Blockchain, Criptomoedas & Tecnologias Descentralizadas

Tecnologias descentralizadas:

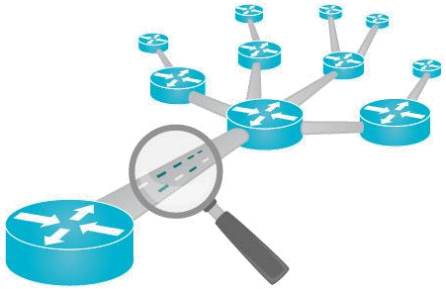
Tor e Privacidade

Prof. Dr. Marcos A. Simplicio Jr. – mjunior@larc.usp.br
Escola Politécnica, Universidade de São Paulo

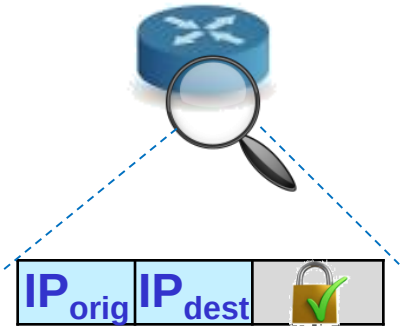
Objetivo:

Pergunta: existe anonimato na Internet?

Roteamento na Internet

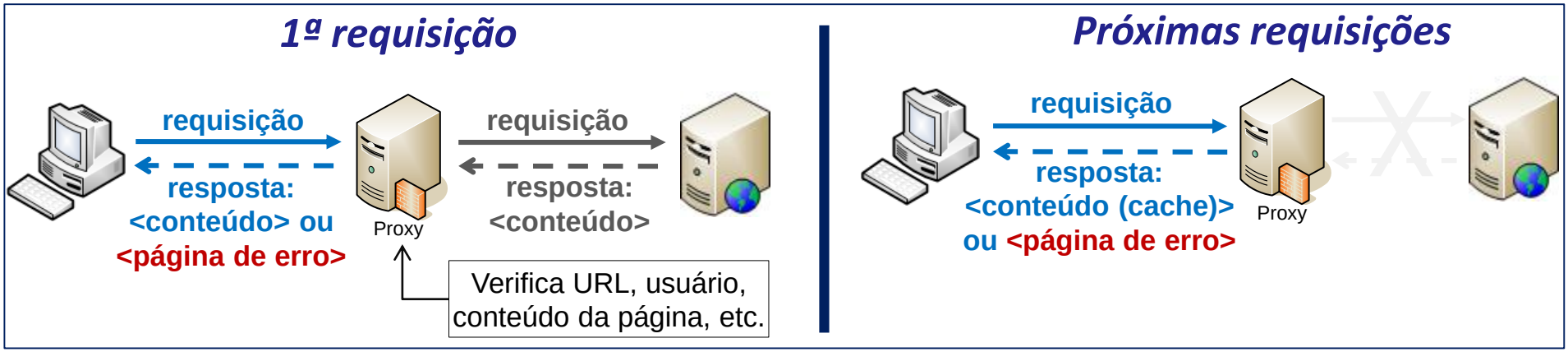


- Nenhuma medida de segurança
  - Tráfego não é cifrado ou autenticado
  - Além da origem e do destino, todos os roteadores intermediários têm acesso ao tráfego
- Solução simples: **s**egurança nas camadas superiores
  - Ex.: HTTP**S**, TL**S**, **S**SH, **S**FTP/**S**CP, etc.
  - Dão confidencialidade, mas não **privacidade**: roteadores intermediários (talvez desonestos) ainda sabem **quem são os nós comunicantes**
- Roteamento com privacidade?
  - "Como disfarçar a origem e o destino dos dados?"

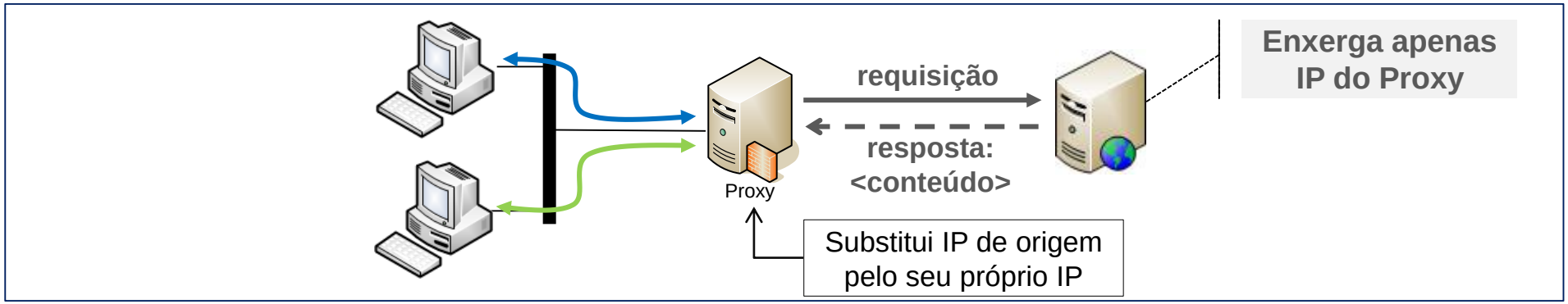


Proxies e privacidade

- Empresas costumam usar **proxies**
  - Objetivos: monitorar conteúdo; otimizar uso de banda



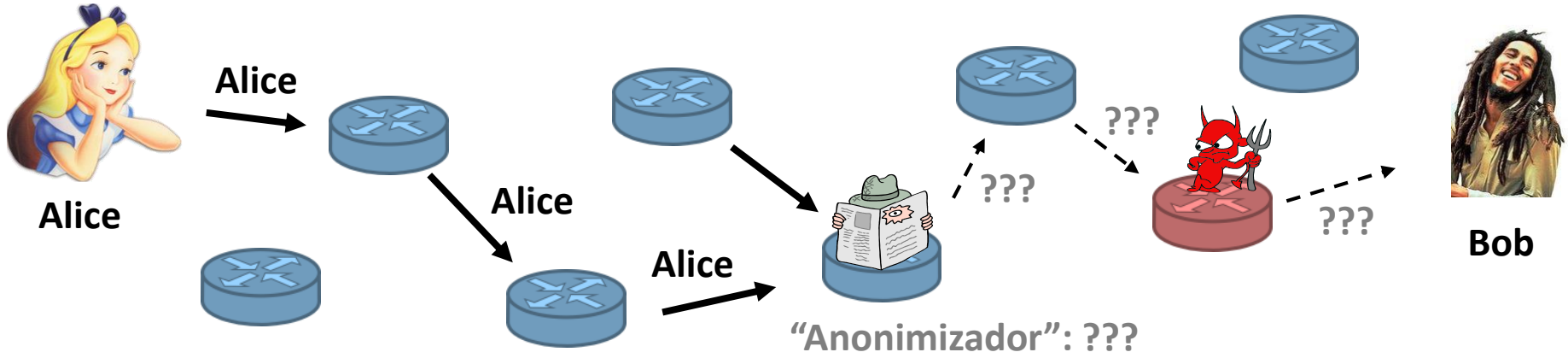
  - Mas também melhoram privacidade da navegação na Internet devido a NAT (Network Address Translation)



