

Simpósio de Integração Acadêmica

“Ciências Básicas para o Desenvolvimento Sustentável”

SIA UFV 2023



Desenvolvimento de um software de armazenamento e auditoria de dados de seções eleitorais utilizando *blockchain* e *smart contracts*

Victor Hugo Faria, Rodrigo Smarzarro - Universidade Federal de Viçosa, Campus Rio Paranaíba

Blockchain, Smart Contract, Eleições

Introdução

Com o advento das tecnologias, é imprescindível que sistemas sejam constantemente atualizados e melhorados para cumprir com requisitos de segurança e confiabilidade que mudam ao longo do tempo. Uma nova alternativa no *design* de sistemas transacionais é a *blockchain*. A *blockchain* consiste em uma sequência de blocos ligados por meio de criptografia, que, em conjunto com a tecnologia de *smart contracts*, permite o armazenamento de dados, garantindo imutabilidade e, conseqüentemente, oferecendo ganhos em termos de segurança e transparência. Uma possível aplicação dessa tecnologia é nos sistemas de votação eletrônicos, como o sistema adotado pelo Brasil desde 1996.

Objetivos

O objetivo do trabalho foi o desenvolvimento de um sistema que possa ser integrado ao atual sistema eleitoral (do lado do servidor), permitindo que dados de seções eleitorais sejam armazenados em uma *blockchain*, da qual também poderão ser lidos para fim de auditoria.

Materiais e Métodos

O desenvolvimento do projeto envolveu as etapas de planejamento, implementação do sistema e testes. Na etapa de planejamento, foram levantados os requisitos e foi definida uma arquitetura para o sistema (Figura 1). Na etapa de implementação foi desenvolvido um *smart contract* utilizando a linguagem Solidity, capaz de armazenar dados como contagem de votos, números de seções eleitorais e candidatos. Prosseguiu-se com a implementação de um servidor e uma interface por linha de comando escritos na linguagem de programação C#. O servidor expõe uma interface de métodos que possibilita comunicar-se com a *blockchain*, e a interface por linha de comando permite comunicação com o servidor, facilitando a integração com sistemas externos.

Resultados e Discussão

Foram realizados testes de desempenho para estimar o tempo necessário para o armazenamento dos dados na *blockchain*. Foram realizados cinco testes com 10 mil seções cada (contendo votos simulados para quatro candidatos). A média dos resultados foi de 7 minutos para o armazenamento de todas as entradas.

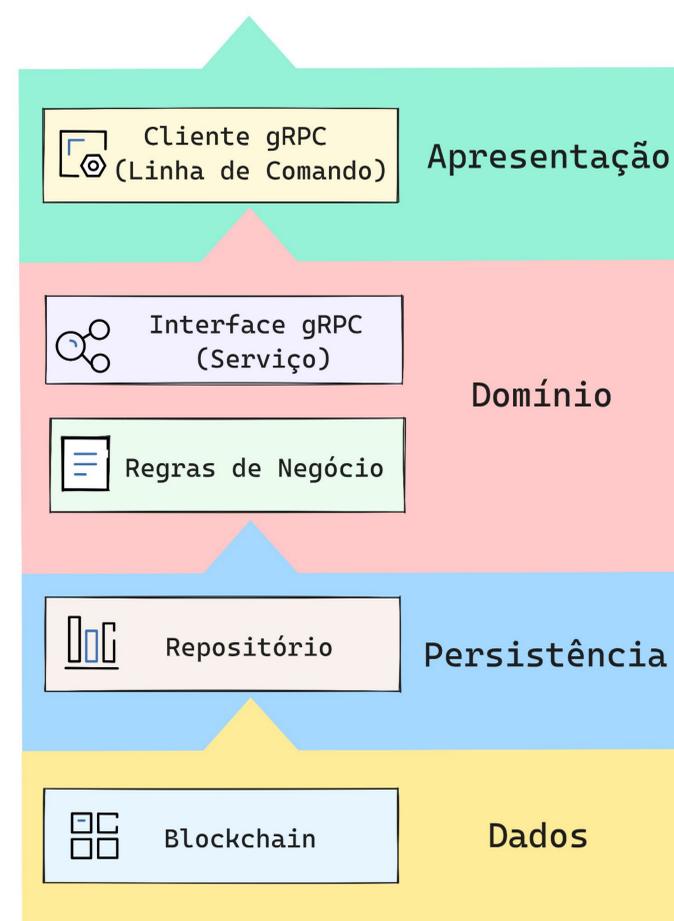


Figura 1 - Esquema de alto nível da arquitetura utilizada no sistema.

Fonte: Próprio Autor.

Conclusões

Extrapolando os dados obtidos para o número de seções da eleição de 2022 (472075 seções), estima-se uma duração aproximada de 5 horas e 30 minutos para completar a operação na *blockchain*. O resultado é positivo quando comparado a trabalhos similares, e indica que a aplicação da tecnologia de *blockchain* deve ser considerada para este contexto.

Bibliografia

- SILVA, M. P. A segurança da democracia e a blockchain. Estudos eleitorais : vol. 13, n. 3 (set./dez. 2018).
- RUAN, P. et al. Blockchains vs. Distributed Databases: Dichotomy and Fusion. arXiv, 2019.
- HELLWIG, D.; KARLIC, G.; HUCHZERMEIER, A. Build Your Own Blockchain. Springer International Publishing, 2020.