

Revolução Blockchain | Impactos da Tecnologia

Retomando o "*demos*" da Democracia.

 Por Matheus Alencar (mtsalenc@gmail.com)

Quem sou eu? 🐧

Sumário

1. Arquitetura 

2. Criptoeconomia 

3. Impactos 

4. Urnas Eletrônicas 

5. Q&A 

6. Extra 

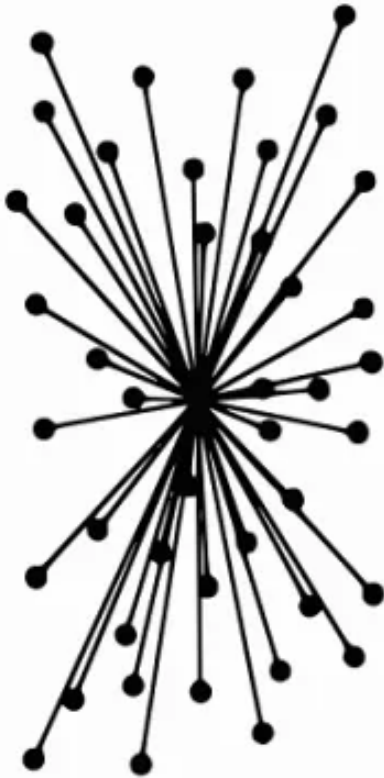
Prólogo

Um grande caminho a frente

Conteúdo potencialmente técnico, mas caminharemos juntos.



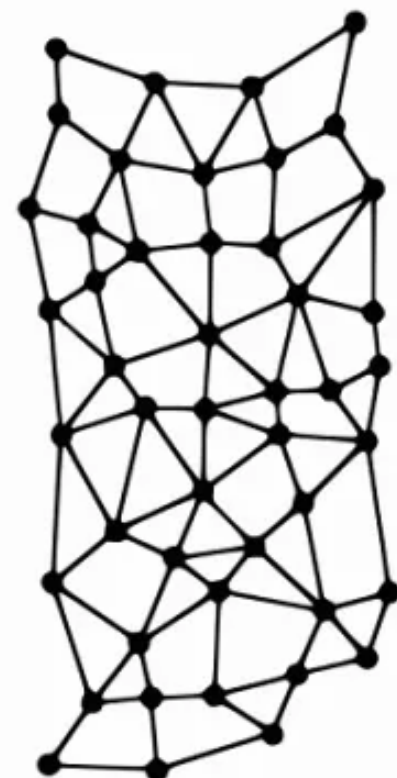
Arquiteturas



Centralized






Decentralized



Distributed

Criptoeconomia

- Qualquer pessoa pode processar transações. 
- Incentivos economicos para se comportar bem. 
- Desincentivos para quem se comporta mal. 

Criptoeconomia

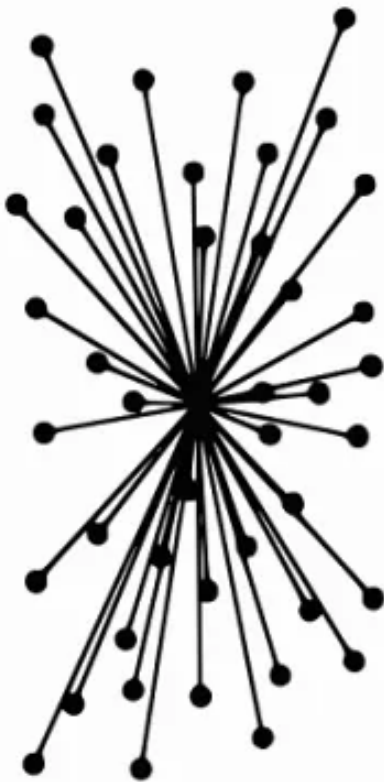
- A suprema corte criptográfica -> Punições financeiras para quem se comporta mal. 💰
- Recompensas para detetives. 🕵️

E daí?