Proxies e privacidade

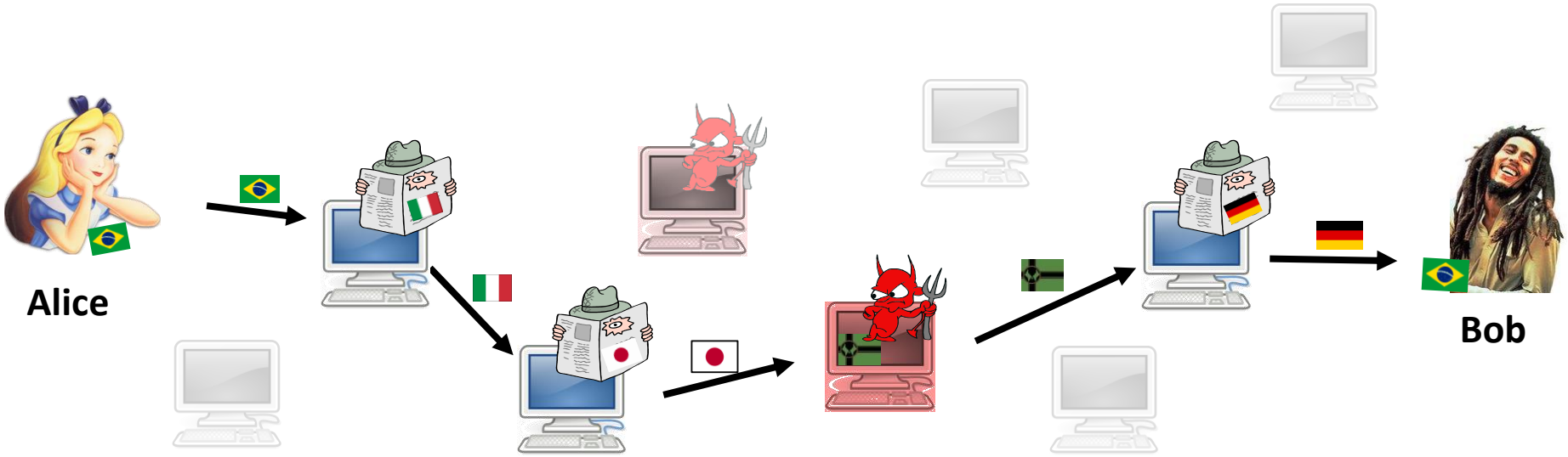
- Proxies web: fazem um serviço semelhante
  1. Proxy acessa página pedida, com IP do próprio Proxy
  2. Página acessada responde normalmente (preferências, como linguagem, são aquelas configuradas pelo Proxy)
  3. Proxy entrega resultado para usuário dentro de seu próprio site (conteúdo HTML do site gerado dinamicamente)
- Conexões normalmente são cifradas (TLS/VPN)
  - Podem também incluir recursos extras, como esteganografia
  - Exemplo: https://hide.me/en/proxy
- Vamos generalizar (e melhorar!) a ideia
  - Afinal, o Proxy pode registrar requisições, ou ser tirado do ar

Generalização: roteamento aleatorizado



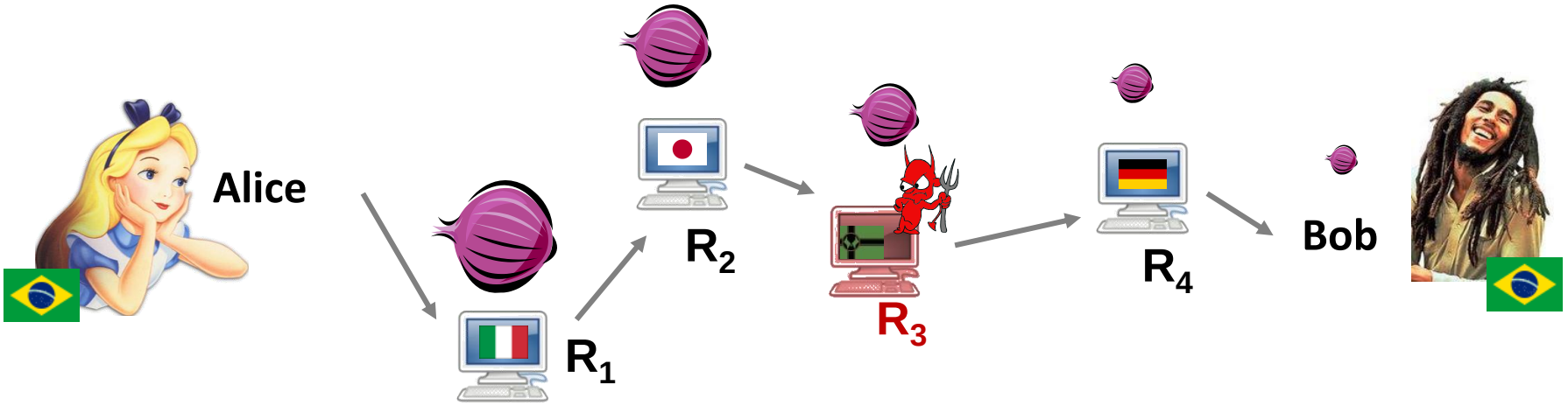
- Disfarça origem das mensagens fazendo roteamento aleatório
  - Técnicas populares: Crowds, Freenet, Onion routing
  - Roteadores não têm certeza se a origem aparente de uma mensagem é de fato seu originador ou outro roteador

Onion Routing

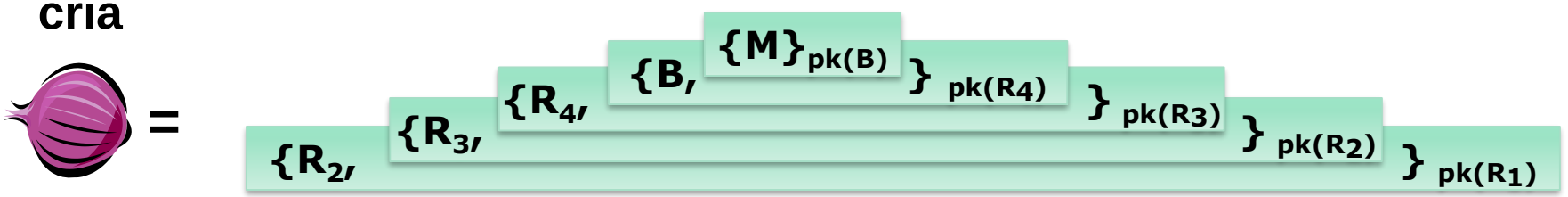


- Origem escolhe uma sequência aleatória de roteadores
  - Alguns roteadores são honestos, outros são controlados por atacantes
  - Origem decide a comprimento do caminho

Onion Routing



cria



Info de roteamento de cada link é cifrada com a chave pública (pk) do roteador

Cada roteador descobre apenas a identidade do próximo roteador

Apenas destinatário acessa mensagem M

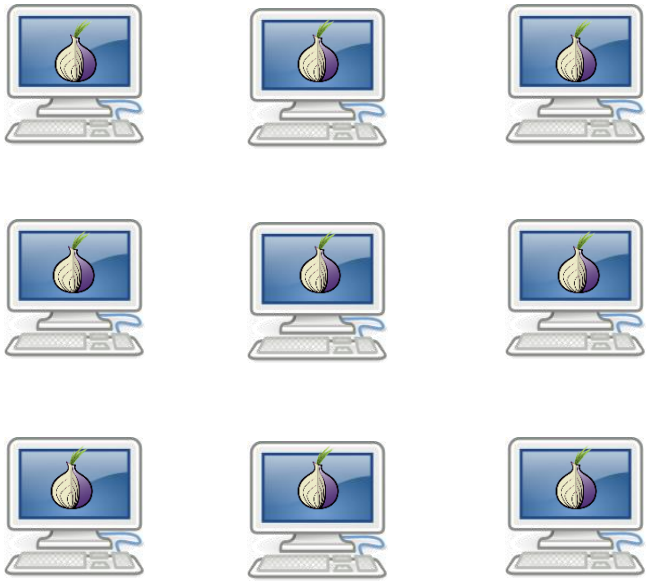
Tor

- Segunda geração do onion routing
  - http://tor.eff.org
  - Desenvolvido by Roger Dingledine, Nick Mathewson and Paul Syverson
  - Projetado especificamente para comunicações na Internet que requerem baixa latência
- Ativo desde Outubro de 2003
  - Diversos nós espalhados pelo mundo todo
  - Milhares de usuários
  - Clientes de "fácil uso" (plugins, Tor Browser)
  - Navegação anônima e gratuita

