Faculdade de Design, Tecnologia e Comunicação
Universidade Europeia

Sistemas Distribuídos

LEI - 2021/2022

Relatório Final do Projeto

Votechain
A blockchain-based online voting system

GitHub

Felipe Silva - 20190795

Willian Santa Ana - 20190919

Índice

Enquadramento do Projeto

Em situações de eleições há muito o que ser discutido, nomeadamente um dos assuntos mais discutidos é a segurança e validação dos votos, e na maioria das democracias no contexto de eleições públicas os sistemas de votação através do papel ainda predominam, sendo geridos por uma autoridade local e são totalmente centralizados podendo ser difícil garantir a fiabilidade e autenticidade do resultado, tornando um dos principais motivos de contestação e desconfiança dos eleitores [1].

É neste contexto que surgem sistemas de votação online distribuídos e baseados em blockchains, embora ainda não seja uma realidade há muita pesquisa e interesse neste assunto. Um sistema de votação baseado em blockchain é uma abordagem extremamente interessante, uma plataforma blockchain oferece uma base de dados segura e distribuída, transparente ao público, imutável, e de código aberto a todos para ser auditado [2]. Blockchains podem armazenar qualquer tipo de informação, permitindo desenvolver aplicativos poderosos baseados em blockchain. Para um sistema de votação online isso fornece a segurança e fiabilidade necessária para funcionar adequadamente.

Adotando esta abordagem um sistema de votação baseado em uma blockchain terá várias vantagens. A rede é descentralizada e tolerante a faltas tornando o sistema robusto. Todos os registros de votos são transparentes ao público e podem ser verificados por qualquer pessoa, com riscos mínimos de modificação, garantindo maior segurança e confiabilidade no resultado. Isso porque por design os registros na rede são imutáveis, cada bloco contém a hash do bloco anterior e uma alteração em um único bloco na rede invalidaria os demais blocos seguintes [3]. Em termos de privacidade, apesar do endereço dos registros serem representados por uma hash, há estudos que revelam que as transações em altcoins, como o Bitcoin por exemplo, podem ser vinculadas para revelar informações do utilizador [4], tornando um desafio ainda a ser superado e devidamente estudado. Estes fatos sugerem uma aplicabilidade interessante de uma blockchain para um sistema de votação online distribuído, sendo uma possível solução para o problema.

Neste projeto implementamos uma blockchain utilizando o Substrate Framework, que é desenvolvido pela Parity Technologies, trata-se de uma estrutura para construir blockchains personalizadas. Elas podem ser executadas de forma totalmente autônoma, sem depender de qualquer outra tecnologia para funcionar. O Substrate por design suporta módulos personalizados, esses módulos são chamados de "pallets", do qual permite criar aplicações customizadas que interagem com a blockchain. Para resolver o problema da votação online distribuída, criamos um pallet chamado Votechain para tratar da lógica do sistema. Todas estas informações são armazenadas nos blocos como transações, e cada transação deste tipo tem um peso definido que será usado para calcular o custo em tokens ao autor.

O Substrate utiliza por padrão o consenso Proof of Authority, que funciona com uma lista de autoridades definidas que irão cooperar para criar e fechar blocos, este tipo de consenso é utilizado particularmente em blockchains privados e centralizados. Para o nosso problema decidimos que a blockchain seria pública e descentralizada, portanto alteramos o consenso para Nominated Proof of Stake, esta abordagem também utiliza o consenso Babe para criar blocos e o consenso Grandpa para finalizá-los. Em termos práticos haverá uma lista de validadores e outra lista de nominadores, os validadores assumem o papel de validar os blocos e garantir sua fiabilidade, e os nominadores votam de maneira transparente em um conjunto de validadores em um determinado período de tempo.

Para as estações de votos, desenvolvemos uma aplicação cliente com React. Nela o utilizador precisa autenticar-se para interagir com o sistema. Há funcionalidades definidas que precisam de permissão de administrador, como criar uma eleição por exemplo, e outras não como o voto e o resultado.

Casos de Uso

Interação com o sistema de votação

1. Criar uma eleição

   Pré-condições:

   - Utilizador com privilégios de administrador autenticado na plataforma.

   Passos:

   1. Na página criar eleição, o utilizador preenche o formulário com os dados da eleição (i.e., nome da eleição).
   2. Com o formulário preenchido, o utilizador clica em salvar para guardar a eleição.
   3. A eleição é registrada como uma transação na blockchain.
2. Adicionar candidatos:

   Pré-condições:

   - Utilizador com privilégios de administrador autenticado na plataforma.