Ataques de Negação de Serviço - O que é?

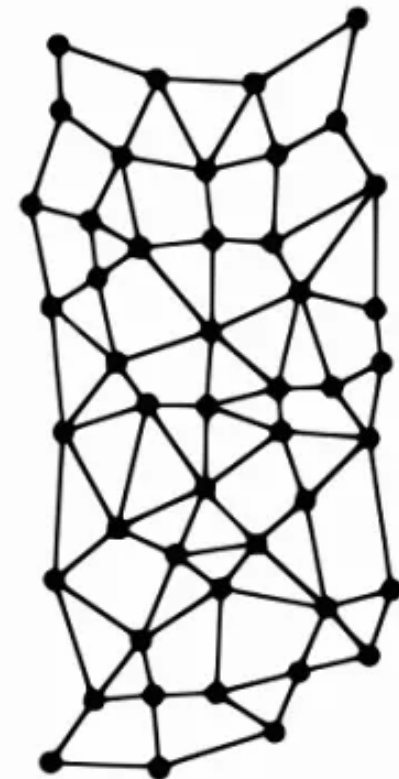
Programas "Imparáveis"



Centralized



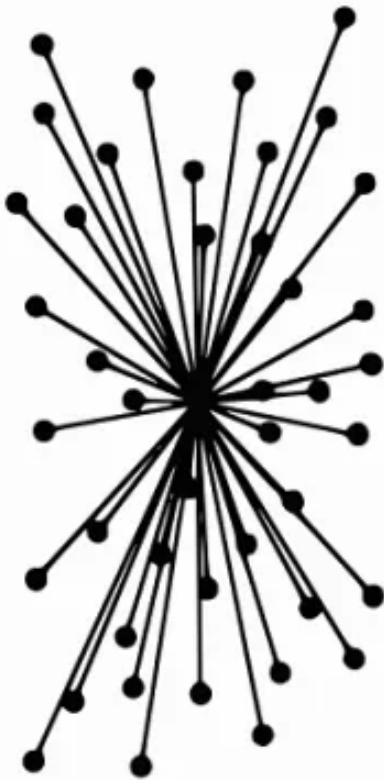
Decentralized



Distributed

Censura

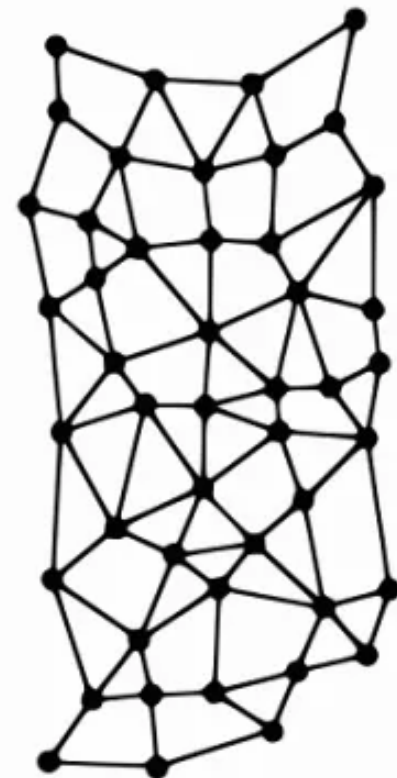
Eleições "Incensuráveis"



