Faculdade de Design, Tecnologia e Comunicação
Universidade Europeia

Proposta de Projeto Sistemas Distribuídos

2022

Online Voting Blockchain

Repositório GitHub

Felipe Silva - 20190795

Willian Santa Ana - 20190919

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.

Portanto o que propomos para este projeto é a implementação de uma blockchain baseada em um template básico com o mínimo para fornecer uma estrutura inicial de uma implementação correta de um blockchain, permitindo-nos desenvolver a rede *peer to peer* e a plataforma para o sistema de votação online. Na qual eleições poderão ser criadas por administradores e os eleitores podem autenticar-se para efetivamente formalizar um voto.

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, descrição, candidatos, período da eleição).
   2. Com o formulário preenchido, o utilizador clica em salvar para guardar a eleição.

2. Votar:

   Pré-condições:

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

   Passos:

   1. Na página de votação, é listado os candidatos cadastrados na eleição.
   2. O utilizador escolhe um candidato, e clicar em votar.
   3. O voto é registrado como uma transação na blockchain.

3. Resultado da eleição:

   Pré-condições:

   - Utilizador autenticado na plataforma.
   - Fim do período de eleição.

   Passos:

   1. Na página da eleição 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 API Rest 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.

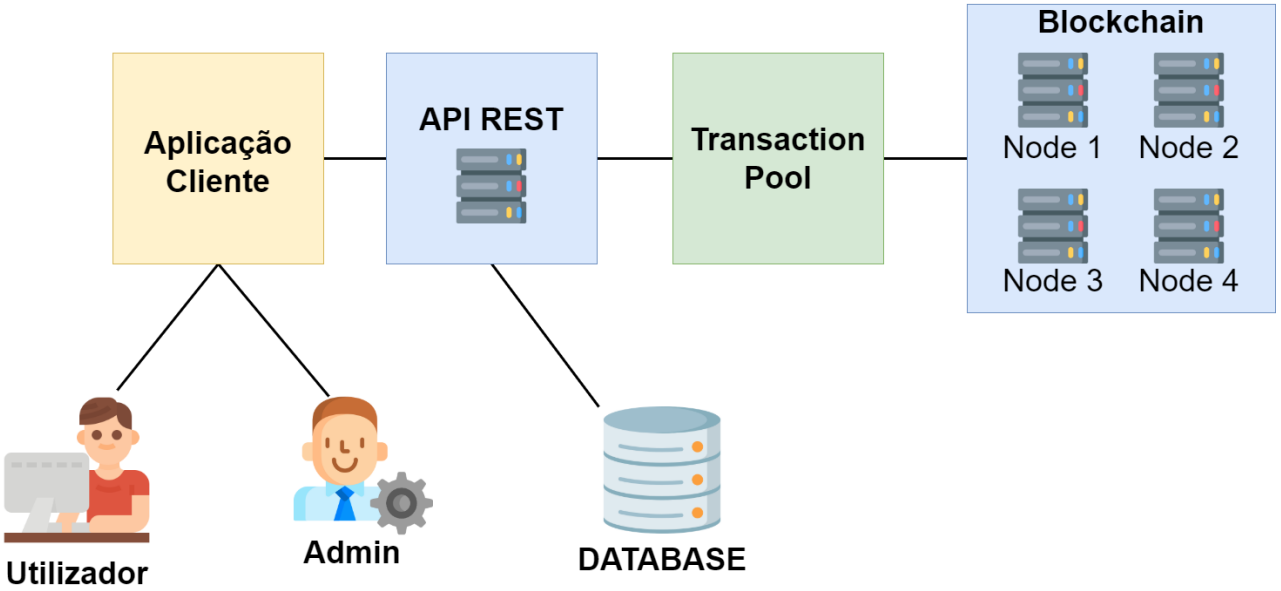
II. Enquadramento nas áreas da Unidade Curricular:

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 gRPC entre os nós na rede, definir mecanismo de consenso para validar os blocos, aplicação cliente para interação com utilizadores e administradores, API REST para comunicação cliente e servidor.

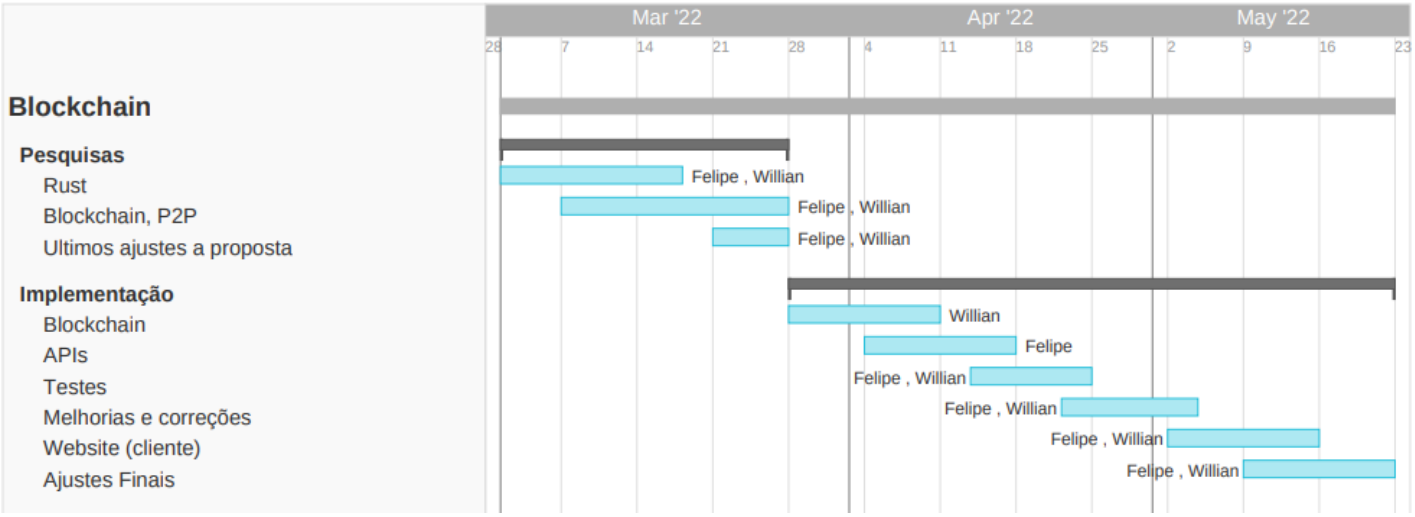
IV. Arquitetura da Solução:



V. Tecnologias a utilizar:

Blockchain em Rust, Base de Dados MongoDB, API Rest com NodeJS e ExpressJS.

Planeamento



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.