

# Blockchain, Criptomoedas & Tecnologias Descentralizadas

## Introdução


Prof. Dr. Marcos A. Simplicio Jr. – [mjunior@larc.usp.br](mailto:mjunior@larc.usp.br)  
Escola Politécnica, Universidade de São Paulo

# Descentralização: definição

- <https://michaelis.uol.com.br/busca?id=3WAa> (descentralizar)
  - Afastar(-se), desviar(-se) do centro; fazer dispersar-se do centro ou de lugar de concentração
  - [Adm, Polít] Dispersar ou distribuir as funções ou os poderes de um governo, autoridade, administração
  - Fazer dispersar-se do centro ou lugar de concentração.
- <https://www.dicio.com.br/descentralizacao/>
  - Ato ou efeito de descentralizar, de afastar do centro; descentração.
  - [Polít] Sistema administrativo que busca transferir certos poderes e competências, característicos do poder central e concentrados num só lugar, para outros setores menores, periféricos ou locais.
  - [Polít] Atribuição de poderes às instâncias locais.



# Descentralização: Internet

- Internet: concebida para ser descentralizada!
  - Motivação: **resiliência**, até contra uma guerra nuclear
- Projeto inclui como características:
  - **Nenhum ponto central** de controle.
  - Comutação de **pacotes**: pequenos pedaços de dados **podem seguir por caminhos diferentes** (e.g., BGP)
  - Queda de um nó **não implica em parada total** da rede.
  - Interoperabilidade, mesmo entre **dispositivos heterogêneos**
- Primórdios: discagem direta (**dial-up**)
  - Conectar ao servidor = ligar para o número correspondente
    - Bastava a rede telefônica, sem a necessidade de um provedor de Internet (*Internet Service Provider* – ISP)
  - O som da Internet: 

