Trabalho de Conclusão de Curso

A Privacidade e a Segurança de Dados no Uso de Blockchains em Urnas Eletrônicas: Analisando Modelos baseados em Ethereum

Rael Gugelmin Cunha
ICMC/USP
rael.gc@gmail.com

Orientador: Prof. Mario Gazziro

Sumário

1. Motivação
2. Objetivo
3. Revisão Bibliográfica
4. Problema
5. Metodologia
6. Análise/Resultados
7. Conclusão

1. Motivação

- Ascenção da “Web 3.0”

- Críticas recentes à urna eletrônica brasileira

2. Objetivo

- Analisar os modelos de votação eletrônica propostos sobre o Ethereum utilizando critérios sistemáticos.

- Analisar se algum dos modelos propostos poderia ser um candidato viável a urna eletrônica brasileira.

3. Revisão Bibliográfica

- Conceitos Relacionados:
  - Blockchain (1)
  - Bitcoin (2)
  - Ethereum (3)
  - E-Voting (4)
  - Prova de Conhecimento Zero (5)

1: CHAUM (1979), HABER e STORNETTA (1991), BAYER (1992), DAI (1998), NAKAMOTO (2008)
2: NAKAMOTO (2008)
3: BUTERIN (2014)
4: WIKIPEDIA (2022)
5: BLUM, FELDMAN e MICALI (1988)

3. Revisão Bibliográfica

Artigos Relacionados:

- ARANHA et al (2014)
- **KOÇ et al (2018)**
- **KHOURY et al (2018)**
- ~~**FAYEMI, THOMPSON e AYENI (2021)**~~
- **CHRISTYONO, WIDJAJA e WICKSANA (2021)**
- **McCORRY, SHAHANDASHTI e HAO (2017)**
- TAŞ e TANRIÖVER (2020)

4. Problema

- Como comparar os modelos propostos?

- Os modelos propostos apresentam níveis de segurança e privacidade satisfatórios, considerando que os dados estão em uma blockchain pública?

5. Metodologia

- Os modelos foram analisados seguindo critérios sistemáticos descritos em
  - “A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting” (TAŞ e TANRIÖVER, 2020)

5. Metodologia

- Critérios:

1. Não produzir recibo
2. Não produzir resultados preliminares
3. Integridade de dados
4. Privacidade/votação anônima
5. Somente eleitores registrados
6. Voto único
7. Robustez
8. Confiabilidade
9. Verificabilidade

6. Análise/Resultados

Trabalho / Critério	Towards Secure E-Voting Using Ethereum Blockchain	Decentralized Voting Platform Based on Ethereum Blockchain	Go-Ethereum for electronic voting system using clique as proof-of-authority	A Smart Contract for Boardroom Voting with Maximum Voter Privacy
Não produzir recibo	✓	✓	✓	✓
Não produzir resultados preliminares			? (*)	✓
Integridade	✓	✓		✓
Privacidade				✓
Somente Registrados	✓	✓	✓	✓
Voto Único	✓	✓	✓	✓
Robustez				
Confiabilidade				✓ (**)
Verificabilidade	✓	✓	✓	✓

7. Conclusão

- Nenhum dos modelos propostos atende a todos os requisitos propostos por TAŞ e TANRIÖVER (2020).

- Em vista disso, estaria algum dos modelos propostos aptos a substituir a urna eletrônica brasileira?

- Trilema das redes blockchains: descentralização, segurança e escalabilidade.