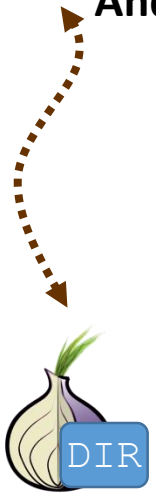
Tor: resumo

Não necessariamente cifrado
Cifrado pelo protocolo Tor

André

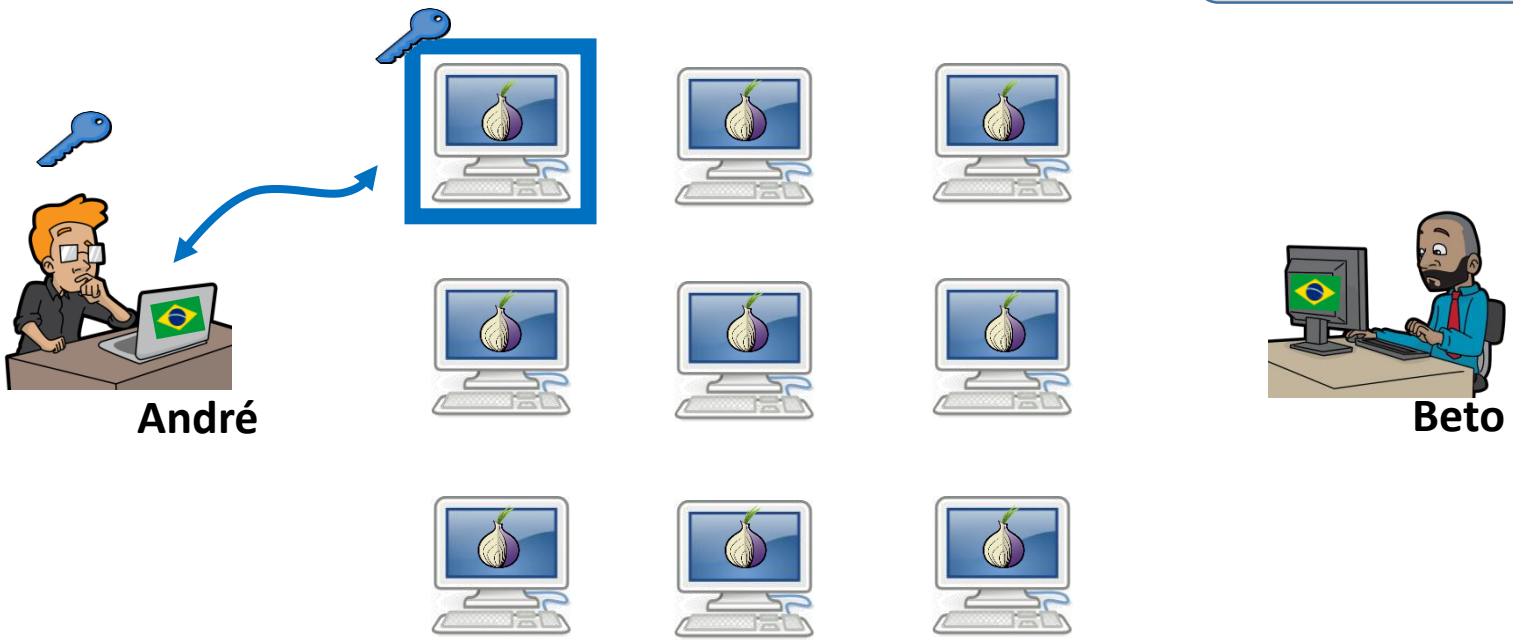


Beto



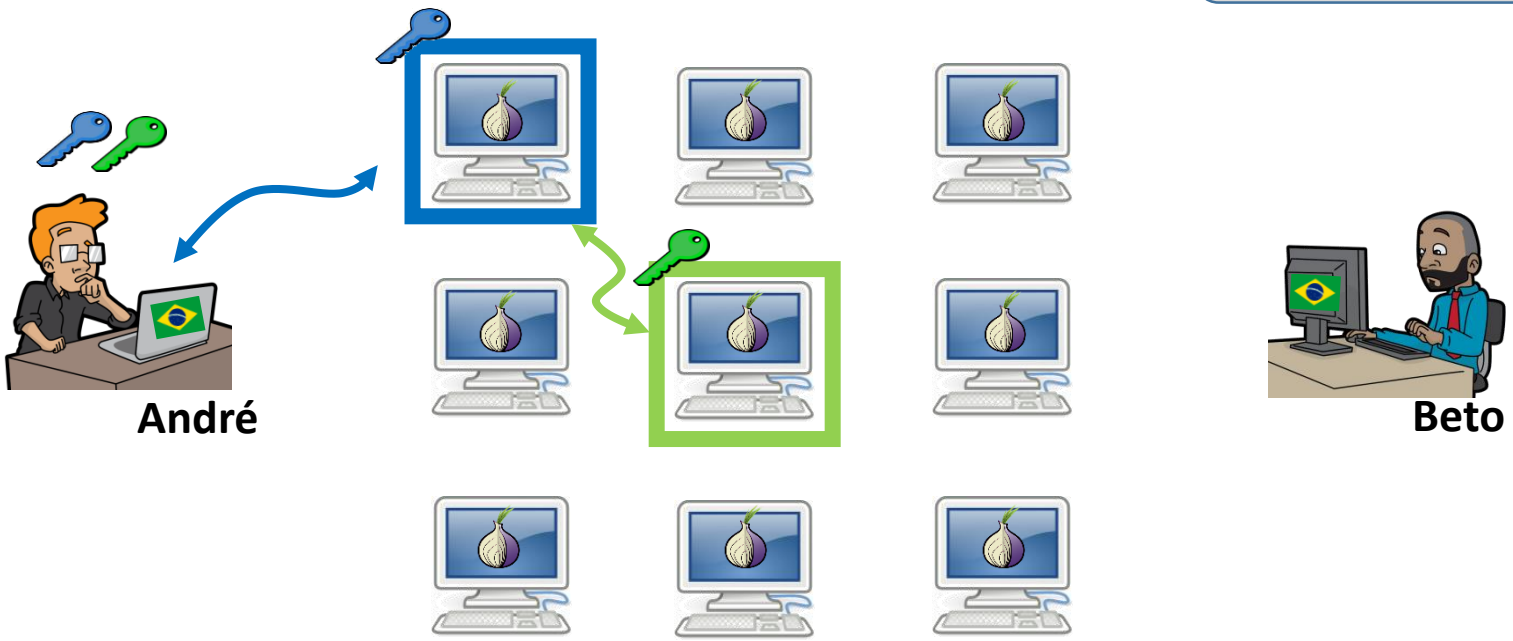
Passo 1: cliente Tor obtém lista de nós Tor em servidor de diretórios