Centralized



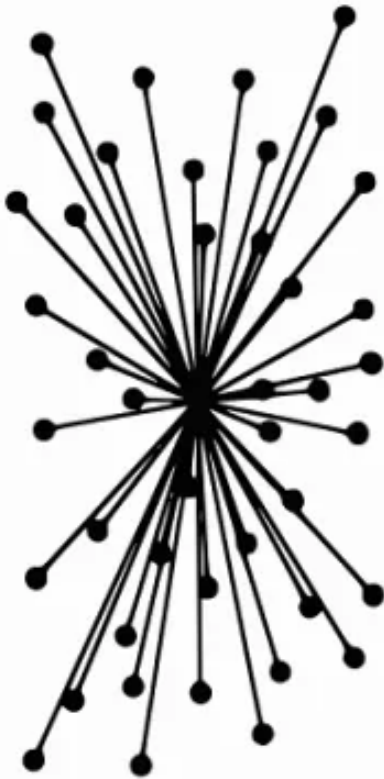
Decentralized



Distributed

Hacks no Código

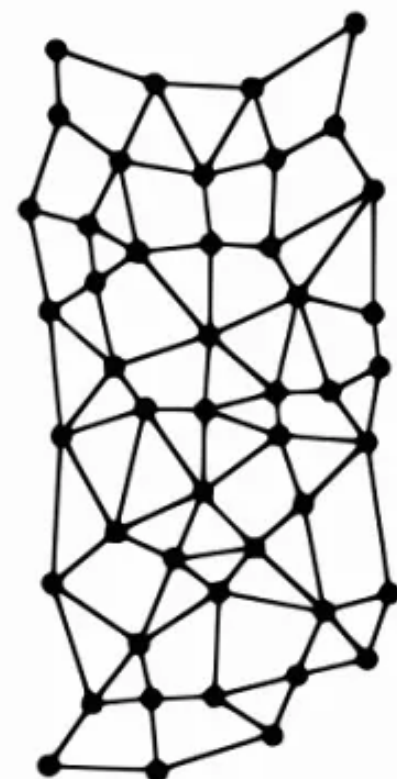
Código imutável e auditável



Centralized



Decentralized



Distributed

Descentralizado vs Descentralizado

Falando de Autoridades, diferença entre:

- Rede distribuída.
- Poder distribuído.

Comparando Impactos

Característica	Tradicional	Blockchain
Alteração de Código	Vulnerável ✗	Resistente ✓
Ataques DDoS	Ponto de falha único ✗	P2P ✓
Censura	1 autoridade ✗	Milhares de Autoridades ✓
Auditorias	Centralizado ✗	Descentralizado ✓

Criptomoedas

- O que dá valor ao Bitcoin?
- O que dá valor ao Dólar?
- **Pessoas e escassez.**




Criptomoedas

- Quem controla a emissão de Reais? 🧑
- Quem controla a emissão de Bitcoins? 💻



Impacto na Economia

- Fim do imposto sem representatividade. 
- Exigência de transparência na cobrança de impostos.
- Casa da moeda descentralizada.

Funcionamento Básico: Livro Razão Replicado

ID	Qtd	Unidade	Remetente	Destinatário
..
3925	3	real	João	Alice
3928	20	real	-	para Alice
3926	2	real	Alice	para Carlos
3927	1	real	Carlos	para João
3928	1	real	João	para Alice
...

Saldos Acumulados

Carteira	Quantidade
..	...
Alice	351234
Bob	5234242
João	774567
Ronaldo	923451
...	...

Urnas Eletrônicas



Tipos de Urnas

1ª Geração - Dependentes de Software, modelo DRE.



Tipos de Urnas

2ª Geração - Independentes de Software, DRE com VICE.



