**TECNOLOGIA ETHERVOLTZ PARA ELEIÇÕES AUDITÁVEIS.**

***Matheus Faria de Alencar.***

Faculdade ETEP/Faculdade de Tecnologia de São José dos Campos, Avenida Barão do Rio Branco, 882, Jardim Esplanada – 12242-800 - São José dos Campos-SP, Brasil, mtsalenc@gmail.com.

**Resumo -** Este artigo apresenta o desenvolvimento de uma prova de conceito de sistema eleitoral independente de software que remove do administrador a responsabilidade de garantir a disponibilidade, integridade e confiabilidade dos registros digitais dos votos. O código é escrito na linguagem *Solidity* e posteriormente compilado para *bytecode* que pode ser interpretado pela máquina virtual *Ethereum*. O resultado é a criação de uma criptomoeda que existe para representar cada voto, onde cada transação fica gravada num blockchain resistente a censura, ataques de negação de serviço e que está sempre disponível para auditorias.

**Palavras-chave:** eleições, blockchain, ethereum, criptomoeda, ethervoltz.

**Área do Conhecimento:** Engenharia da Computação

**Introdução**

Em sistemas eleitorais de primeira, segunda e terceira geração, os registros digitais dos votos ficam salvos na memória dos equipamentos que precisam ser levados dos locais de votação de volta para as centrais para que ocorra a apuração dos votos. Além dos custos envolvidos para garantir que estes equipamentos não sejam alterados ou destruídos durante o transporte, o administrador também precisa guardar estes registros após a apuração de votos para posteriores auditorias.

Após o período eleitoral, caso um cidadão queira auditar os resultados das eleições ele precisa interagir com o administrador do processo eleitoral para ter acesso os registros digitais, aos equipamentos e aos registros independentes de software (caso o administrador tenha optado por sistemas que utilizem VICE). Cabe ao administrador decidir se ele tem ou não permissão para realizar a auditoria e quais são condições para a realização da mesma.

Os problemas deste tipo de centralização de poderes ficam evidentes no Brasil. Embora não seja objetivo deste documento discutir os efeitos da centralização de poderes em sistemas eleitorais, três casos bem documentados são brevemente listados a seguir:

1. O Caso Marília, SP - 2004: Em auditoria, os Arquivos de Espelhos de Boletins de Urna da 400º Zona Eleitoral indicavam que muitas seções eleitorais tiveram seus resultados recebidos para apuração antes do início da votação. Dois processos judiciais foram iniciados decorrentes destas constatações, ambos encerraram em 2009 sem julgamento final. [1]
2. O Caso Itajaí, SC - 2008: Foi constatada burla intencional na cerimônia de carga e lacração das urnas em que nenhuma urna preparada para a votação passou pelo teste obrigatório prescrito pelo Art. 32 da Res. TSE 22.712/08. Um caso foi o da 97ª Zona Eleitoral onde a urna da seção 236 que foi sorteada para o teste obrigatório foi substituída por outra na hora do teste, preparada exclusivamente para este fim. A urna que foi utilizada para o teste foi posteriormente colocada à parte e recarregada, procedimento que destruiu eventuais provas nela gravadas. [2]
3. O Caso Alagoas - 2006: Diversas irregularidades nos arquivos gerados pelas urnas foram detectadas por auditores externos [4]. Frente as evidências, o administrador negou acesso aos arquivos solicitados pelos auditores e transferiu ao requerente uma cobrança antecipada no valor de R$ 2 milhões para que fosse desenvolvida uma perícia das urnas. Diante do não pagamento do valor proibitivo, o requerente foi multado e condenado por litigância de má-fé.

Este projeto faz do blockchain, da máquina virtual Ethereum e da infraestrutura já em funcionamento formada pelos milhares de nós ao redor do mundo para transformar cada voto em uma criptomoeda que existe somente para este fim. Assim o sistema herda todas as características de segurança da plataforma como redundância, resistência contra ataques de negação de serviço, transparência e autenticação com criptografia por chaves assimétricas.

**Metodologia**

E.

**Resultados**

O.

**Discussão**

O.

**Conclusão**

EtherVoltz é uma proposta que visa decentralizar o processo eleitoral e de auditorias ao transferir a responsabilidade de gerenciar dos registros digitais de votos a um programa que executa em uma máquina virtual que não possui autoridade central, é imutável e resistente a censura. Ao transformar o voto do eleitor em uma criptomoeda, o sistema imediatamente ganha todas as propriedades de segurança do protocolo de consenso e de disponibilidade da rede peer-to-peer utilizado na plataforma.

Embora ainda exista a necessidade da emissão e controle dos VICEs para garantir o Princípio da Independência de Software ao sistema, a separação do destino das duas provas produzidas no momento do voto dá aos eleitores poder de auditoria com limitada necessidade do envolvimento de intermediários.

**Referências**

ACCIOLY, F. Publicações eletrônicas [mensagem pessoal]. Mensagem recebida por mfmendes@uff.br em 24 abr. 2000.

CHEN, H.U; WU, L. Introduction and expiration effects of derivative equity warrants in Hong Kong, Inter.Ver.Fin.Anal. v.10,n.1, 2001. Disponível em : <http://www.elsevier.nl:80/homepage/sae/econbase/finana/menu.sht>. Acesso em: 24 abr.2001.

FISCHER, G.A. Drug resistence in clinical oncology and hematology introduction. **Hematol. Oncol. Clin. North Am.** V.9, n.2, p.11-14, 1995.

HOLTZMAN D.M. Washington University’s Department of Neurology. Disponível em: <http://www.neuro.wustl.edu/neuromuscular/pics/diagrams/nmj.gif>. Acesso em 26 dez. 2001.

RUIZ-SILVA, C. Efeito da corrente elétrica de baixa intensidade em feridas cutâneas de ratos. 2006. 121f. Dissertação (Mestrado em Bioengenharia) – Instituto de Pesquisa e Desenvolvimento, Universidade do Vale do Paraíba, 2006.

WATSON, T. Estimulação Elétrica para a cicatrização de feridas. In: KITCHEN, S.; BAZIN, S. **Eletroterapia de Clayton.** 10. ed. São Paulo: Ed. Manole, 1998.