INSTITUTO DE INFORMÁTICA

SISTEMA DE VOTAÇÃO EM BLOCKCHAIN

DOCUMENTO DE ESPECIFICAÇÃO TÉCNICA

SOFTWARE CONCORRENTE E DISTRIBUÍDO

2024.01

LEONARDO RIBEIRO PALMEIRA
GABRIEL CARDOSO DE CASTRO
GABRIEL MESQUITA
MURILO HENRIQUE FREUA
VITOR LIMA RIBEIRO

SUMÁRIO

1. Introdução

1.1. Visão Geral

O Sistema aqui desenvolvido é fruto do trabalho da equipe Aristóteles, e, nele, propomos a criação de um software de Votação por Blockchain, que consiste numa plataforma descentralizada desenvolvida para gerenciar e facilitar a criação e o gerenciamento de processos de votação e candidatura de pessoas, de forma segura, confiável e transparente, baseada na tecnologia Ethereum. Por meio de contratos inteligentes escritos em Solidity, o sistema visa a garantir a integridade dos votos e proporcionar uma plataforma acessível para os usuários interessados na proposta de utilizar um sistema mais seguro e tolerante a falhas.

A blockchain oferece um registro imutável e criptografado de todas as transações, prevenindo manipulações e permitindo auditorias públicas. A plataforma é projetada para ser escalável tanto técnica quanto governamentalmente, eliminando intermediários e proporcionando uma experiência intuitiva para os usuários.

1.2. Contextualização

A realidade que se impõe pela crescente onda de censuras e restrições às liberdades individuais promovidas por governos ao redor do globo coincide e é respondida, de certa forma, com as novíssimas propostas da Web 3.0 e pela implementação de sistemas distribuídos, de Sistemas de Registro de Títulos de Propriedade até criptomoedas, como o Bitcoin e a Ethereum. Surge então, naturalmente, a necessidade de votações eletrônicas, neste mundo cada vez mais digital e globalizado.

Sistemas tradicionais de votação eletrônica - como nos domínios já citados - frequentemente enfrentam desafios significativos, como a segurança dos dados, a transparência no processo de contagem e a acessibilidade, no entanto. Para isso, essa tecnologia em blockchain pode oferecer uma resposta robusta a essas questões ao fornecer um sistema descentralizado que é resistente a fraudes e manipulações.

A blockchain, por sua natureza, garante que todos os registros sejam imutáveis e seguros, utilizando criptografia para proteger os dados e distribuir a carga de validação entre múltiplos nós. Isso cria um ambiente em que cada voto é registrado de maneira permanente e verificável, permitindo a qualquer pessoa a auditoria e a validação do processo eleitoral.

Além disso, a escalabilidade da plataforma é um aspecto crucial. Sistemas tradicionais podem enfrentar limitações quando se trata de lidar com grandes volumes de votos e demandas crescentes por transparência. O uso de contratos inteligentes em Ethereum possibilita a automação de processos e a gestão eficiente de grandes quantidades de dados, sem a necessidade de intermediários, além de

eliminar o problema da centralização de dados, que são fortemente sujeitos a um controle central.

Nesse contexto, portanto, este sistema se destaca como uma solução moderna que atende à demanda por segurança, transparência e acessibilidade, enfrentando as limitações dos métodos tradicionais, de modo a proporcionar uma plataforma confiável para suprir a crescente demanda que já se avista no horizonte.

1.3. Objetivos

Na literatura, entende-se que a concepção de um sistema de votação eficiente e seguro é guiada, principalmente, por princípios que visam assegurar a integridade, a transparência e a acessibilidade do processo eleitoral. Esses princípios incluem a proteção contra fraudes, a garantia de uma contagem precisa e transparente dos votos, e a capacidade de oferecer um acesso universal e equitativo ao sistema de votação.