# Des-Descentralização da Internet

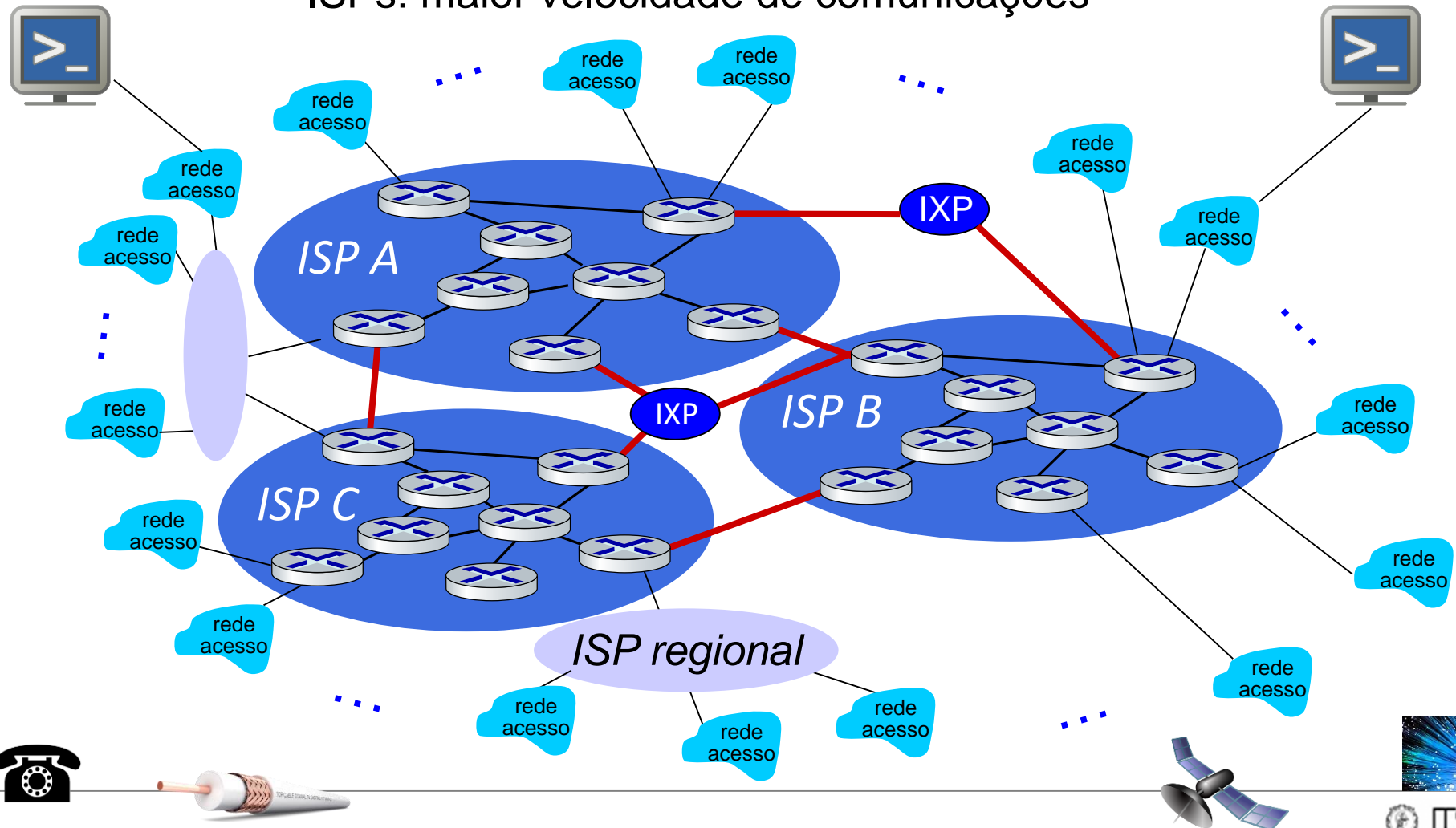
Internet: primórdios



# Des-Descentralização da Internet

Internet: hoje

ISPs: maior velocidade de comunicações



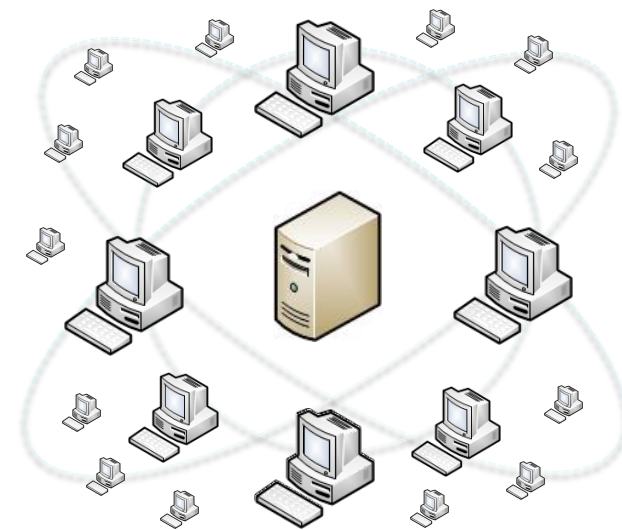
# Internet: Serviços Centralizados

- Arquitetura principal: **cliente-servidor**
- **Cliente:**
  - Inicia comunicação com servidor (“fala primeiro”)
  - Tipicamente, solicita serviços a servidor e aguarda resposta.
  - Web: cliente implementado no browser; e-mail: leitor de correio
- **Servidor:**
  - Aguarda solicitações de clientes
  - Fornece os serviços solicitados aos clientes interessados
  - Ex.: servidor web envia a página Web solicitada; servidor de e-mail envia as mensagens, etc.