Tor: resumo



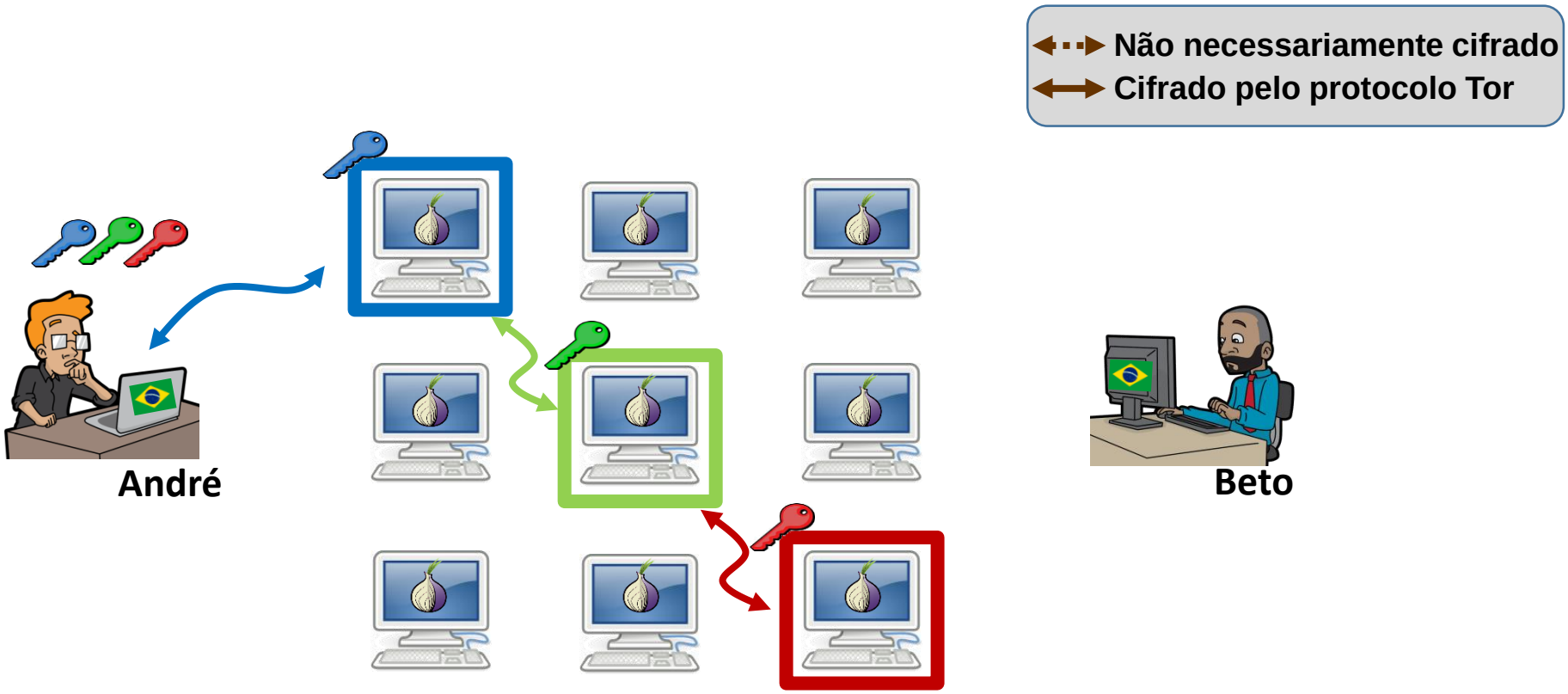
Passo 2: Chave simétrica de sessão com Onion Router #1: (circuito inicial)

Tor: resumo



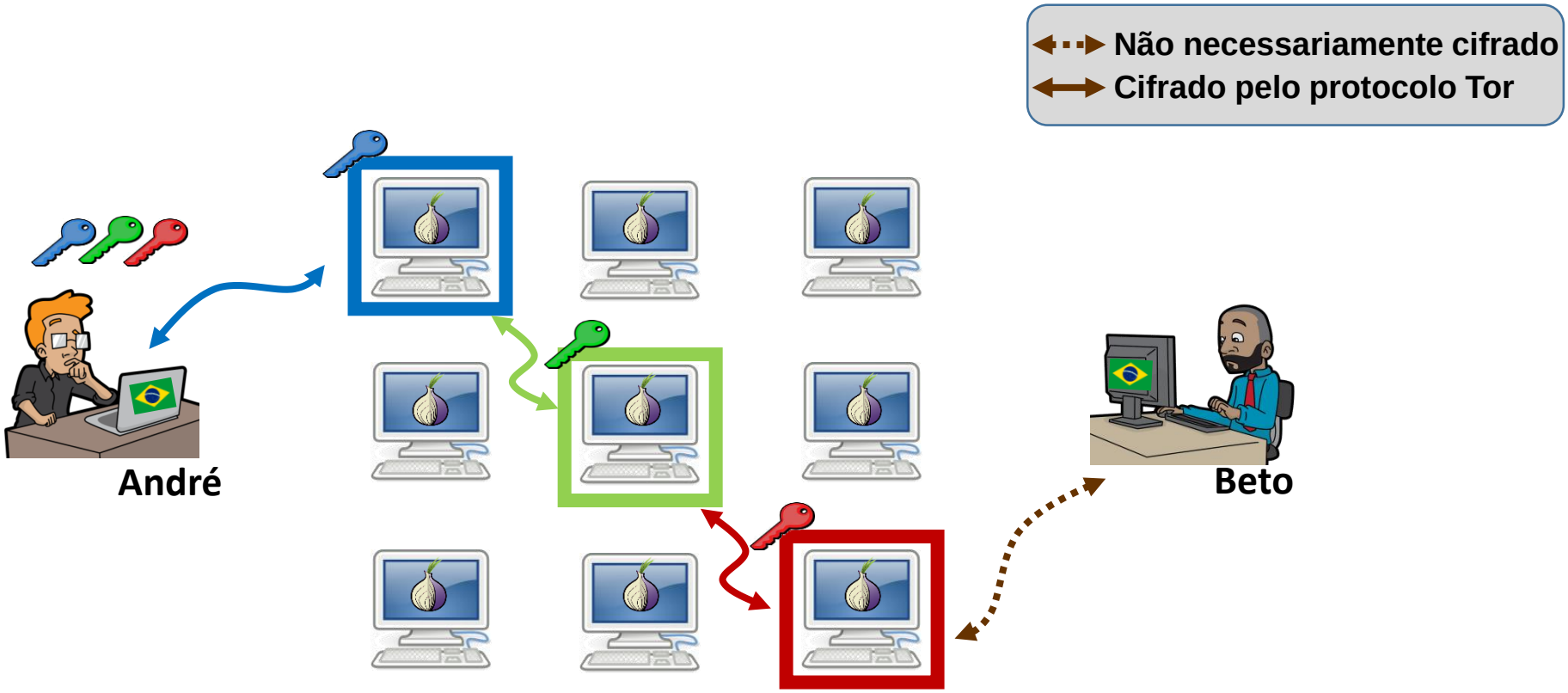
Passo 3: circuito estendido via nova chave simétrica de sessão com Onion Router #2 (tunelamento via router #1)

