

# ETHERVOLTZ

**Matheus Faria de Alencar**

Orientador(a) Acadêmico:  
**Marize C. Simões**

**TRABALHO DE CONCLUSÃO DE CURSO**  
**Curso**



# INTRODUÇÃO

## INTRODUÇÃO

Alguns casos fraudes nas eleições no Brasil.

## OBJETIVO

O Caso Diadema, SP – 2000

O Caso Marília, SP – 2004

## DESENVOLVIMENTO

O Caso Alagoas – 2006

## RESULTADOS

O Caso Itajaí, SC - 2008

## CONCLUSÃO

# INTRODUÇÃO

## 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

## OBJETIVO

## DESENVOLVIMENTO

## RESULTADOS

## CONCLUSÃO

# INTRODUÇÃO

## INTRODUÇÃO

### Restrições em auditorias

## OBJETIVO

- Burocracia
- Permissões

## DESENVOLVIMENTO

- Tempo

## RESULTADOS

- Profundidade (depuração proibida, cod prod.)
- Quantidade (linhas de código, dados,

## CONCLUSÃO

compilador)

# INTRODUÇÃO

## 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.

## OBJETIVO

## DESENVOLVIMENTO

## RESULTADOS

## CONCLUSÃO

Fonte: Financial Times. AHMED, Murad. 2014

# OBJETIVO

INTRODUÇÃO

**OBJETIVO**

DESENVOLVIMENTO

RESULTADOS

CONCLUSÃO

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

INTRODUÇÃO

OBJETIVO

DESENVOLVIMENTO

RESULTADOS

CONCLUSÃO

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

# DESENVOLVIMENTO

## INTRODUÇÃO

O Voto como criptomoeda: VoltToken.

## OBJETIVO

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

## DESENVOLVIMENTO

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

## RESULTADOS

## CONCLUSÃO



# DESENVOLVIMENTO

INTRODUÇÃO

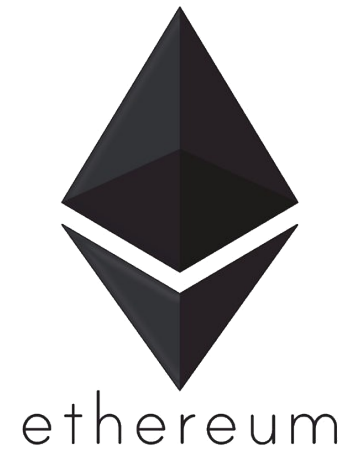
Mas o que é Ethereum?