# Internet: Serviços Centralizados

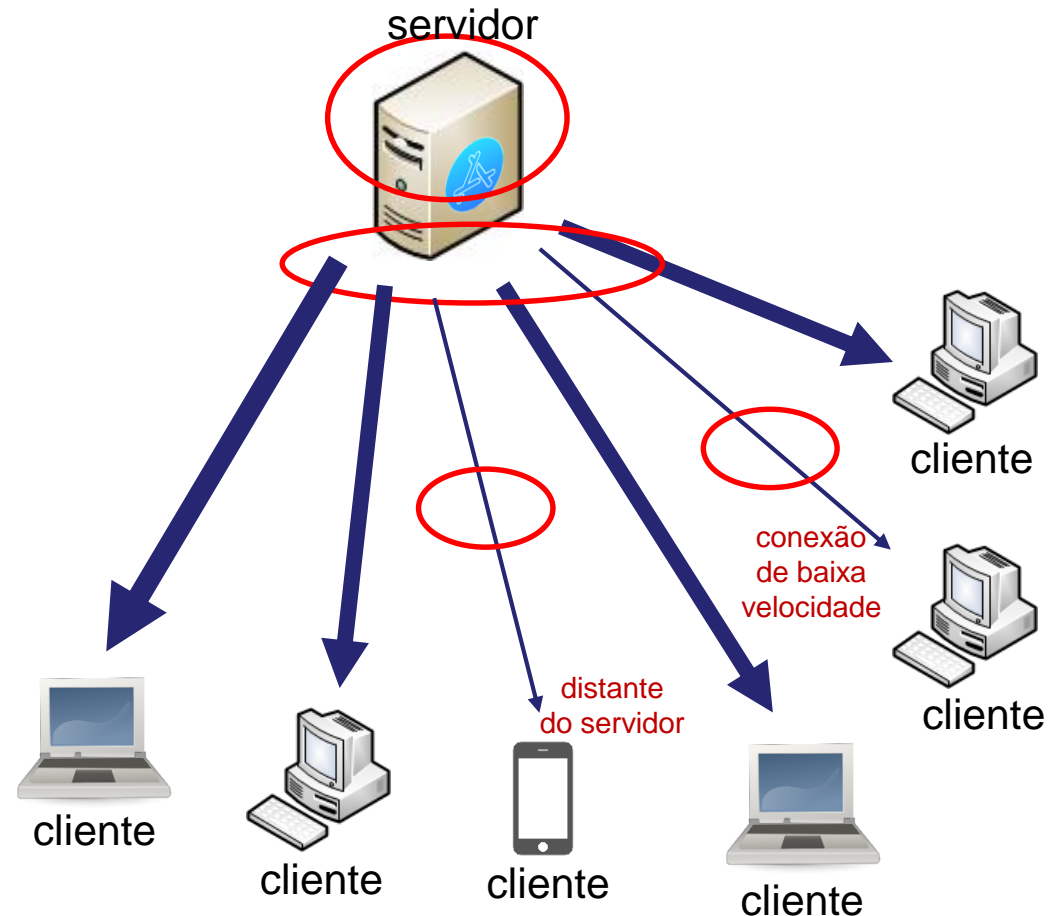
- **Acesso a informações e arquivos:** espalhados em vários sites...
  - Porém, busca por dados centralizada em gigantes como **Google**
- **Entretenimento:** gigantes de streaming, como **Youtube e Netflix**
- **Comunicação:** gigantes de redes sociais (**Twitter, Facebook, Instagram**) e apps de mensagem (**WhatsApp, Telegram**)
- **Operações financeiras:** bancos (Bradesco, Itau, BB, ...) e **operadoras de cartão** (Visa, Mastercard, Elo, ...)
- ...