Tor: resumo

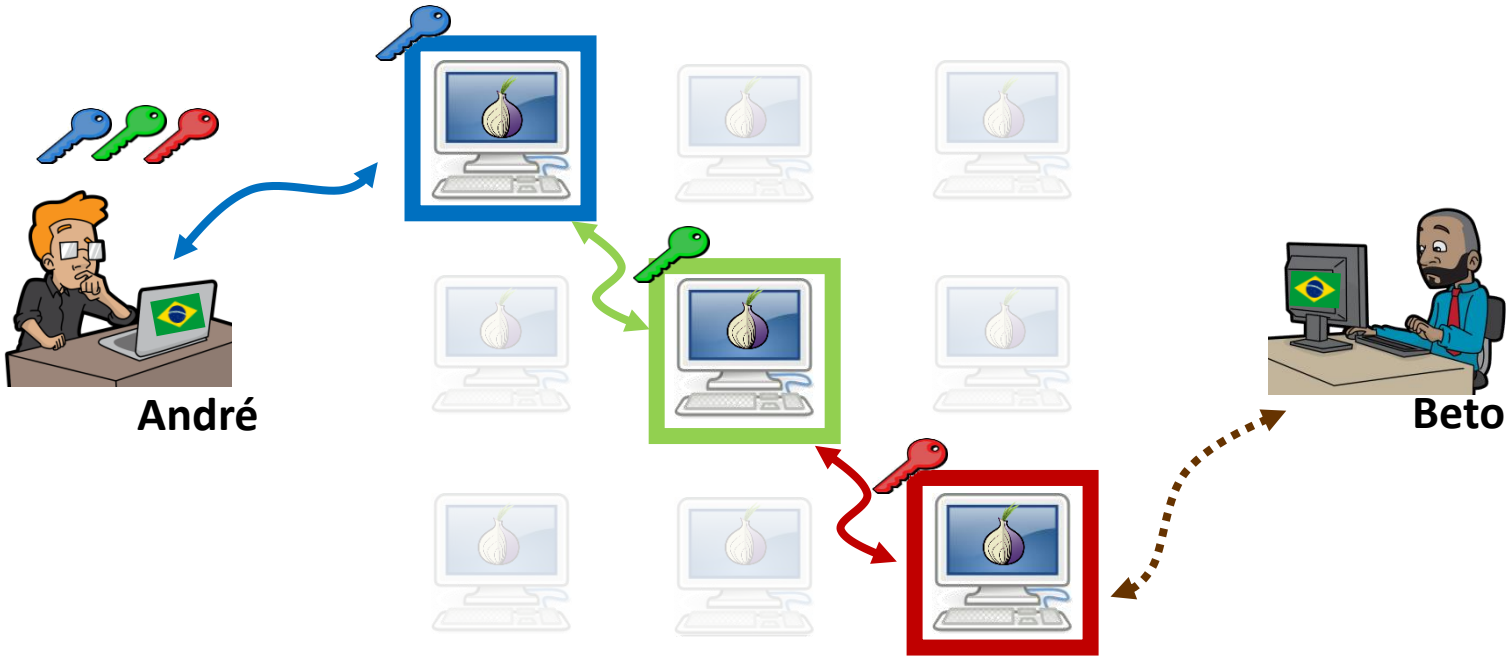


Passo 4: circuito estendido via nova chave simétrica de sessão com Onion Router #3 (tunelamento via router #1 e #2)

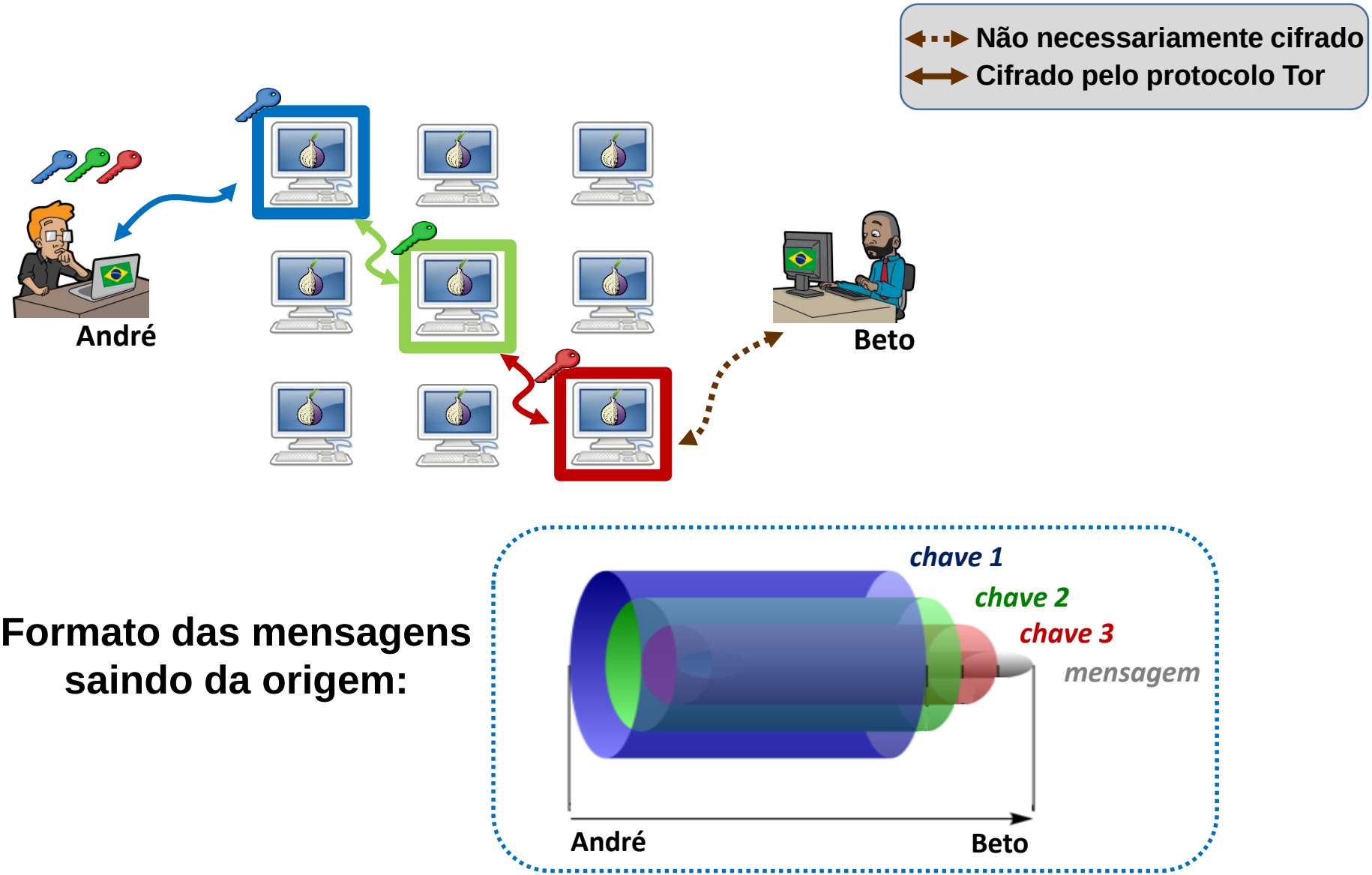
Tor: resumo



Passo 5: Cliente acessa destino final via circuito estabelecido: destino vê apenas Onion Router #3