   Passos:

   a. Na página adicionar candidato, o administrador irá preencher o formulário com o nome do candidato e selecionar a eleição.
   b. Com o formulário preenchido, o utilizador clica em salvar para adicionar o candidato à eleição.
   c. O candidato é registrado na eleição como uma transação na blockchain.

3. Encerrar a eleição:

   Pré-condições:

   - Utilizador com privilégios de administrador autenticado na plataforma.

   Passos:

   a. Na página encerrar eleição, o administrador irá selecionar a eleição que deseja encerrar.
   b. Com a eleição selecionada, o utilizador clica em salvar para confirmar o encerramento da eleição.
   c. O novo estado da eleição é registrado como uma transação na blockchain.

4. Votar:

   Pré-condições:

   - Utilizador autenticado na plataforma.
   - Utilizador não ter efetuado nenhum voto na mesma eleição.

   Passos:

   1. Na página de votação, o utilizador deve selecionar a eleição em que deseja votar.
   2. Com a eleição selecionada, vão ser listados os candidatos cadastrados na eleição.
   3. O utilizador escolhe um candidato, e clicar em votar.
   4. O voto é registrado como uma transação na blockchain.

5. Resultado da eleição:

   Passos:

   1. Na página de resultados o utilizador deve selecionar qual eleição deseja ver o resultado.
   2. Os candidatos são listados em uma leaderboard com o total de votos que receberam e o total de votos válidos na eleição.