**Problemas com centralização?**

# Serviços Centralizados: Gargalos

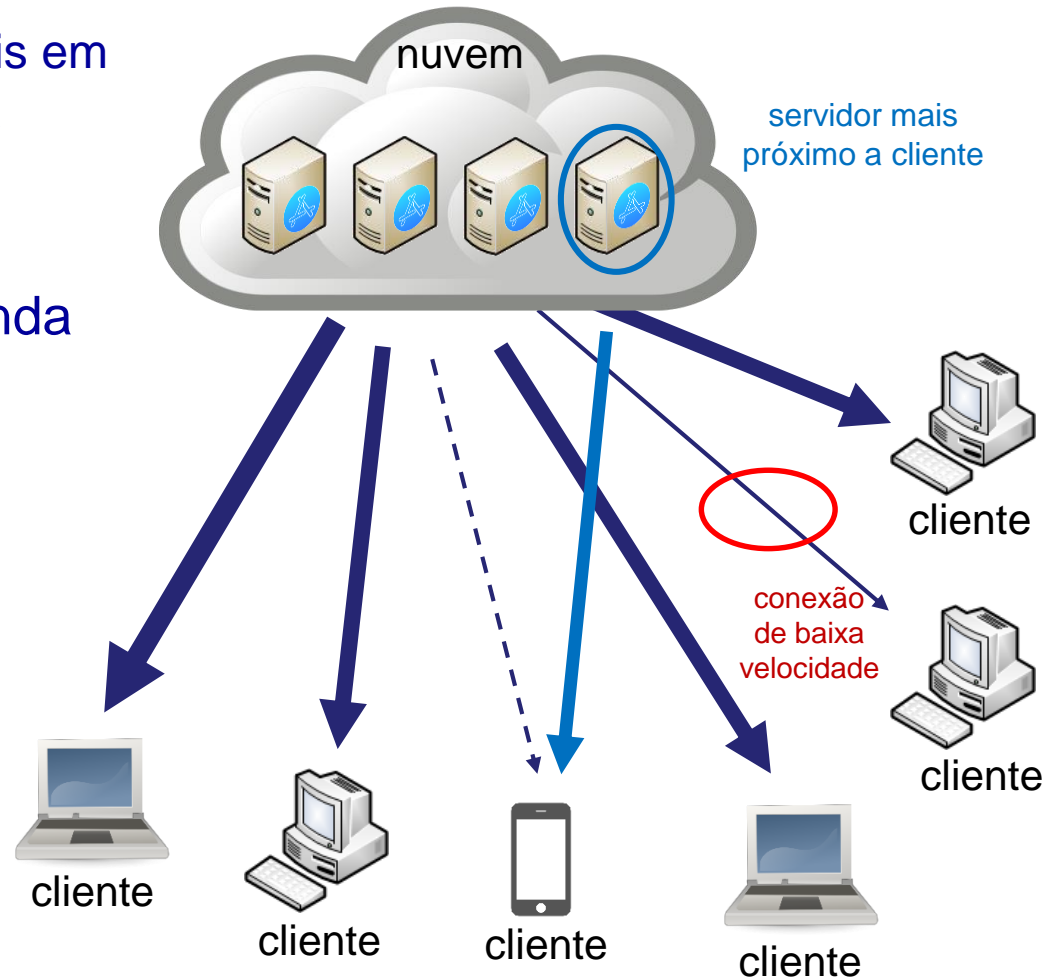
- Gargalos:
  - Servidor
  - Conexões do servidor
  - Conexões dos clientes
- Escalabilidade limitada
- Ponto único de falha
- Concentração de poder: controle sobre dados e regras do sistema





# Serviços Centralizados: Gargalos

- **Nuvem:** implantação distribuída
  - **Lógica:** máquinas virtuais em balanceamento de carga
  - **Física:** datacenters em diferentes localidades
- Escalabilidade sob demanda
  - Custos do provedor
- Maior resiliência a falhas
  - Relegada a provedor
- **Concentração de poder:** provedor do serviço e da nuvem
  - controle sobre dados e regras do sistema



# Serviços Centralizados: Gargalos

- Arquitetura cliente-servidor: cara de criar e manter
  - Custo estimado de centro de dados Google em Dalles: \$1.2bi <sup>1</sup>
  - \$7 bi anunciados em 2021 para construção de novos centros de dados <sup>2</sup>
  - Cada centro usa de 50 a 100 MW de potência <sup>3</sup>