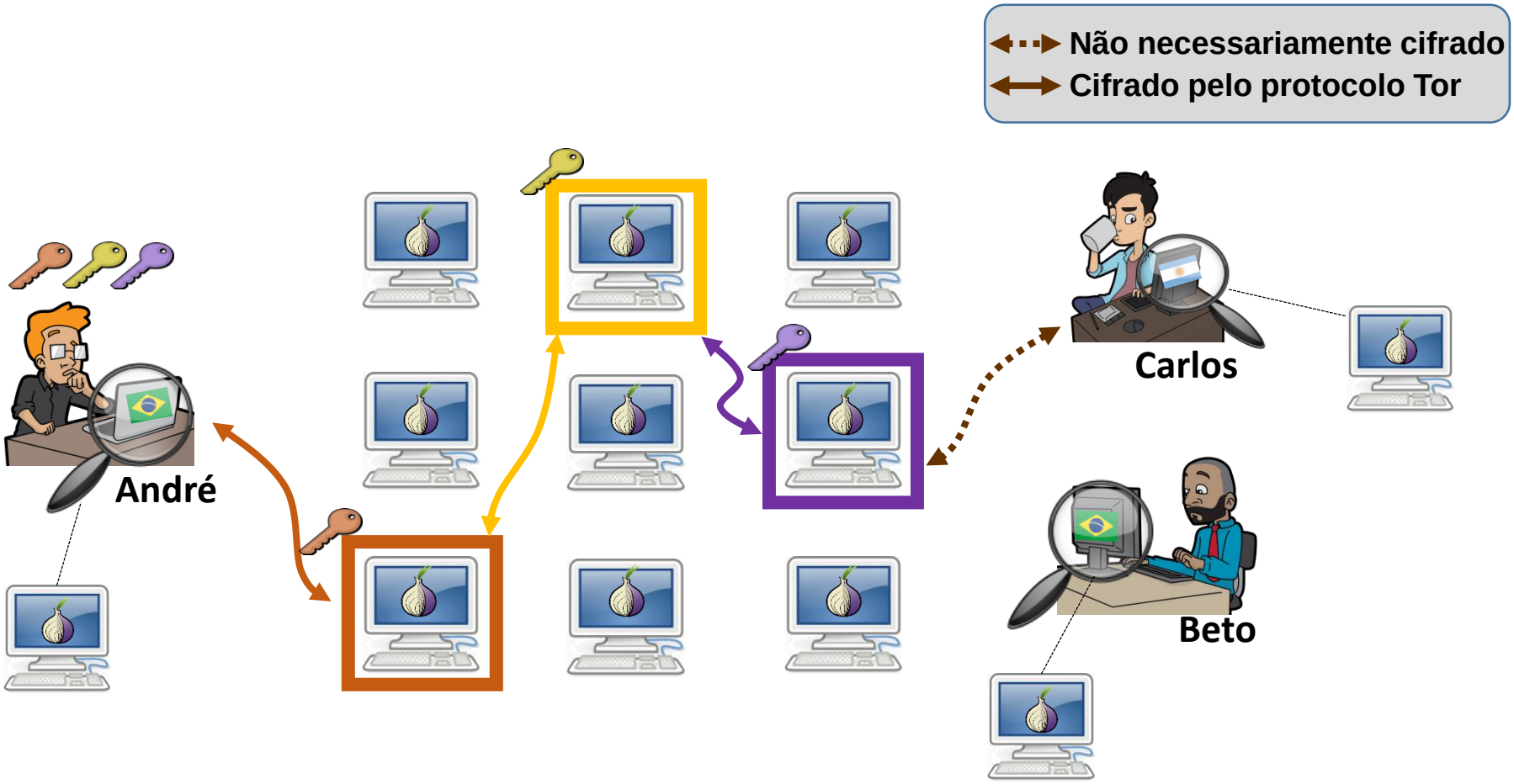

André
Beto

Tor: resumo



Formato das mensagens saindo da origem:

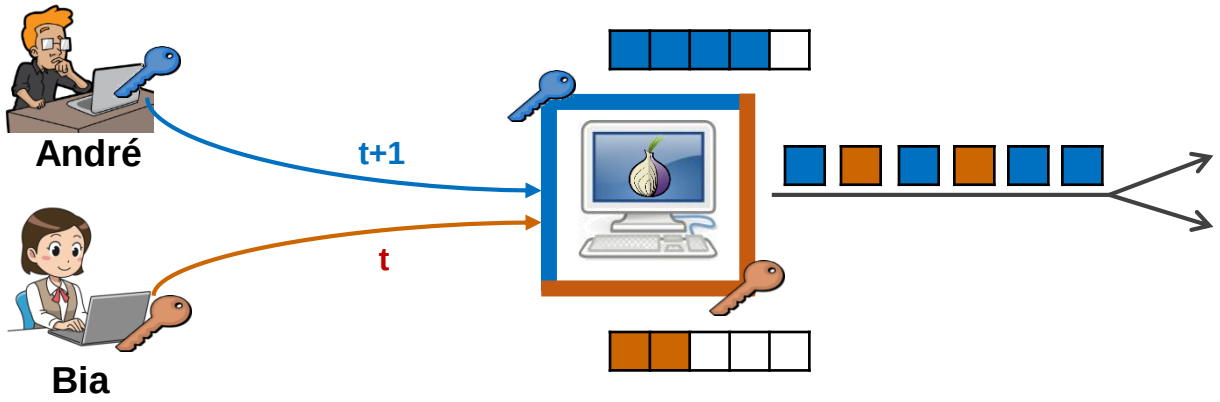
Tor: resumo



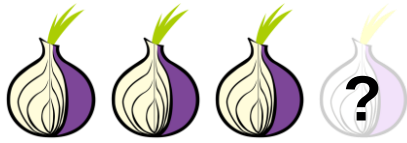
- Novo circuito pode ser estabelecido quando desejado
- Todos os usuários atuam como nós Tor

Tor: características

- **Comutação de células**: privacidade contra escuta
  - Pacotes trafegados têm 512 bytes (header:3, payload:509): previne identificação de fonte pelo **tamanho** das mensagens
  - Algum **embaralhamento interno** nos nós Tor evita deanonimização por **temporização**
    - Objetivo principal é "**equidade**", mas ajuda privacidade
    - Embaralhamento mais robusto **aumentaria latência**



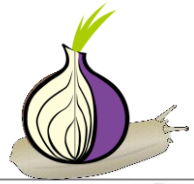
Por que 3 nós e não mais?



- Pergunta: ter mais nós aumenta segurança...?
- Cenário simplificado: 10% da rede comprometida:
  - Qual a chance de pelo menos 1 nó ser malicioso, e derrubar a conexão por não ter controle sobre outros nós relevantes (D)?
- 3 nós: $D = 1-(9/10)^3 = 27\%$
- 4 nós: $D = 1-(9/10)^4 = 34\%$

➔ Mais nós facilita **negação de serviço** por nó malicioso que acredita não conseguir monitorar comunicação...

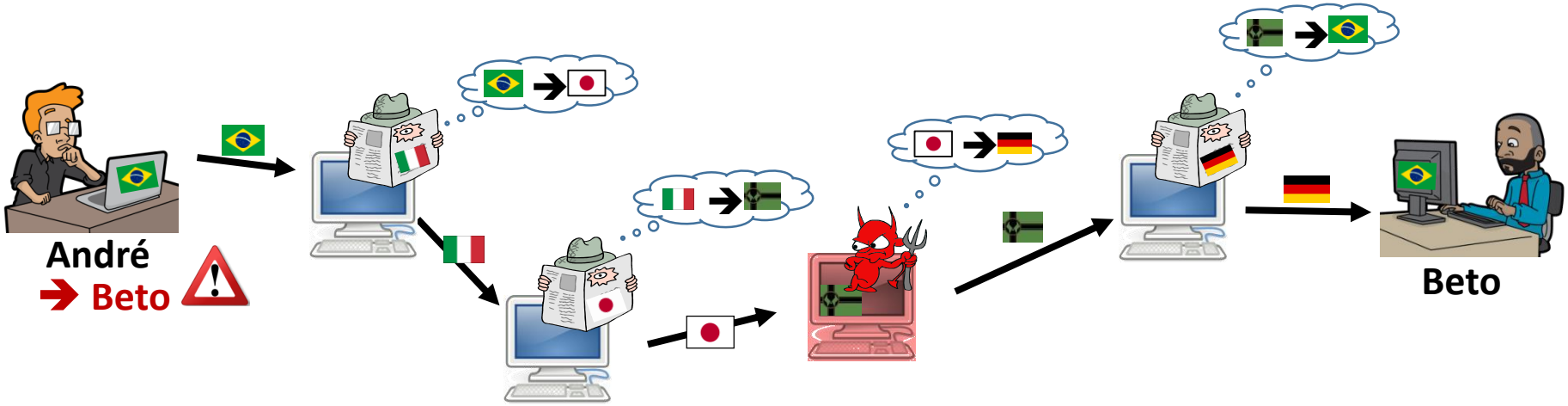
➔ Mais nós também **reduz desempenho** (latência e possibilidade de queda de algum link da conexão)



