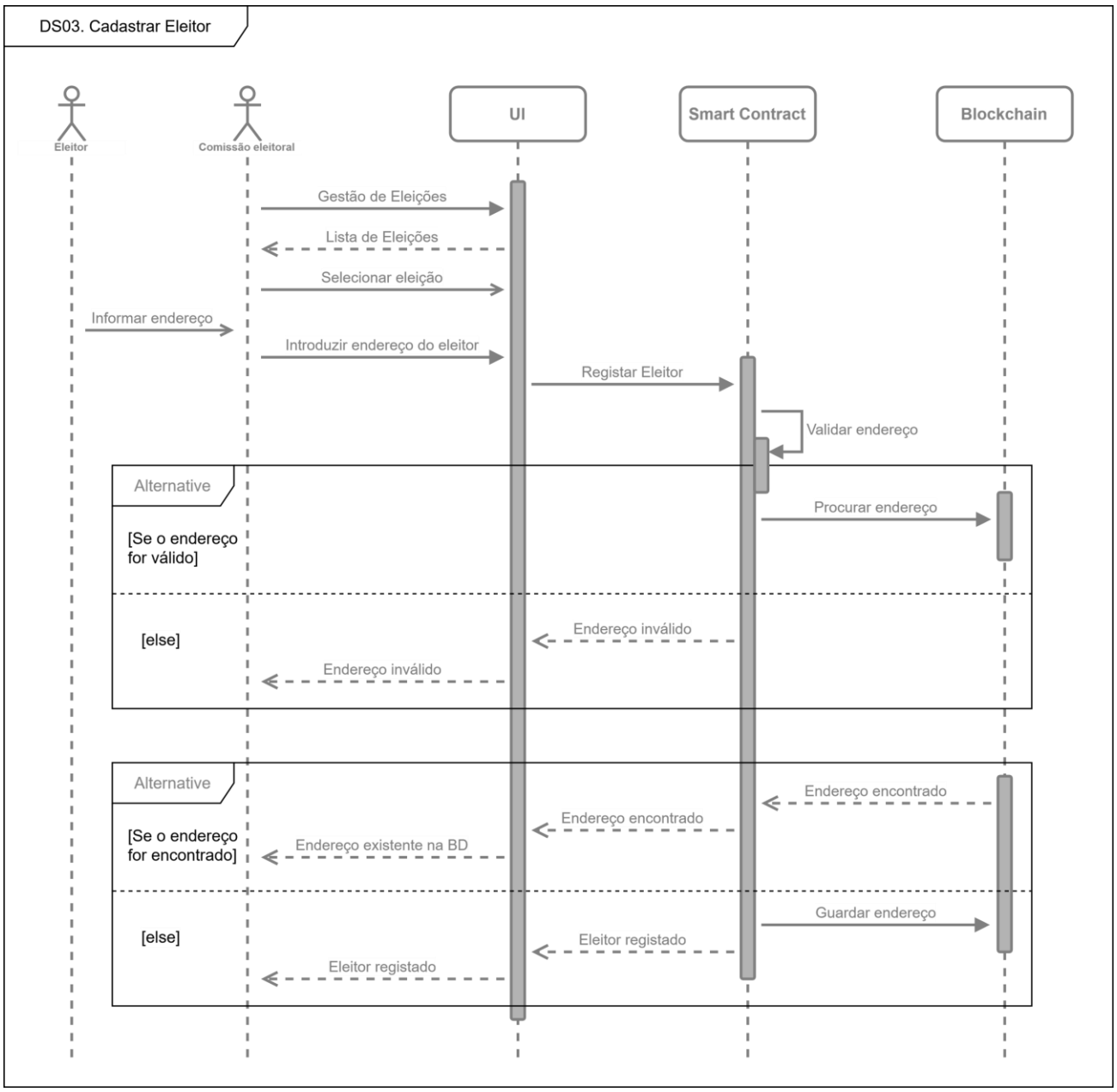


Figura A4 – 3: DS03. Cadastrar eleitor

Diagrama de sequência do caso de uso “Registar voto”