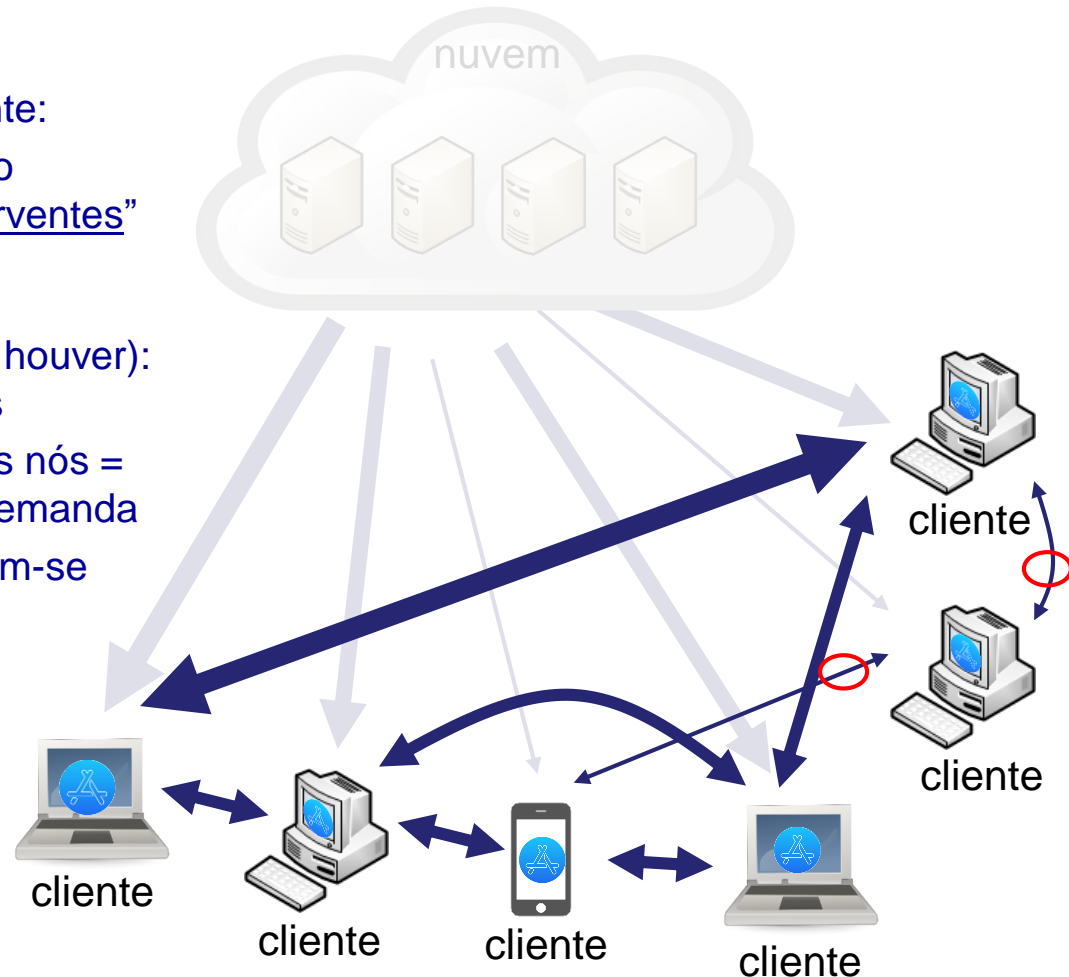
1. "Google Data Center FAQ, Part 2" - <https://www.datacenterknowledge.com/google-data-center-faq-part-2>

2. "Google outlines \$7B U.S. data center, office investment" <https://www.fiercetelecom.com/telecom/google-outlines-7b-u-s-data-center-office-investment>

3. "Baxtel - Google Locations" <https://baxtel.com/data-centers/google>

# Serviços Descentralizados

- Alternativa mais colaborativa (*peer-to-peer*, P2P):
  - Nós se comunicam diretamente:
  - Atuam simultaneamente como servidores e clientes: são “serventes”
- Benefícios:
  - **Alivia carga no servidor** (se houver): explora conexões alternativas
  - **Escalável por natureza**: mais nós = mais recursos, não só mais demanda
  - **Resiliência inerente**: eliminam-se pontos centrais de falha
  - **Custos** de operação distribuídos entre nós
  - **Controle distribuído**: os usuários são o sistema
  - Em alguns casos, maior **privacidade**



# Serviços Descentralizados: Desafios

- P2P: diversos atrativos, mas nem tudo são flores...