Tor: características

- "Perfect Forward secrecy"
  - No onion routing, um nó poderia gravar mensagens e depois comprometer a chave privada de todos os nós até o destino
  - No Tor, são criadas chaves de sessão, que são removidas após uso e, assim, não podem ser comprometidas
- Alguns serviços:
  - Diversos fluxos TCP podem **compartilhar** um mesmo circuito
  - Verificação de **integridade no ponto de saída** da rede
  - Nós confiáveis atuam como **servidores de diretório**: listas de roteadores conhecidos assinadas digitalmente
  - Pontos de encontro (rendezvous) e **serviços escondidos**: anonimato dos servidores

Servidores com localização oculta



- Mas e a proteção do IP dos servidores?
  - Origem enxerga IP dos destino!
    - Pode-se usar geolocalização: ataques físicos (ex.: captura)
    - Pode-se usar IP: ataques lógicos (ex.: negação de serviço)
  - Mecanismo extra do Tor: **serviços escondidos (.onion)**

Servidores com localização oculta

- Objetivo: servidor na Internet com as seguintes características:

  - **Disponibilidade**: acessível por qualquer pessoa de qualquer lugar,

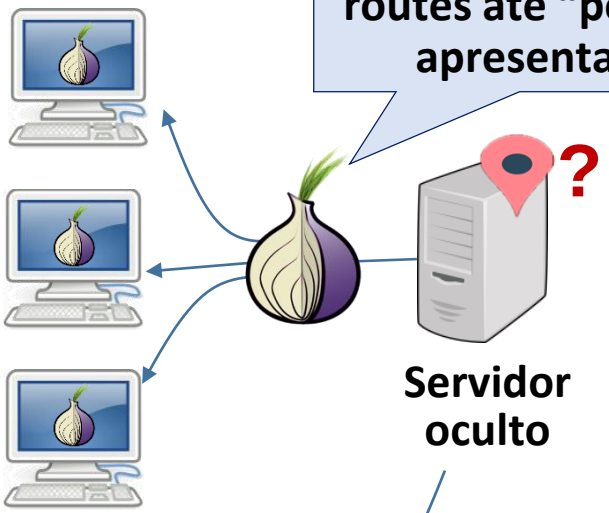
  - **Privacidade**: pessoas que acessam servidor não sabem onde ele está ou quem o controla

- **Resultado**: servidor resistente a censura

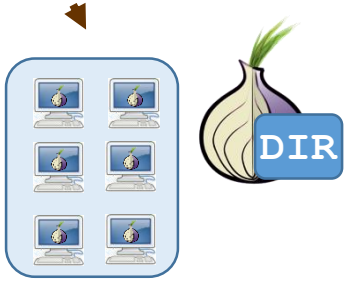
  - Capaz de resistir a ataques de negação de serviço: serviço distribuído, com acesso controlado
  - Resistente a captura física: não se sabe onde está o servidor físico!

Criando um servidores com localização oculta

1) Servidor cria onion routes até “pontos de apresentação”



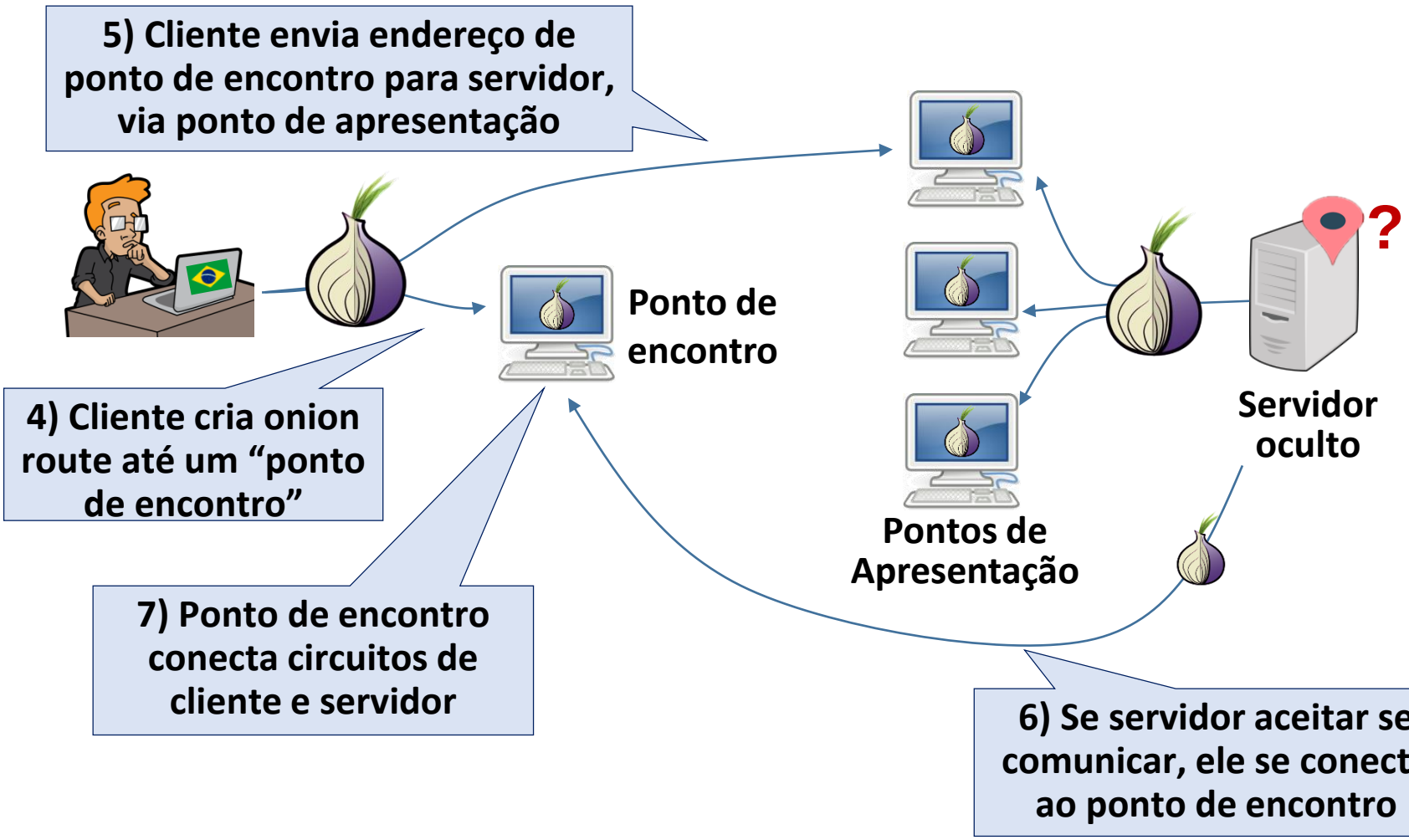
3)Cliente obtém descritor de serviço e endereço de ponto de apresentação



