ETHERVOLTZ

Matheus Faria de Alencar

Orientador(a) Acadêmico:
Marize C. Simões

TRABALHO DE CONCLUSÃO DE CURSO
Curso

ETEP FACULDADES

INTRODUÇÃO

Alguns casos fraudes nas eleições no Brasil.

O Caso Diadema, SP – 2000

O Caso Marília, SP – 2004

O Caso Alagoas – 2006

O Caso Itajaí, SC - 2008

INTRODUÇÃO

Ataques e Facilitadores

- Centralização das evidências
- Centralização da apuração
- Dependência de Software
- Anacronismo
- Descrição das causas facilitadoras de fraude
- Inviável auditar o código que está sendo executado em produção

INTRODUÇÃO

Restrições em auditorias

- Burocracia
- Permissões
- Tempo
- Profundidade (depuração proibida, cod prod.)
- Quantidade (linhas de código, dados, compilador)

INTRODUÇÃO

Capitalização de mercado de sistemas de votação:

- Smartmatic (2014): US$ 250 Milhões/ano.
- EveryoneCounts, Syctl, outras: US$ 1525 Milhões/ano.
- +150 países usam sistemas de votação.

Fonte: Financial Times. AHMED, Murad. 2014

OBJETIVO

Criar um modelo de sistema eleitoral que respeite o Princípio da Independência de Software em Sistemas Eleitorais e que descentralize o destino das provas geradas em cada voto, de forma que os registros físicos ficam sob custódia do administrador e os registros digitais ficam sob controle de um programa autônomo que pode ser auditado de sem a necessidade de interagir com o administrador.

DESENVOLVIMENTO

1. Velocidade de Apuração;
2. Disponibilidade
3. Integridade
4. Decentralizado e Autônomo
5. Independência de Software

DESENVOLVIMENTO

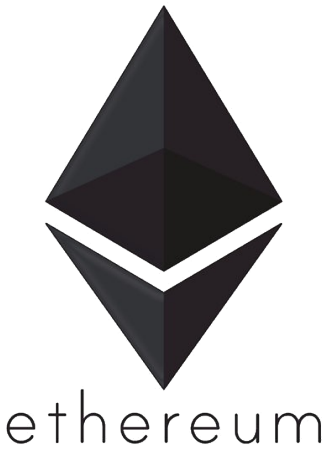
O Voto como criptomoeda: VoltToken.

Regras de emissão e transferência são definidas em um contrato inteligente programado na linguagem *Solidity*.

Este contrato é compilado para byte code que pode ser interpretado pela máquina virtual Ethereum.