No sistema proposto, esses princípios são ampliados, já que a blockchain oferece uma infraestrutura que melhora a segurança e a transparência, enquanto a natureza distribuída e concorrente da tecnologia assegura a integridade e a escalabilidade do sistema. Os principais objetivos desse Sistema incluem:

- **Segurança**: A proteção do sistema contra fraudes e manipulações é essencial para a confiança dos eleitores. A utilização de criptografia e anonimização, bem como a descentralização da blockchain asseguram que todos os votos sejam registrados de forma segura e imutável. Esses mecanismos são projetados para prevenir qualquer tentativa de alteração não autorizada dos dados, garantindo a integridade do processo eleitoral.
- **Transparência**: A capacidade de auditar publicamente todas as transações e votos é crucial para a confiança e legitimidade do sistema. A blockchain oferece um registro imutável e acessível de todas as transações, permitindo que qualquer pessoa possa verificar e confirmar a integridade dos resultados. A arquitetura distribuída assegura que a transparência seja mantida, com dados acessíveis e verificáveis em múltiplos pontos (nodos) da rede.
- **Escalabilidade Técnica**: À medida que o número de eleitores e votos cresce, o sistema deve manter sua eficiência e desempenho. A blockchain oferece soluções para a escalabilidade técnica, distribuindo a carga de trabalho entre vários nós e utilizando técnicas de otimização. Isso assegura que o sistema possa expandir sua capacidade sem comprometer a performance.
- **Integridade e Concorrência**: Em um sistema distribuído, é fundamental gerenciar a concorrência e garantir a integridade dos dados. Os contratos inteligentes e o mecanismo de consenso asseguram que todas as transações sejam processadas de forma ordenada e consistente, evitando conflitos e garantindo que nenhum voto seja perdido ou duplicado. A arquitetura

distribuída do sistema assegura que a integridade do processo eleitoral seja mantida, com dados sincronizados corretamente entre todos os nós da rede.

1.4. Trabalhos relacionados

Diversos estudos e propostas têm explorado o mesmo domínio, contribuindo significativamente para a evolução desse conceito. A seguir, apresentamos uma visão geral dos trabalhos relacionados que influenciam e contextualizam nosso projeto:

- No artigo "Blockchain-Based E-Voting System", publicado na 11ª Conferência Internacional sobre Computação em Nuvem (CLOUD) [1], os autores exploram a aplicação da tecnologia blockchain em sistemas de votação eletrônica e avaliam as implementações atuais. O estudo também destaca o uso de contratos inteligentes para garantir a privacidade e a integridade dos votos, além de abordar a descentralização e a privacidade como aspectos cruciais para a segurança do sistema de votação. A pesquisa demonstra a viabilidade de sistemas de votação baseados em blockchain, destacando a possibilidade de enviar centenas de transações por segundo para a blockchain.
- No artigo"Crypto-voting, a Blockchain based e-Voting System", apresentado na 10ª Conferência Internacional Conjunta sobre Descoberta de Conhecimento, Engenharia de Conhecimento e Gestão do Conhecimento (IC3K 2018) [2], os autores propõem um sistema de votação baseado em blockchain que utiliza criptografia para garantir a segurança e a integridade dos votos. O estudo enfatiza a importância dos contratos inteligentes e da tecnologia blockchain para assegurar a transparência e a confiabilidade do processo eleitoral, aspectos que são centrais em nossa proposta.
- Em "A Proposal of Blockchain-Based Electronic Voting System", apresentado na Segunda Conferência Mundial sobre Tendências Inteligentes em Sistemas, Segurança e Sustentabilidade (WorldS4) [3], os autores apresentam uma proposta de sistema de votação eletrônica baseado em blockchain, utilizando proof of stake, com uma transação por bloco e com envio de dados via JSON numa rede P2P.
- O artigo seminal "Bitcoin: A Peer-to-Peer Electronic Cash System" [4] introduz a tecnologia blockchain e o conceito de criptomoeda, que serve como a base para sistemas de votação baseados em blockchain. Nakamoto descreve o funcionamento da blockchain, a prova de trabalho e a descentralização como fundamentais para garantir a segurança e a integridade das transações. Este trabalho é a pedra angular teórica para qualquer implementação de sistemas em blockchain, incluindo sistemas de votação, e oferece uma compreensão fundamental dos princípios tecnológicos que suportam nosso sistema.

- Jafar et al. (2021): No artigo "Blockchain for Electronic Voting System—Review and Open Research Challenges", publicado na revista Sensors [5], os autores revisam os sistemas de votação baseados em blockchain, bem como suas características e os conceitos chave das arquiteturas mais comuns, além de identificar desafios de pesquisa em aberto.