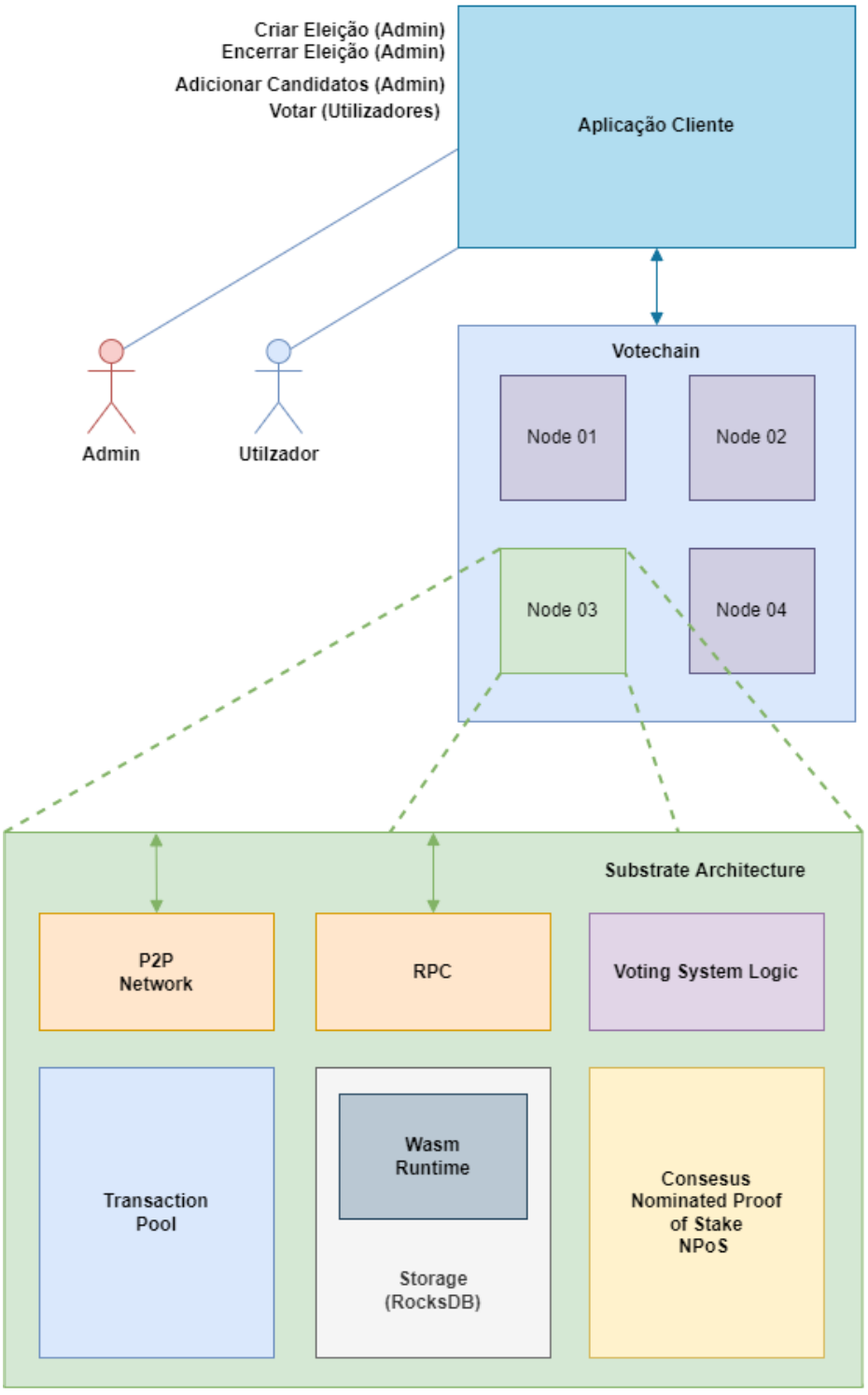
Descrição da Implementação

I. **Descrição genérica da solução a implementar:**
A aplicação de votos será disponibilizada por um site, que utiliza uma WebSockets RPC para se comunicar com a blockchain. Os votos são validados para garantir que cada utilizador só vote uma vez em cada eleição antes de ser salvo na blockchain. Além disso, a aplicação suporta a criação de novas eleições pelos administradores, enquanto os demais utilizadores podem apenas votar e verificar o resultado da eleição.

II. **Enquadramento nas áreas da Unidade Curricular:**
Um sistema de votos pode ser utilizado no contexto de uma eleição, sendo que para esse fim o sistema deve ser capaz de tolerar faltas e principalmente garantir a segurança das informações dos utilizadores. Nesse caso faz todo sentido implementar o sistema em uma blockchain, onde a informação do utilizador é criptografada e toda a informação é replicada por toda a rede.

III. **Requisitos Técnicos para desenvolvimento do projeto:**
Peer to peer network para comunicação HTTP e WebSocket RPC entre os nós na rede, definir mecanismo de consenso para validar os blocos, aplicação cliente para interação com utilizadores e administradores.

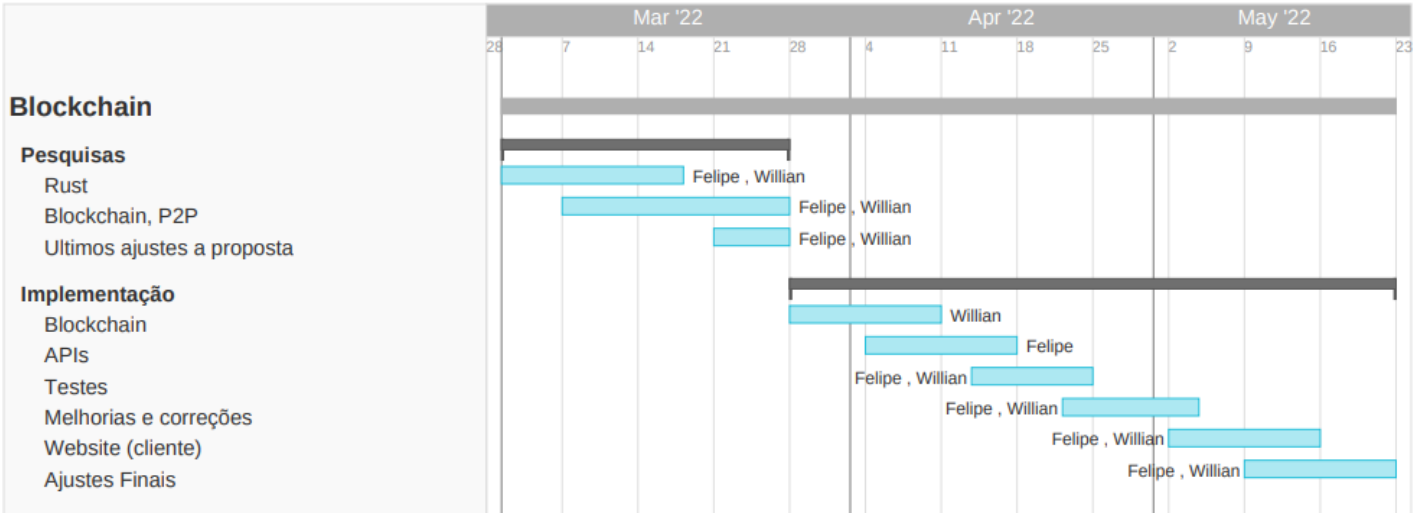
IV. Arquitetura da Solução:



V. Tecnologias a utilizar:

Blockchain em Rust e Substrate Framework, cliente front-end em React, RocksDB

Planeamento



Resultados

Conseguimos implementar aquilo que havíamos proposto no início do projeto. Como resultado temos uma blockchain totalmente independente com um sistema de votação online integrado. Para interagir com o blockchain desenvolvemos uma aplicação cliente em React, que utiliza WebSocket RPC para comunicar-se com a blockchain.