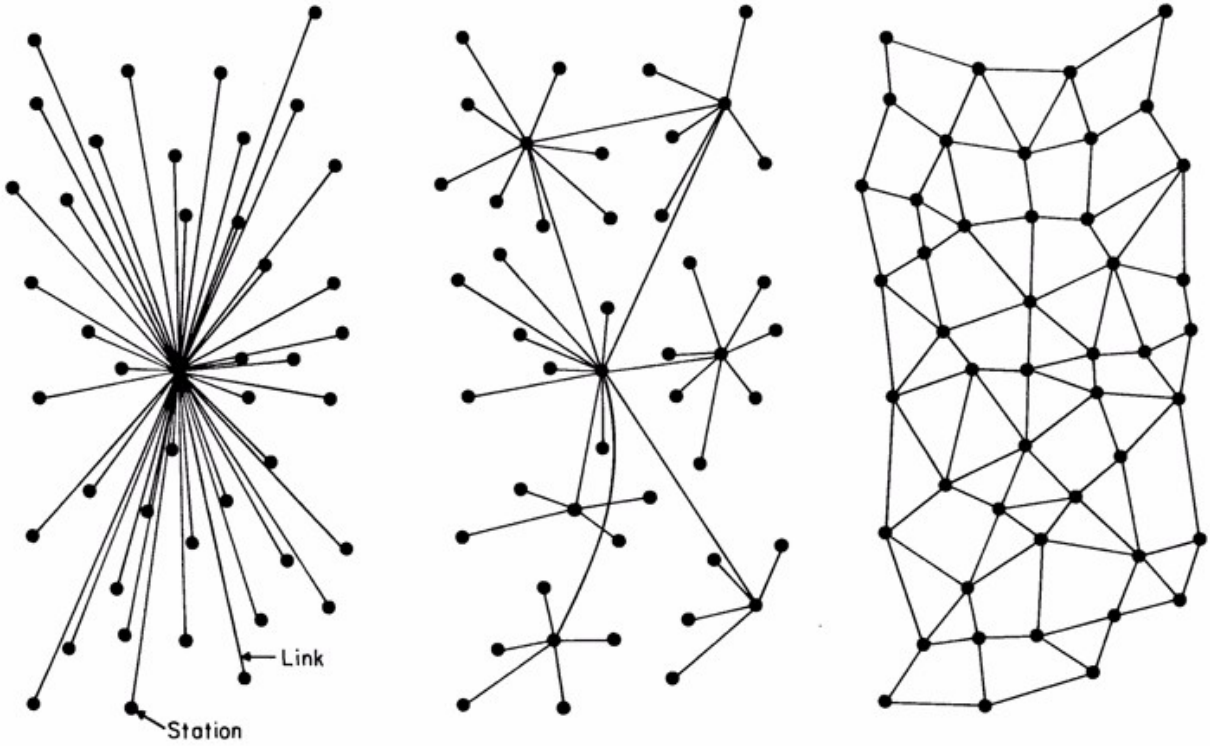
DESENVOLVIMENTO

Mas o que é Ethereum?