OBJETIVO

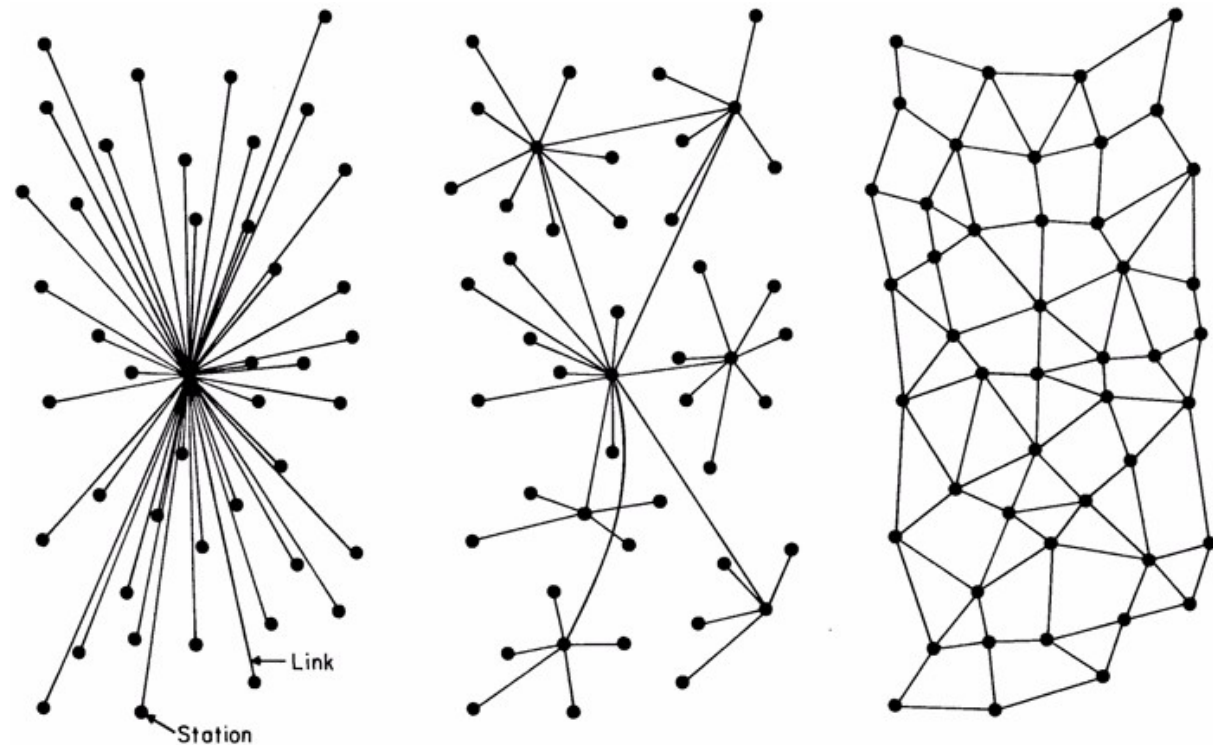
DESENVOLVIMENTO

RESULTADOS

CONCLUSÃO

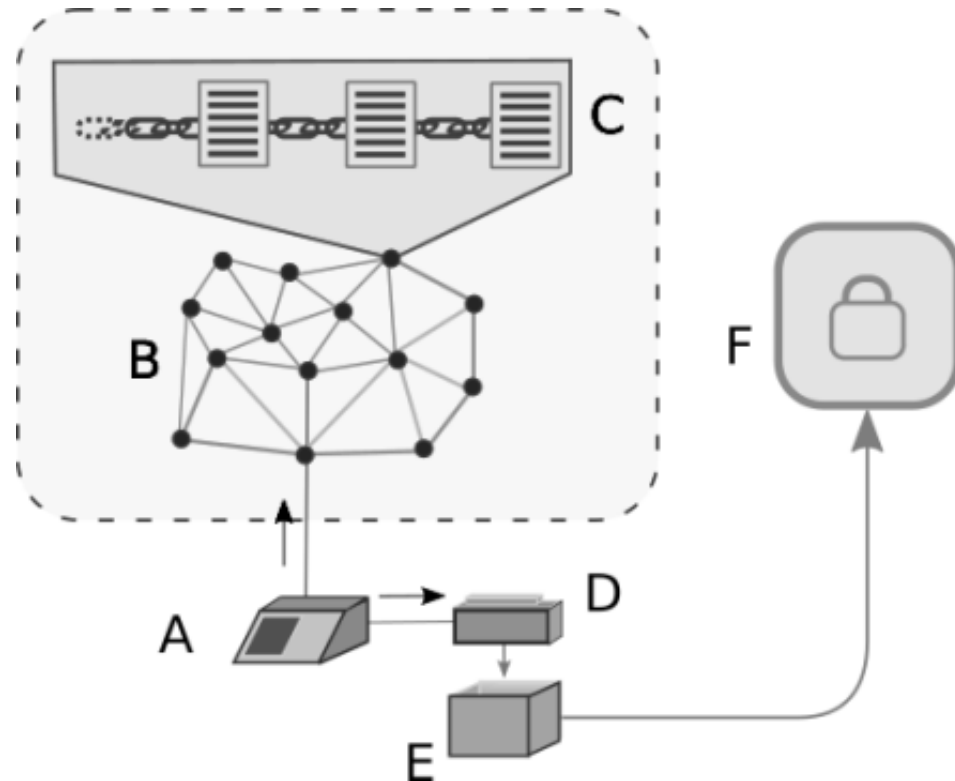


## Arquitetura aplicações tradicionais vs ethervoltz



# DESENVOLVIMENTO

## Arquitetura



# DESENVOLVIMENTO

INTRODUÇÃO

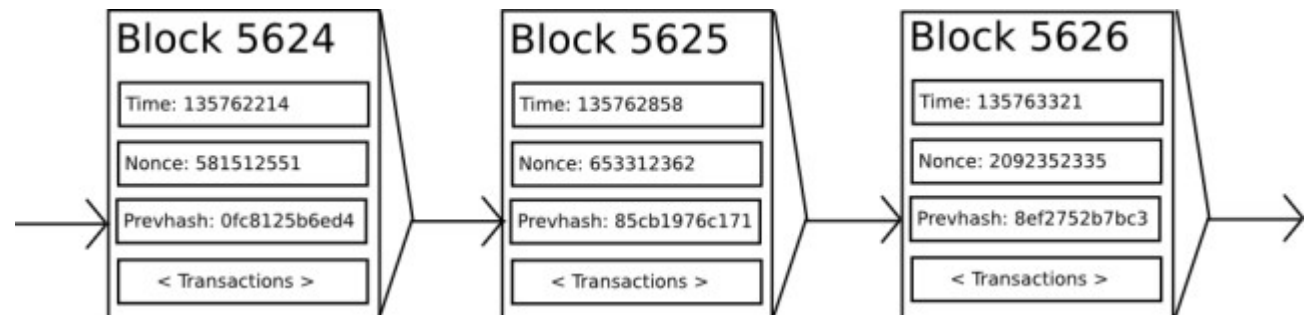
OBJETIVO

DESENVOLVIMENTO

RESULTADOS

CONCLUSÃO

De maneira similar a outras aplicações distribuídas como o *Bitcoin* (CHOHAN, 2017), a infraestrutura 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