Esses trabalhos oferecem um excelente norte para o desenvolvimento e a implementação do presente Sistema, com evidências e soluções suficientes para os desafios enfrentados em nosso projeto.

2. Requisitos

Foi elaborado um Documento de Requisitos, em forma de Histórias de Usuário, que pode ser encontrado neste link. Para este documento, no entanto, delineamos os principais requisitos do Sistema, de maneira sucinta que se seguem abaixo.

2.1. Funcionais

Administrador

- Criar, iniciar e encerrar eleições
- Adicionar, atualizar e remover candidatos
- Adicionar e atualizar eleitores
- Adicionar distritos
- Estender ou definir o período eleitoral

Candidato

- Retirar-se de uma eleição

Eleitor

- Votar em candidatos

2.2. Não Funcionais

Segurança e Integridade

- Criptografia: Todos os votos e transações devem ser criptografados para garantir a segurança e privacidade dos dados.
- Integridade: Utilização da blockchain para garantir que os votos não sejam alterados após o registro.

- Autenticidade: Verificação da identidade de eleitores e candidatos para evitar fraudes.

Escalabilidade e Desempenho

- Escalabilidade: O sistema deve ser capaz de tolerar perdas de nós na rede com um número crescente de eleitores e candidatos sem degradação significativa de desempenho.

Usabilidade

- Interface Intuitiva: A plataforma deve ser fácil de usar, com uma interface clara e amigável para administradores, candidatos e eleitores, de modo que fique claro ao usuário o impacto de suas ações no Sistema e a irreversibilidade dos votos.
- Acessibilidade: A plataforma deve ser acessível a partir de diferentes dispositivos e navegadores, garantindo que todos os usuários possam participar.

3. Fundamentos

Nesta seção, discutiremos os fundamentos de sistemas distribuídos e concorrentes com aplicações no escopo deste projeto e alguns dos conceitos mais relevantes de Blockchain e suas implementações na rede Ethereum.

3.1. Princípios de Sistemas Distribuídos

Quando se discute a distribuição de um sistema, surge também a ideia de descentralização. Um sistema distribuído é um sistema de computadores em rede no qual processos e recursos estão distribuídos entre múltiplos computadores, enquanto um sistema descentralizado refere-se a uma rede onde o controle e os recursos não estão concentrados em um único ponto, mas sim espalhados entre vários participantes [6].

Neste contexto, a descentralização significa que a rede não depende de um único ponto central de controle. Em vez disso, a blockchain é mantida por uma rede de nós distribuídos em um modelo peer-to-peer, que colaboram para validar e registrar transações. Cada nó na rede Ethereum possui uma cópia completa da blockchain, o que permite a replicação e sincronização das informações entre todos os nós.

Para garantir a legitimidade das informações inseridas em um nó, como as provenientes de uma transação, é necessário um mecanismo de consenso. O

mecanismo de consenso tem como objetivo garantir que todos os nós na rede distribuída tenham uma visão consistente e sincronizada do estado da blockchain. Isso inclui concordar sobre quais transações são válidas, a ordem das transações e a versão mais recente da blockchain.

Na rede Ethereum, a partir da atualização para Proof of Stake (PoS), validadores são escolhidos com base na quantidade de criptomoedas que possuem (staking) e estão dispostos a "arriscar". Esses validadores propõem e validam blocos. O processo de consenso envolve a comunicação entre validadores via RPC (Remote Procedure Call), para confirmar e adicionar novos blocos à blockchain.

Quando um nó cria um novo bloco, ele começa a propagá-lo para os nós conectados na rede. Esse processo de propagação, conhecido como "broadcast", utiliza protocolos como TCP/IP para transmitir o bloco para outros nós. O bloco é enviado como uma mensagem de rede contendo todas as informações necessárias, como o cabeçalho do bloco e as transações que ele contém.

Para que essa transmissão se dê de maneira eficaz, é necessário que o sistema tenha resiliência e tolerância a falhas. Na Ethereum, a descentralização e a replicação dos dados entre múltiplos nós ajudam a garantir que a rede continue funcionando mesmo se alguns nós falharem ou se comportarem de forma maliciosa, mas esse objetivo já é alcançado pela própria natureza de uma blockchain, que pratica a redundância dos dados entre os nós.