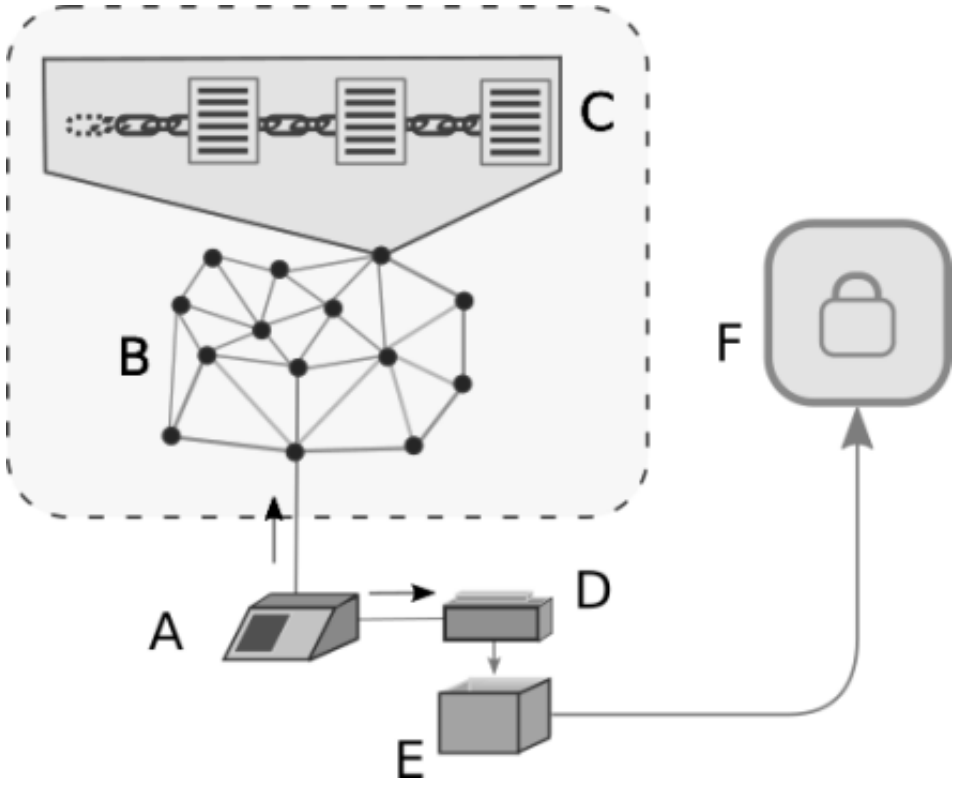
DESENVOLVIMENTO

Arquitetura aplicações tradicionais vs ethervoltz



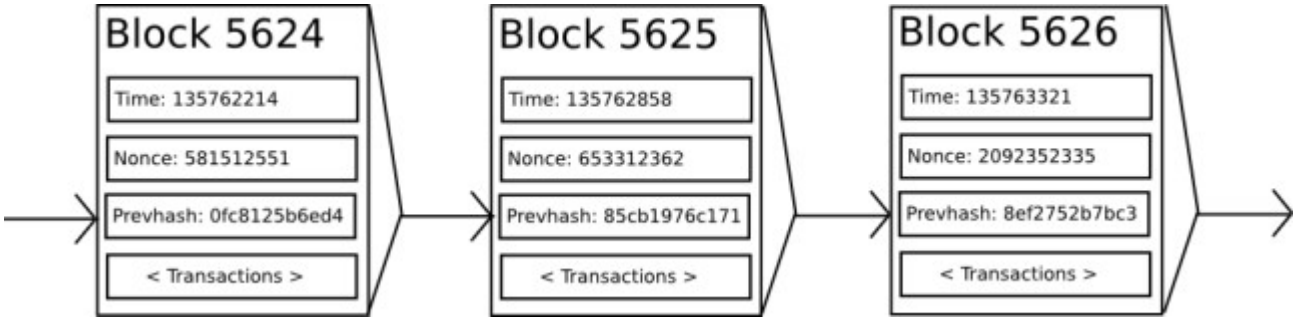
DESENVOLVIMENTO

Arquitetura



DESENVOLVIMENTO

De maneira similar a outras aplicações distribuídas como o *Bitcoin* (CHOHAN, 2017), a infraestutura não possui uma autoridade central com poder de emitir ou realizar transferências de VoltTokens de forma indetectável ou fora das regras de negócio definidas no contrato inteligente.



DESENVOLVIMENTO

Para atingir o item 2 dos requisitos, atender ao Princípio de Independência de Software, a estratégia utilizada é a emissão de uma versão modificada da prova auditável pelo eleitor utilizada em urnas de 2ª geração.

RESULTADOS

Um sistema de votação independente de software e que grava os registros digitais de votos numa base de dados autônoma e resistente a censura. Foi escrito um contrato inteligente na linguagem *Solidity* utilizando o *framework Truffle*.

Cada função criada possui testes unitários desenvolvidos utilizando *javascript*, as suites de asserção *mocha.js* e *chai.js* e o cliente RPC *testrpc* para a execução dos testes automatizados.

RESULTADOS

- A transferência de VoltTokens *para candidatos* só pode ocorrer durante o período eleitoral;
- Apenas endereços de carteiras que representam candidatos podem receber VoltTokens;
- O número total de VoltTokens em circulação é finito e sua quantidade é definida em código.
- Nenhuma nova unidade da moeda pode ser emitida após a criação do sistema;

RESULTADOS

- Cada urna recebe precisamente o número de VoltTokens correspondente ao número de eleitores que devem votar naquela urna;
- O administrador só pode definir candidatos e urnas antes do período eleitoral;
- O administrador só pode distribuir VoltTokens às urnas antes do período eleitoral.

RESULTADOS

- A aplicação distribuída foi implantada na rede de testes Rinkeby sob protocolo de consenso Prova-de-Autoridade para simular uma eleição real em funcionamento no blockchain.

