EtherVoltz: Um Sistema De Votação Auditável No Blockchain Ethereum

Matheus Faria de Alencar, Marize Correa Simões, Diógenes Ramos da Silva
mtsalenc@gmail.com, marize.simoes@etep.edu.br, diogenes.silva@etep.edu.br

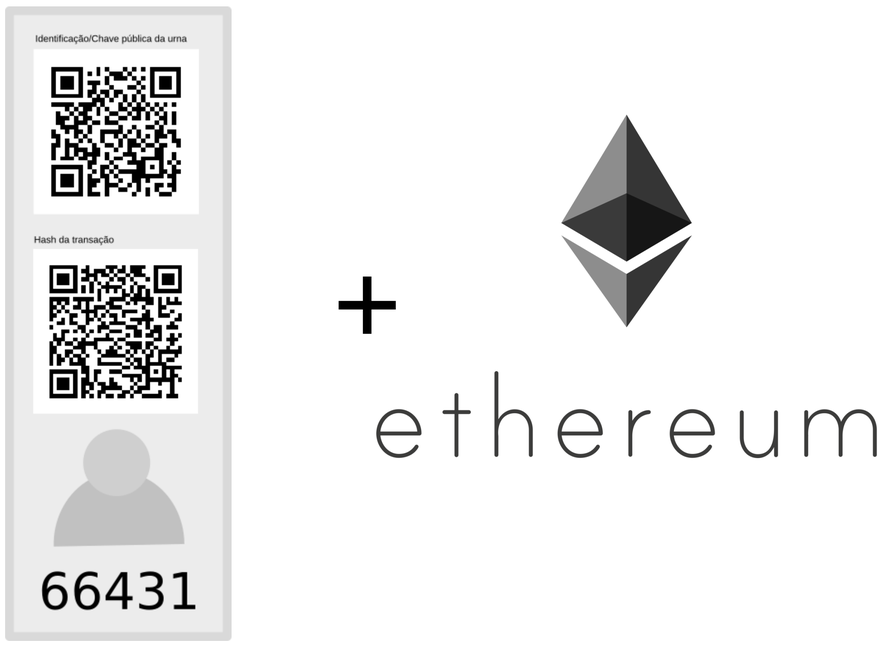
INTRODUÇÃO

Nos sistemas de votação atuais, a centralização das evidências nas mãos do administrador culmina em fraudes e burlas além de dificultar auditorias. Este trabalho apresenta um sistema de votação independente de software que transforma o voto do eleitor em uma criptomoeda batizada de VoltToken para descentralizar e dar auditabilidade ao processo eleitoral.

METODOLOGIA

O sistema EtherVoltz utiliza o computador mundial Ethereum formado pelos milhares de validadores e produtores de blocos ao redor do globo. Para respeitar o Princípio de Independência de Software em Sistemas Eleitorais, o sistema propõe a utilização de uma versão modificada do VICE, que inclui o hash da transação resultante do voto.

FIGURA 1 – Provas Físicas e Digitais

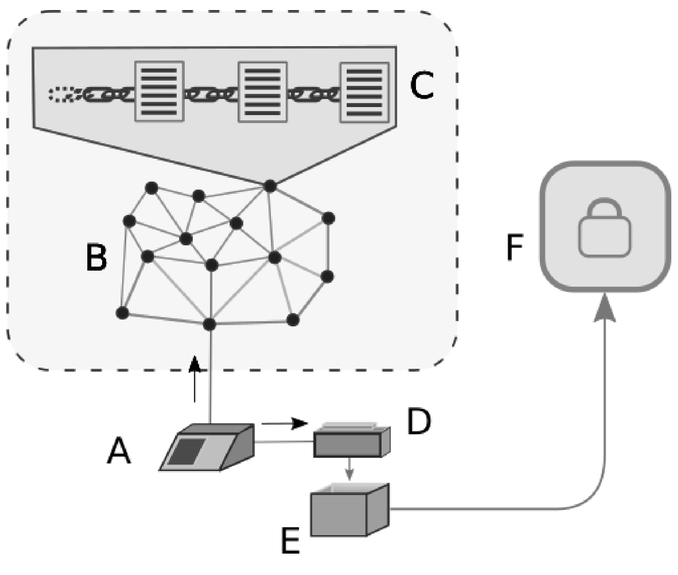


(Fonte: Matheus F. Alencar, 2017)

RESULTADOS

A Figura 2 mostra a arquitetura do sistema EtherVoltz, destacando nas setas os destinos das provas geradas no instante do voto.

FIGURA 2 – Destino das Provas no EtherVoltz



(Fonte: Matheus F. Alencar, 2017)

Backend do sistema é resistente a ataques de negação de serviço distribuídos e possui garantia de uptime enquanto houverem nós e produtores de blocos ativos na rede.

Tabela 1 – Chaves Públicas Utilizadas Em Simulação

Ator	Chave Pública
Administrador	0x51e6Dd45486b5faFedA75595b7501891c9fC54e7
Candidato A	0x063407a72493c8058b415f50076bc990c3927958
Urna A	0x2330D7654399d22A750bd22B8Fc8501A347B7547
Contrato	0xDc2B8EA73104807285A3fAd17c35dcC80E54bA46

(Fonte: Rede de testes Rinkeby, 2017)

A Tabela 1 apresenta as chaves públicas dos atores relevantes do sistema. Através delas um auditor pode analisar o caminho do token desde a sua emissão, distribuição para a carteira das urnas e transferência para a carteira que representa o candidato. O código fonte completo e mais informações do projeto estão disponíveis em https://github.com/mtsalenc/ethervoltz.

CONCLUSÃO

Ao utilizar um programa descentralizado e distribuído como plataforma de hospedagem, o sistema permite que auditorias possam ser realizadas por qualquer indivíduo com acesso a internet, sem a necessidade de envolvimento de uma autoridade central.

Votos são finitos e cada voto é rastreável desde a sua emissão e distribuição para as carteiras das urnas até a carteira que representa o candidato.

Escalabilidade é atingida através do uso de Plasma Chains com protocolo de consenso Prova-de-Autoridade.

REFERÊNCIAS

BRUNAZO, A.F. **Modelos e Gerações dos Equipamentos de Votação Eletrônica.** Disponível em: <www.brunazo.eng.br/voto-e/textos/modelosUE.htm>. Acesso em: 06/08/2017.

ETHERSCAN. **Transferências de VoltToken**. Disponível em: https://rinkeby.etherscan.io/token/0x063407a72493c8058b415f50076bc990c3927958. Acesso em 19/09/2017.

NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008.

RIVEST, R.L.; WACK, J.P. **On the notion of "software independence" in voting systems**. 2006.

SERVULO, S.S. et al. **1º Relatório do Comitê Multidisciplinar Independente.** 2010.

VOGELSTELLER, F. et al. **Ethereum White Paper**. Disponível em: <https://github.com/ethereum/wiki/wiki/White-Paper>. Acesso em: 9 jul. 2017.

AVALIAÇÃO DO TCC