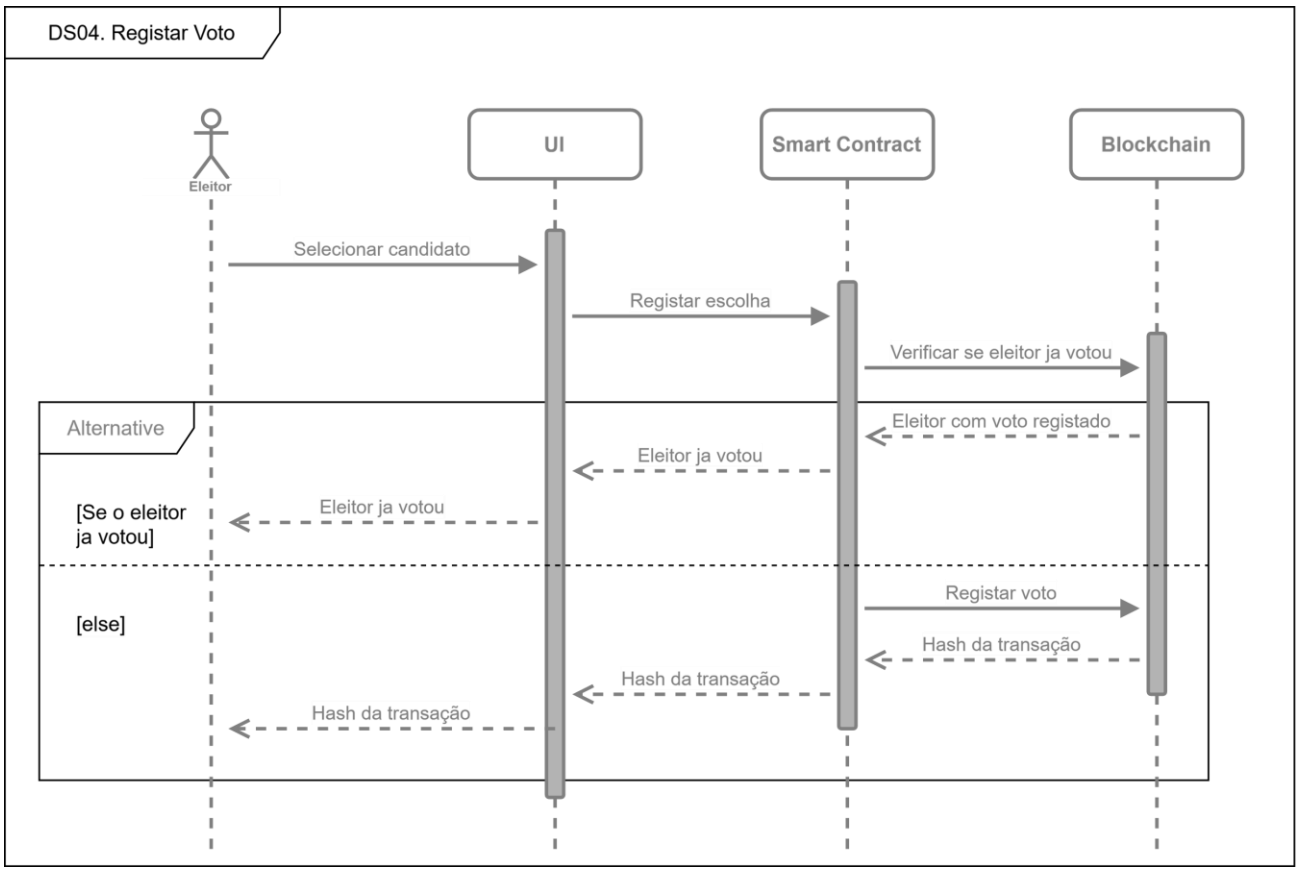


Figura A4 – 4: DS04. Registar voto

Anexo 5: Código do Protótipo e Ambiente de Desenvolvimento

Nesta secção são apresentadas algumas funções que compõem os contractos inteligentes, assim como as configurações para o deploy dos contractos.

```
PS C:\LEWIS\www\projects\blockvoting\blockchain> npx hardhat ignition deploy ./ignition/modules/Election.ts --network ganache --reset
√ Confirm deploy to network ganache (1337)? ... yes
√ Confirm reset of deployment "chain-1337" on chain 1337? ... yes
Hardhat Ignition 🚀

Deploying [ ElectionModule ]

Batch #1
  Executed ElectionModule#Election

[ ElectionModule ] successfully deployed 🚀

Deployed Addresses

ElectionModule#Election - 0x3b01B73e5A98acfD365ffd69A3227AAc7765FDF1
PS C:\LEWIS\www\projects\blockvoting\blockchain>
```

Figura A5 – 1: Deploy do contracto inteligente

A função *registerVoter(address voterAddress, string name)* é utilizada para registar eleitores autorizados.

```
function registerVoter(address voterAddress, string name) public {
        require(CommissionMembers[msg.sender], "Apenas a comissão eleitoral pode registrar eleitores.");
        voters[_voter] = Voter(voterAddress, name);
  }
```

Figura A5 – 2: Registo de eleitores

A função *addCandidate(string name, string listDetails)* regista um novo candidato:

```
function addCandidates(string name, string listDetails) public {
  require(CommissionMembers[msg.sender], "Apenas a comissão eleitoral pode registar candidatos.");
  candidatesCount++;
  candidates[candidatesCount] = Candidate(candidatesCount, name, listDetails);
}
```

Figura A5 – 3: Registo de candidatos

A função *vote(uint candidateId)* permite que um eleitor lance o seu voto, após a verificação de que ainda não votou e que a fase actual permite a votação.

```
function vote(uint _candidateId) public {
    require(isElectionActive(), "A eleicao nao esta ativa.");
    Voter storage sender = voters[msg.sender];
    require(sender.isRegistered, "Eleitor nao registrado.");
    require(!sender.hasVoted, "Eleitor ja votou.");
    sender.hasVoted = true;
    candidates[_candidateId].voteCount++;
}
```

Figura A5 – 4: Registo do voto

A função *getResults()* retorna o número de votos de cada candidato.

```
function getResults(uint _candidateId) public view returns (uint) {
        return candidates[_candidateId].voteCount;
}
```

Figura A5 – 5: Resultados da votação