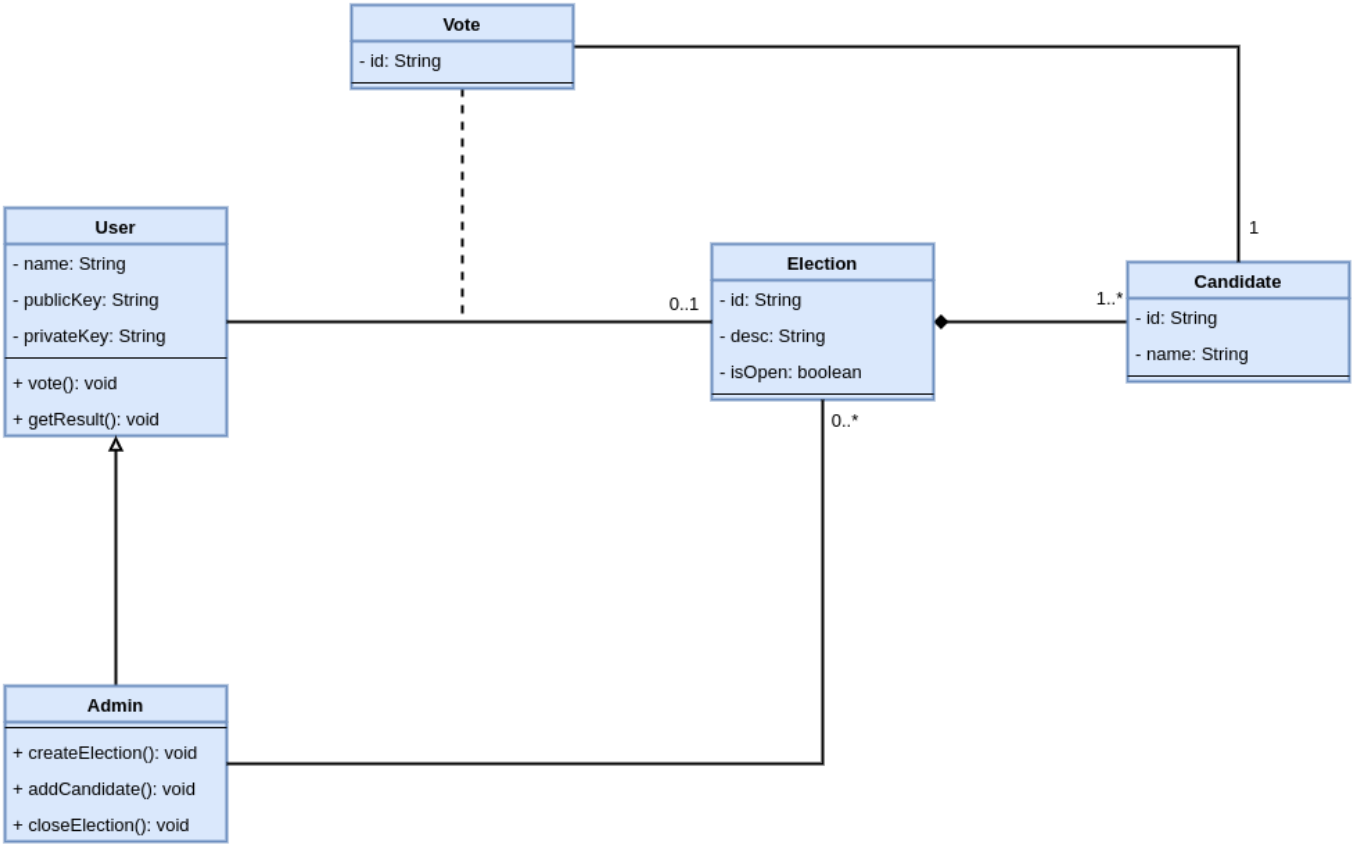
O pallet tem funcionalidades para criar eleições, adicionar candidatos, encerrar a eleição, votar, tratamentos de erros, e não é permitido um ator votar mais de uma vez durante a mesma eleição. Todos os dados referentes à eleição são armazenados no formato de transações dentro dos blocos.

Não conseguimos implementar um período de tempo para a eleição, existe um bloqueio na biblioteca std do Rust no escopo de desenvolvimento dos pallets. Em vez disso, criamos uma funcionalidade para encerrar a eleição, que só pode ser utilizada por um utilizador com permissão de administrador, alterando o estado da eleição para encerrado.