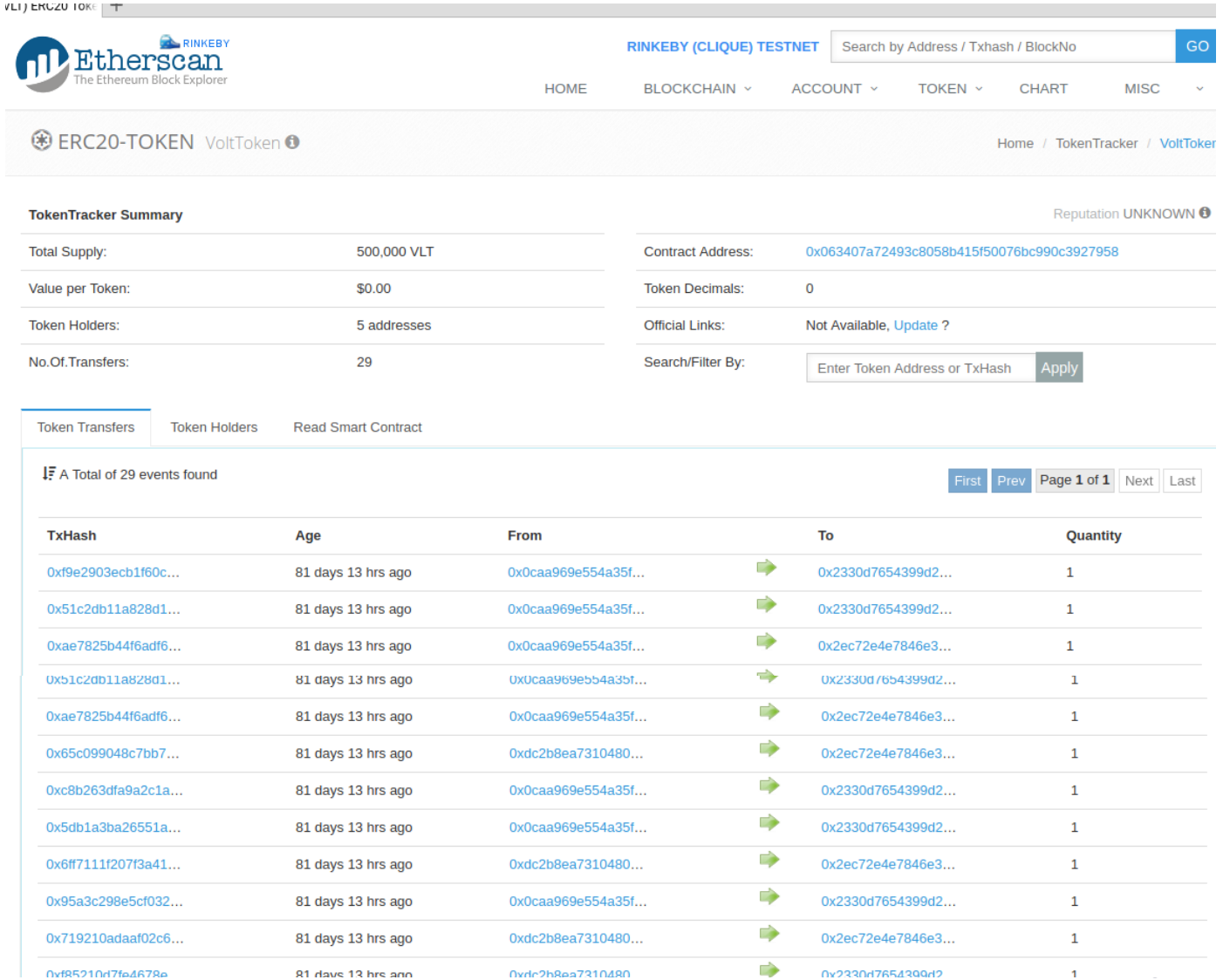
Tabela 2 – Chaves públicas das carteiras utilizadas.

	Chave Públicas
(1)	0x51e6dd45486b5fafeda75595b7501891c9fc54e7
(2)	0x2ec72e4e7846e33bd0cc88cbaecdf4bb01bcd3ff
(3)	0x2330d7654399d22a750bd22b8fc8501a347b7547
(4)	0x0caa969e554a35f1176d739e384045691d21ee64
(5)	0xdc2b8ea73104807285a3fad17c35dcc80e54ba46
(6)	0x063407a72493c8058b415f50076bc990c3927958

Fonte: Blockchain Rinkeby.

RESULTADOS

- INTRODUÇÃO
- OBJETIVO
- DESENVOLVIMENTO
- RESULTADOS
- CONCLUSÃO



RESULTADOS

CONCLUSÃO

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 nativa da plataforma.

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.

Obrigado

Matheus Faria de Alencar
mtsalenc@gmail.com
mtsalenc.github.io/project-pages/ethervoltz