- **Desafios de administração**

- **Entrada e saída** dos nós dinamicamente
  - Solução: **redundância**; detecção & recuperação
- Difícil garantir **qualidade de serviço**
  - Solução: **incentivo** para colaboração
- **Heterogeneidade** dos nós:
  - Solução: **middlewares** para abstração; padrões **abertos**
- Acesso **concorrente**, sem relógio global: possíveis **conflitos**
  - Solução: **consistência eventual**; mecanismos de **consenso**
- **Baixa confiança** nos nós participantes
  - Solução: criptografia e protocolos de segurança
- **Localização** de nós e **recursos** distribuídos na rede
  - Solução: mecanismos de busca distribuídos; broadcast de dados



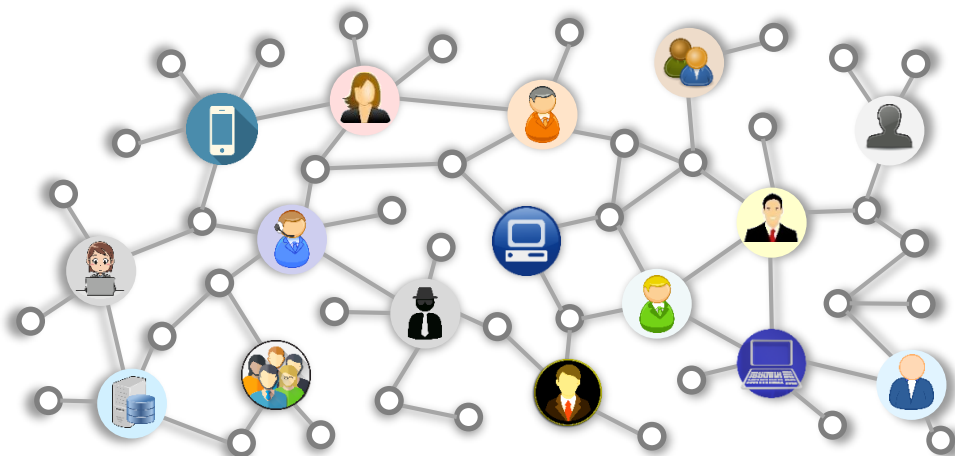
# Serviços descentralizados: novidade?

- Popularização de blockchains elevou interesse em iniciativas de “descentralização”
  - “DApp”: decentralized application
- Porém, vários “DApps” notórios surgiram bem antes (e não dependem de) blockchains
  -  **napster** (1999): compartilhamento de músicas
  -  **SETI@HOME** (1999): busca de vida extraterrestre
  -  **BitTorrent** (2001): compartilhamento de arquivos
- No final, tecnologias P2P retornam Internet a sua visão original: todos criam e consomem conteúdo
  - E um toque de “anarquia”: colaboração direta, liberdade, resistência a censura, robustez, confiabilidade, ...



# Conteúdo da disciplina

- Foco: tecnologias descentralizadas
  - Incluindo, mas indo além dos blockchains!
- Estrutura
  1. Princípios básicos: serviços descentralizados e sistemas P2P
  2. Fundamentos de segurança e criptografia: “Você precisa entender cripto (como em “-grafia”) para entender cripto (como em “-moedas”)”
  3. Blockchain sem o hype: “O que (não) é um Blockchain?”
    - Funcionamento de blockchains
    - Tecnologias correlatas: e.g., logs transparentes
  4. Se Blockchain não serve para descentralizar tudo, então o que serve?
    - Diversos: Tor, DHT, Gossip, Bittorrent, OAuth/OIDC, IPFS, ...



# Blockchain, Criptomoedas & Tecnologias Descentralizadas

## Introdução

Prof. Dr. Marcos A. Simplicio Jr. – [mjunior@larc.usp.br](mailto:mjunior@larc.usp.br)  
Escola Politécnica, Universidade de São Paulo

# Referências

- A Top-Down Approach, 8th ed., J. Kurose, K. Ross, Pearson, 2020
- C. Metz. "What Do the H-Bomb and the Internet Have in Common? Paul Baran". Wired, 09.03.2012. URL: <https://www.wired.com/2012/09/what-do-the-h-bomb-and-the-internet-have-in-common-paul-baran/>
- T. Berners-Lee. "Tim Berners-Lee on the Web at 25: the past, present and future." Wired, 23.08.2014. URL: <https://www.wired.co.uk/article/tim-berners-lee>
- V. Tabora. "The Evolution of the Internet, From Decentralized to Centralized". Hackernoon, March 2018. URL: <https://hackernoon.com/the-evolution-of-the-internet-from-decentralized-to-centralized-3e2fa65898f5>