De modo geral estamos contentes com o resultado obtido, o Substrate está bem amadurecido, o que nos permitiu ter um sistema com um bom nível de robustez. Possibilitando escalabilidade e a adição de novas funcionalidades no futuro.

Anexos

Modelo de Domínio



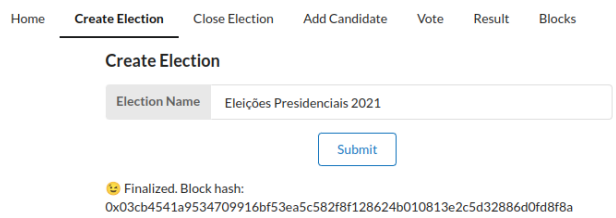
Telas do Sistema

Visualizar Entradas nos Blocos

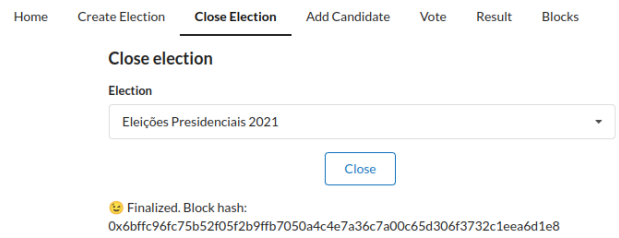
Home | Create Election | Close Election | Add Candidate | Vote | Result | **Blocks**

Key	Value
blockNum	182
blockHash	0x8cc5c53743063f0649ddb309ca64021067dd30790d7765c72cdb6ef6824fbd30
nonce	7
signerId	5GrwvaEF5zXb26Fz9rcQpDWS57CtERHpNehXCPcNoHGKutQY
signature	0xea16326954480a50c7dfa3c3d62a9fc5e769bb25ba2b933fff0320ccae95466185d3b0bf756697c57fe29cbb3f53201061e890cde758e41e250ca1d98325e586
section	votechain
method	createVote
args	**candidate_id:** 0xd97a9d71738fa001da8cde6cef8565b1485a97ef0b5e4b7d7825ca5ead07c56a **election_id:** 0x79ca5b17b4d5ee2b83a46100b5ad7acb07f7d0cd46efe233a7112a60a57b3e52

Criar Eleição



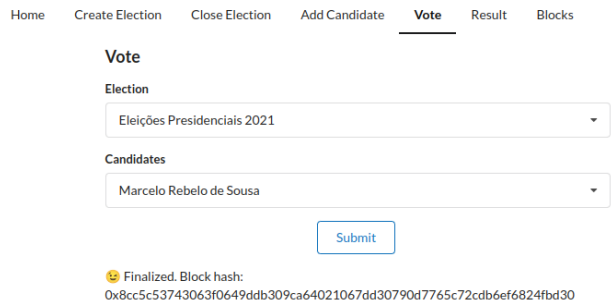
Fechar Eleição



Adicionar Candidato

Visualizar Resultados

Votar



Referências Bibliográficas

[1] Taş R, Tanrıöver ÖÖ. A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting. Symmetry. 2020; 12(8):1328. https://doi.org/10.3390/sym12081328

[2] Riemann, R. and Grumbach, S. (2017). Distributed Protocols at the Rescue for Trustworthy Online Voting. In Proceedings of the 3rd International Conference on Information Systems Security and Privacy - ICISSP, ISBN 978-989-758-209-7; ISSN 2184-4356, pages 499-505. DOI: 10.5220/0006228504990505

[3] Jun Huang, Debiao He, Mohammad S. Obaidat, Pandi Vijayakumar, Min Luo, and Kim-Kwang Raymond Choo. 2021. The Application of the Blockchain Technology in Voting Systems: A Review. ACM Comput. Surv. 54, 3, Article 60 (April 2022), 28 pages. DOI:https://doi.org/10.1145/3439725

[4] Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, Neeraj Kumar, A survey on privacy protection in blockchain system, Journal of Network and Computer Applications, Volume 126, 2019, Pages 45-58, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2018.10.020.

[5] Xuechao Yang, Xun Yi, Surya Nepal, Andrei Kelarev, Fengling Han, Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities, Future Generation Computer Systems, Volume 112, 2020, Pages 859-874, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.06.051.

[6] B. Lashkari e P. Musilek, "A Comprehensive Review of Blockchain Consensus Mechanisms", em IEEE Access , vol. 9, pág. 43620-43652, 2021, doi: 10.1109/ACCESS.2021.3065880.

[7] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen and E. Dutkiewicz, "Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities," in IEEE Access, vol. 7, pp. 85727-85745, 2019, doi: 10.1109/ACCESS.2019.2925010.