México, desde 2012

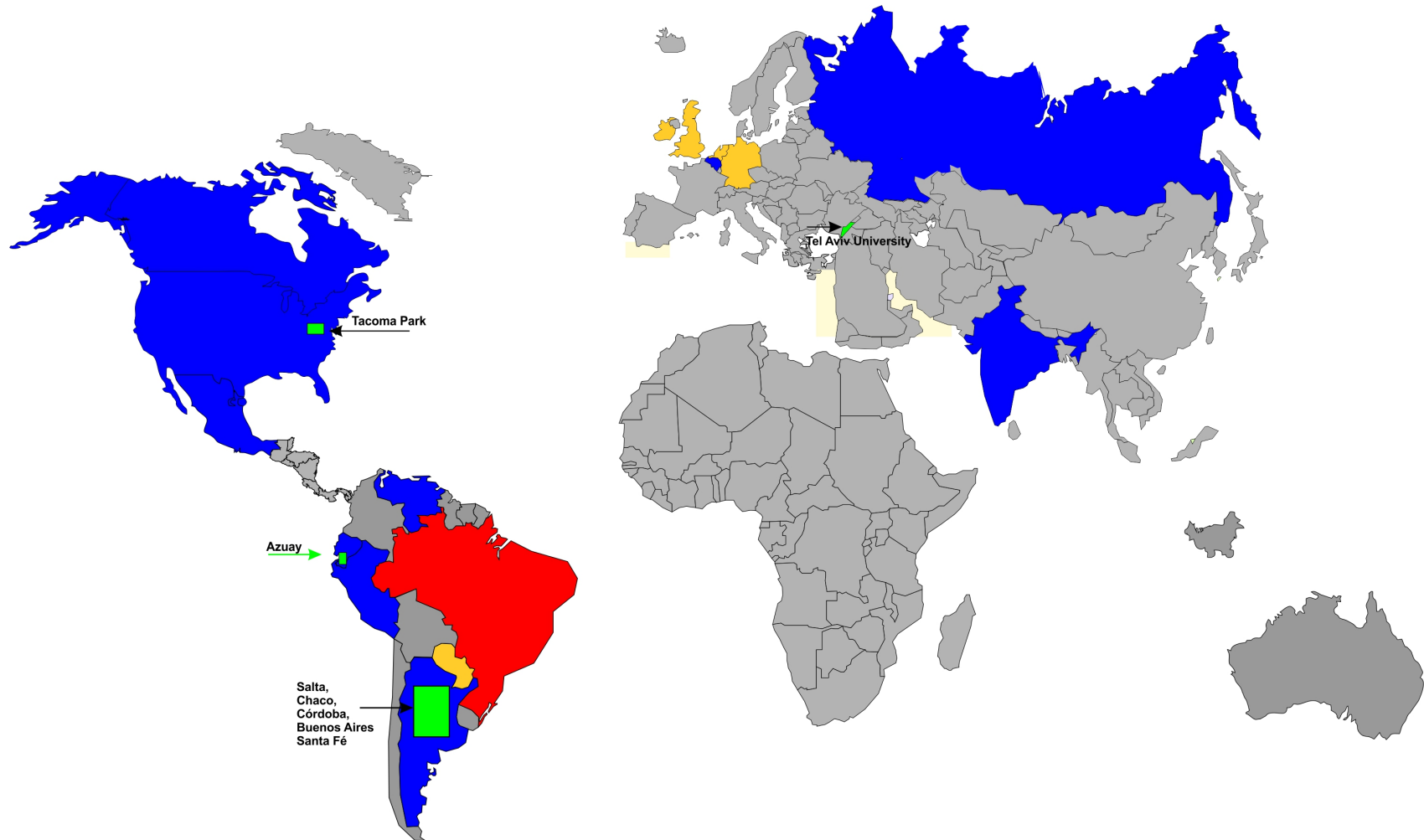
Tipos de Urnas

3ª Geração - Independentes de Software, com BVE.



Israel, EUA, Equador, Argentina.

Comparativo?



Fonte: votoseguro.org, 2014

Centralização de Poderes no Brasil?

TREs e STE = Executivo, Legislativo e Judiciário.



Algumas Consequências

1. O Caso Marília, SP - 2004: Em auditoria, os Arquivos de Espelhos de Boletins de Urna indicavam que muitas seções eleitorais tiveram seus resultados recebidos para apuração **antes** do início da votação
2. O Caso Itajaí, SC - 2008: A urna que foi sorteada para o teste obrigatório **foi substituída** por outra na hora do teste.

Fonte: 1º Relatório do Comitê Multidisciplinar Independente.

Algumas Consequências

3. O Caso Diadema, SP - 2000: Foram negados a todos os partidos que solicitaram o acesso aos registros digitais dos votos realizados nas urnas eletrônicas. Somente 9 meses após a eleição os partidos obtiveram acesso, não aos registros dos votos, mas aos Arquivos de LOG das urnas que apontaram que todas as urnas haviam sido carregadas fora da cerimônia oficial de carga e lacramento das urnas.