A escalabilidade é a capacidade da rede de crescer e lidar com um aumento no volume de transações e nós. Ethereum utiliza técnicas de escalabilidade, como sharding e rollups, para melhorar o desempenho e aumentar a capacidade da rede. Essas técnicas ajudam a distribuir a carga de trabalho e a reduzir o congestionamento, permitindo que a rede suporte um maior número de transações e participantes.

3.2. Princípios de Sistemas Concorrentes

Em sistemas distribuídos como as blockchains, problemas de concorrência são recorrentes e críticos. Esses problemas normalmente aparecem sob a forma de condições de corrida, quando, por exemplo, múltiplas transações competem para alterar o mesmo estado (double-spending e transações sobrepostas), validadores diferentes validam blocos diferentes (forks) e acesso simultâneo por pares diferentes a recursos específicos.

O double-spending surge quando duas transações conflitantes são enviadas quase simultaneamente, criando um conflito sobre qual transação deve ser aceita. A Ethereum trata o double spending por meio de seu mecanismo de consenso, que valida e ordena as transações de forma a garantir que apenas uma transação de gasto duplo seja aceita. O consenso é alcançado com a participação de validadores

que são incentivados a seguir as regras da rede para garantir a integridade das transações.

Nos casos de forks, a Ethereum resolve conflitos através da adoção da cadeia que é mais aceita pelos validadores.

A garantia de que certas operações sejam executadas sem interferências simultâneas é fundamental para manter a integridade dos contratos inteligentes na Ethereum. Para isso, contratos inteligentes podem implementar mecanismos de bloqueio e semáforos para assegurar que apenas uma transação possa acessar um recurso específico de cada vez. Isso ajuda a evitar condições de corrida e a garantir que operações críticas sejam concluídas de forma segura e consistente.

Finalmente, para a visualização de resultados de uma eleição em tempo real, surge o problema de latência na atualização dos resultados, que é fruto de problemas de sincronização.

A latência pode ocorrer entre o momento em que um voto é registrado e a atualização dos resultados exibidos ao usuário. Isso é devido ao tempo necessário para que os blocos sejam minerados, incluídos na blockchain e propagados por todos os nós da rede. Para mitigar esse problema, uma solução é implementar técnicas como polling ou WebSockets para monitorar atualizações de forma mais frequente, além do uso de bibliotecas com alta performance para consultas.

4. Resultados

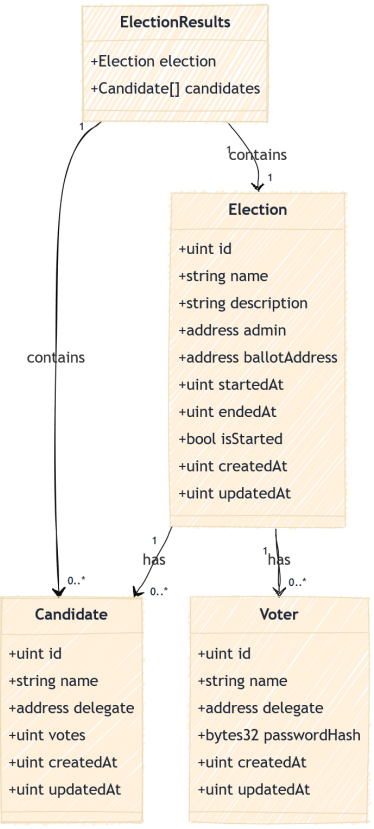
4.1. Arquitetura do Sistema

Pode-se dizer que o Sistema de Votação por Blockchain tem uma arquitetura de blockchain em camadas, composta pelos seguintes componentes:

- **Smart Contract (Blockchain)**: Escrita em Solidity, implementa a lógica de negócios e controla as operações relacionadas a eleições, votos e candidatos com base em permissões autorizadas pela respectiva carteira do usuário.
- **API C#:** Gerencia a autenticação dos usuários e suas carteiras e interage com o smart contract por meio da biblioteca Nethereum. Atua como um intermediário entre o frontend e a blockchain.
- **Frontend** : Interface com o usuário, implementada em HTML, CSS e JavaScript, que comunica com a API para obter dados e realizar operações no smart contract.