INTRODUÇÃO

OBJETIVO

DESENVOLVIMENTO

RESULTADOS

CONCLUSÃO

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

INTRODUÇÃO	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 <i>Solidity</i> utilizando o <i>framework Truffle</i> .
OBJETIVO	
DESENVOLVIMENTO	
RESULTADOS	Cada função criada possui testes unitários desenvolvidos utilizando <i>javascript</i> , as suites de asserção <i>mocha.js</i> e <i>chai.js</i> e o cliente RPC <i>testrpc</i> para a execução dos testes automatizados.
CONCLUSÃO	

# RESULTADOS

## INTRODUÇÃO

## OBJETIVO

## DESENVOLVIMENTO

## RESULTADOS

## CONCLUSÃO

- 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

INTRODUÇÃO

OBJETIVO

DESENVOLVIMENTO

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.

CONCLUSÃO



# 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

VLT | ERC20 TOKEN



RINKEBY (CLIQUE) TESTNET

Search by Address / Txhash / BlockNo

GO

HOME

BLOCKCHAIN ▾

ACCOUNT ▾

TOKEN ▾

CHART

MISC ▾

ERC20-TOKEN VoltToken ⓘ

Home / TokenTracker / VoltToken

## TokenTracker Summary

Reputation UNKNOWN ⓘ

Total Supply:	500,000 VLT
Value per Token:	\$0.00
Token Holders:	5 addresses
No.Of.Transfers:	29

Contract Address: 0x063407a72493c8058b415f50076bc990c3927958

Token Decimals: 0

Official Links: Not Available, [Update ?](#)

Search/Filter By:

Token Transfers

Token Holders

Read Smart Contract

⚡ A Total of 29 events found

**Page 1 of 1**

TxHash	Age	From	To	Quantity
0xf9e2903ecb1f60c...	81 days 13 hrs ago	0x0caa969e554a35f...	0x2330d7654399d2...	1
0x51c2db11a828d1...	81 days 13 hrs ago	0x0caa969e554a35f...	0x2330d7654399d2...	1
0xae7825b44f6adf6...	81 days 13 hrs ago	0x0caa969e554a35f...	0x2ec72e4e7846e3...	1
0xb1c2db11a828d1...	81 days 13 hrs ago	0x0caa969e554a35f...	0x2330d7654399d2...	1
0xae7825b44f6adf6...	81 days 13 hrs ago	0x0caa969e554a35f...	0x2ec72e4e7846e3...	1
0x65c099048c7bb7...	81 days 13 hrs ago	0xdc2b8ea7310480...	0x2ec72e4e7846e3...	1
0xc8b263dfa9a2c1a...	81 days 13 hrs ago	0x0caa969e554a35f...	0x2330d7654399d2...	1
0x5db1a3ba26551a...	81 days 13 hrs ago	0x0caa969e554a35f...	0x2330d7654399d2...	1
0x6ff7111f207f3a41...	81 days 13 hrs ago	0xdc2b8ea7310480...	0x2ec72e4e7846e3...	1
0x95a3c298e5cf032...	81 days 13 hrs ago	0x0caa969e554a35f...	0x2330d7654399d2...	1
0x719210adaaf02c6...	81 days 13 hrs ago	0xdc2b8ea7310480...	0x2ec72e4e7846e3...	1
0xf85210d7fe4678a...	81 days 13 hrs ago	0xdc2b8ea7310480...	0x2330d7654399d2...	1

INTRODUÇÃO

OBJETIVO

DESENVOLVIMENTO

RESULTADOS

CONCLUSÃO

# RESULTADOS

*EtherVoltz*

INTRODUÇÃO RECURSOS COMO FUNCIONA? EQUIPE

INTRODUÇÃO

OBJETIVO

DESENVOLVIMENTO

RESULTADOS

CONCLUSÃO

*EtherVoltz*

## BLOCKCHAIN PARA ELEIÇÕES AUDITÁVEIS

CONTE-ME MAIS

**ELEIÇÕES CENTRALIZADAS NÃO SÃO CONFIÁVEIS.**

*Confira o portfólio das eleições no Brasil.*

# CONCLUSÃO

INTRODUÇÃO	
OBJETIVO	
DESENVOLVIMENTO	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.
RESULTADOS	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.
CONCLUSÃO	

# Obrigado

**Matheus Faria de Alencar**

[mtsalenc@gmail.com](mailto:mtsalenc@gmail.com)

[mtsalenc.github.io/project-pages/ethervoltz](https://mtsalenc.github.io/project-pages/ethervoltz)