Fonte: 1º Relatório do Comitê Multidisciplinar Independente.

Fontes Principais do Problema

- Provas sob custódia do administrador.
- Software sob custódia do administrador.

Auditorias?

- Só com a permissão do administrador.
- Na casa dele.
- Por tempo limitado.
- No computador dele.
- Com ele olhando.



Blockchain como solução:

ID	Qtd	Unidade	Remetente	Destinatário
..
3925	1387	voto	TRE 3	Urna 3 ZE 246
3926	6117	voto	TRE 1	Urna 7 ZE 361
3927	1	voto	Urna 3 ZE 246	Candidato A
3928	1	voto	Urna 3 ZE 246	Candidato B
...

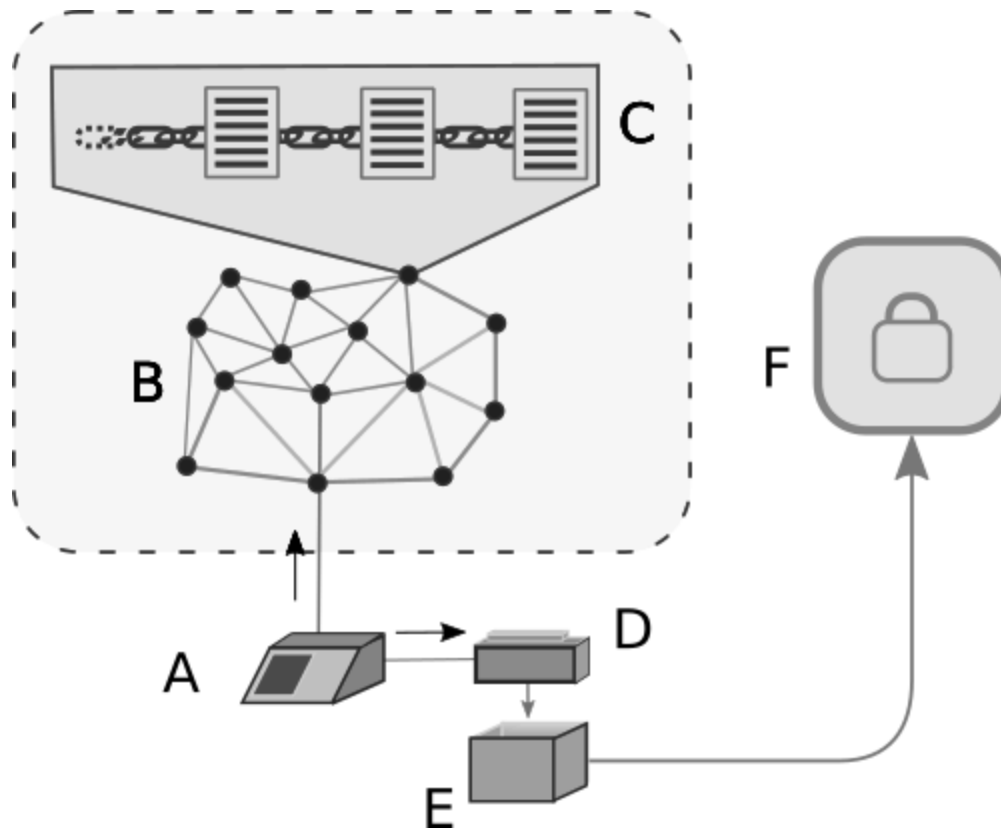
Resultado: Transparência.

- Auditorias acontecem na sua casa.
- Seu computador processa os dados.
- Custódia das provas descentralizada.
- Roubos de votos são visíveis.

Independência de Software: VICE



Destino de Provas



Q&A

Matheus Alencar | mtsalenc@gmail.com | github: mtsalenc