A imagem abaixo mostra a visão geral da arquitetura, comunicação e disposição dos componentes:

4.2. Modelagem dos dados



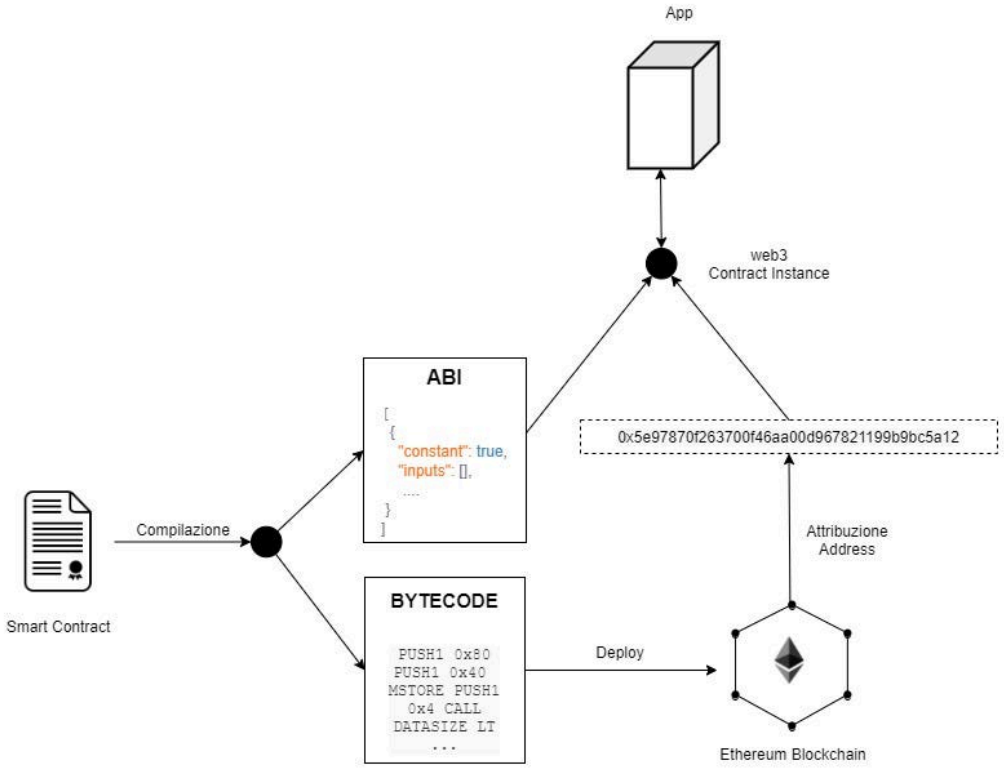
5. Deploy

5.1. Conteinerização

Utilizamos o **Docker** para a criação de imagens da API e dos *Smart Contracts*.

5.2. Blockchain

Realizamos o deploy de contratos inteligentes na blockchain Ethereum, que utiliza **Proof of Work (PoW)** como mecanismo de consenso.



6. Referências

1. F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151. Keywords: Contracts; Electronic voting; Peer-to-peer computing; Privacy; Electronic voting systems; Blockchain; E-Voting; Voting; Smart Contract; Private Blockchain.
2. Fusco, F., Lunesu, M. I., Pani, F., & Pinna, A. (2018). Crypto-voting: A Blockchain-Based E-Voting System. *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance*, 223-227. doi: 10.5220/0006962102230227.
3. C. K. Adiputra, R. Hjort, and H. Sato, "A Proposal of Blockchain-Based Electronic Voting System," 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 2018, pp. 22-27, doi: 10.1109/WorldS4.2018.8611593. Keywords: Blockchain; Electronic voting systems; Electronic voting; Cryptographic hash function; Distributed databases; Blockchain; E-voting; Availability; Universal verifiability.
4. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from https://bitcoin.org/bitcoin.pdf
5. Jafar, U., Ab Aziz, M. J., & Shukur, Z. (2021). Blockchain for Electronic Voting System—Review and Open Research Challenges. *Sensors*, 21(17), 5874. doi: 10.3390/s21175874
6. M. van Steen and A.S. Tanenbaum, Distributed Systems, 4th ed., distributed-systems.net, 2023, p.4.
7. Bashir, Imran. *Mastering Blockchain - Third Edition: A Deep Dive into Distributed Ledgers, Consensus Protocols, Smart Contracts, DApps, Cryptocurrencies, Ethereum, and More*. 3rd ed. Packt Publishing, 2020.