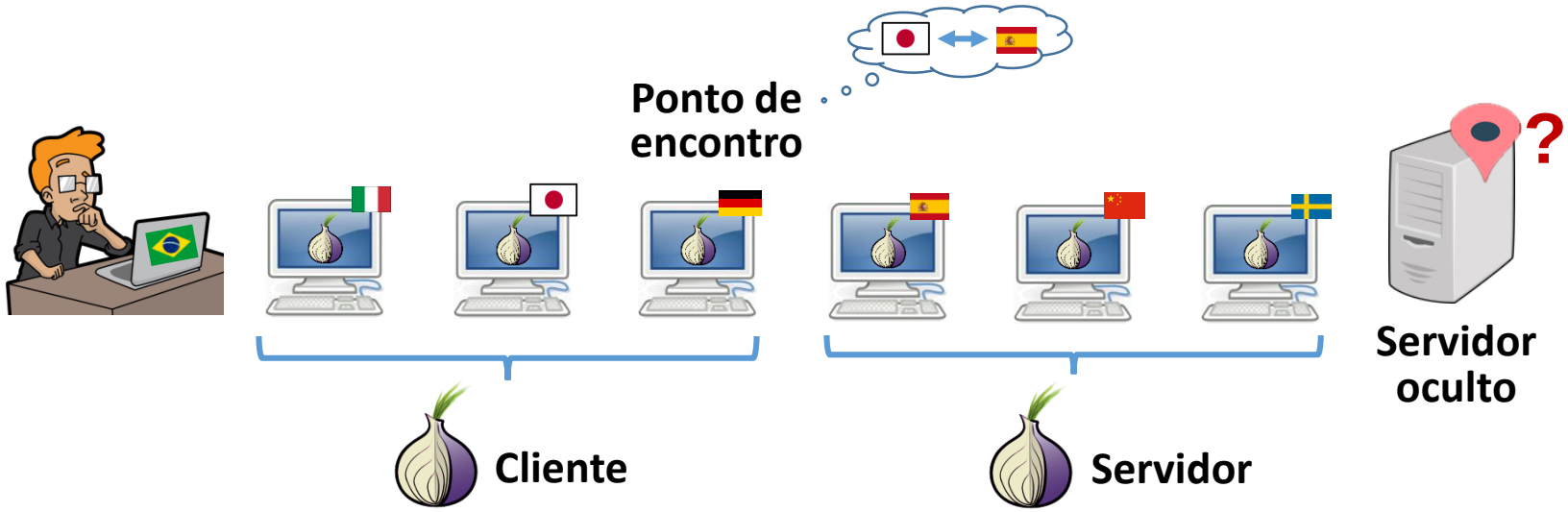
http://3g2upl4pq6kufc4m.onion/

2) Servidor fornece sua descrição e endereços de pontos de apresentação para serviço de diretório

Criando um servidores com localização oculta



Criando um servidores com localização oculta



- Resultado:
  - Servidor não enxerga IP de cliente
  - Cliente não enxerga IP de servidor
  - Nós intermediários não identificam quais são os pontos finais da comunicação

Ataques à rede Tor

- Ataques passivos
  - Não é tão difícil saber se um nó está executando protocolo Tor: o difícil é saber com quem ele está se comunicando
- Ataques ativos
  - DDoS, controle de um nó da rede Tor
- Ataques aos diretórios
  - Destruição ou subversão de servidores de diretório
- Pontos de encontro
  - Ataque a pontos de encontro ou pontos de apresentação

Tor = “Deep Web”?

"Especula-se que a Deep Web [Web profunda] é cerca de 400-500 vezes maior do que a Surface Web [web da superfície]".

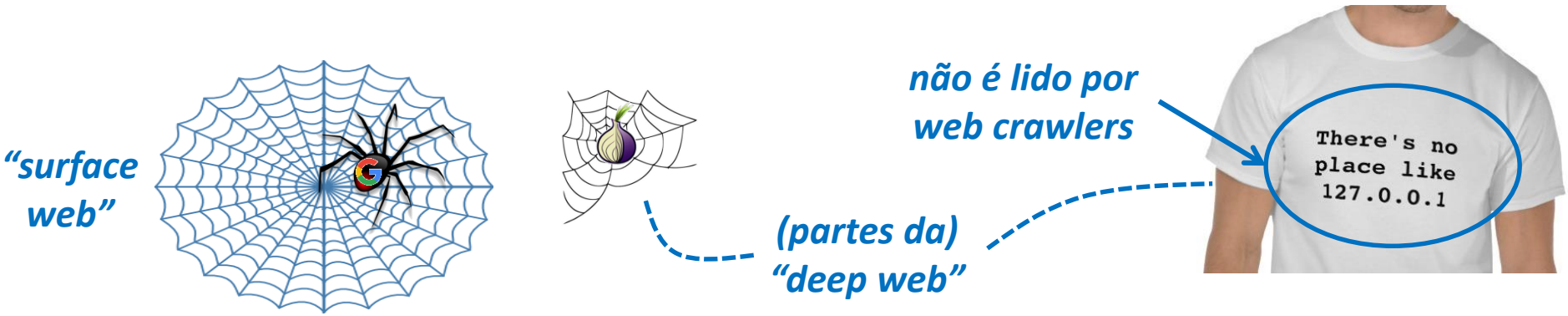
UC Berkley, 2001

Tor, Web e "Deep Web": Indexação

- **Web Crawling**: **indexação** automática de páginas Web
  - Usado, por exemplo, para construir a base de dados de **sites de busca**
- **Web crawlers** (ou Web spiders): programas de computador que **automatizam indexação**
  - Visitam páginas e indexam texto visível e metadados
  - Seguem hiperlinks encontrados, continuando "navegação" pela Web e descobrindo novos sites
  - Podem executar indefinidamente, identificando modificações em páginas já visitadas.

Tor, Web e "Deep Web": Indexação

- "Deep web": conteúdo web não indexado por máquinas de busca tradicionais
  - Conteúdo **gerado dinamicamente** (ex.: via Javascript)
  - Conteúdo para o qual **não existem links** em sites já indexados
  - Conteúdo em **sites privados ou de acesso restrito**
    - Exigem login ou acesso via canal específico (ex.: redes Tor ou Freenet)
  - Texto embutido em **arquivos multimídia**

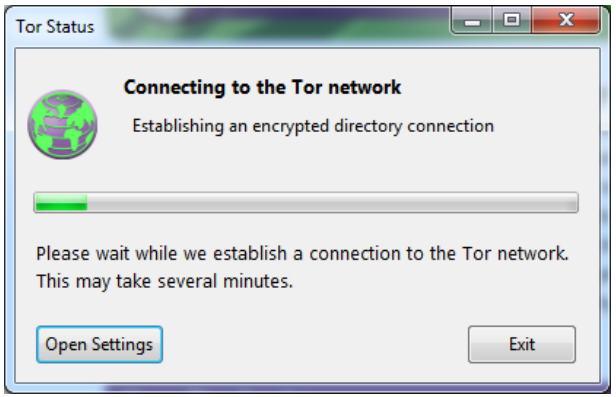


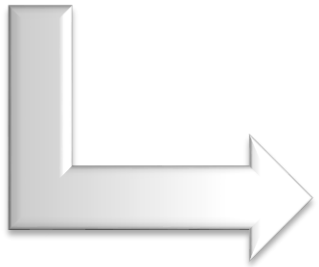
Tor, Web e "Deep Web": Indexação

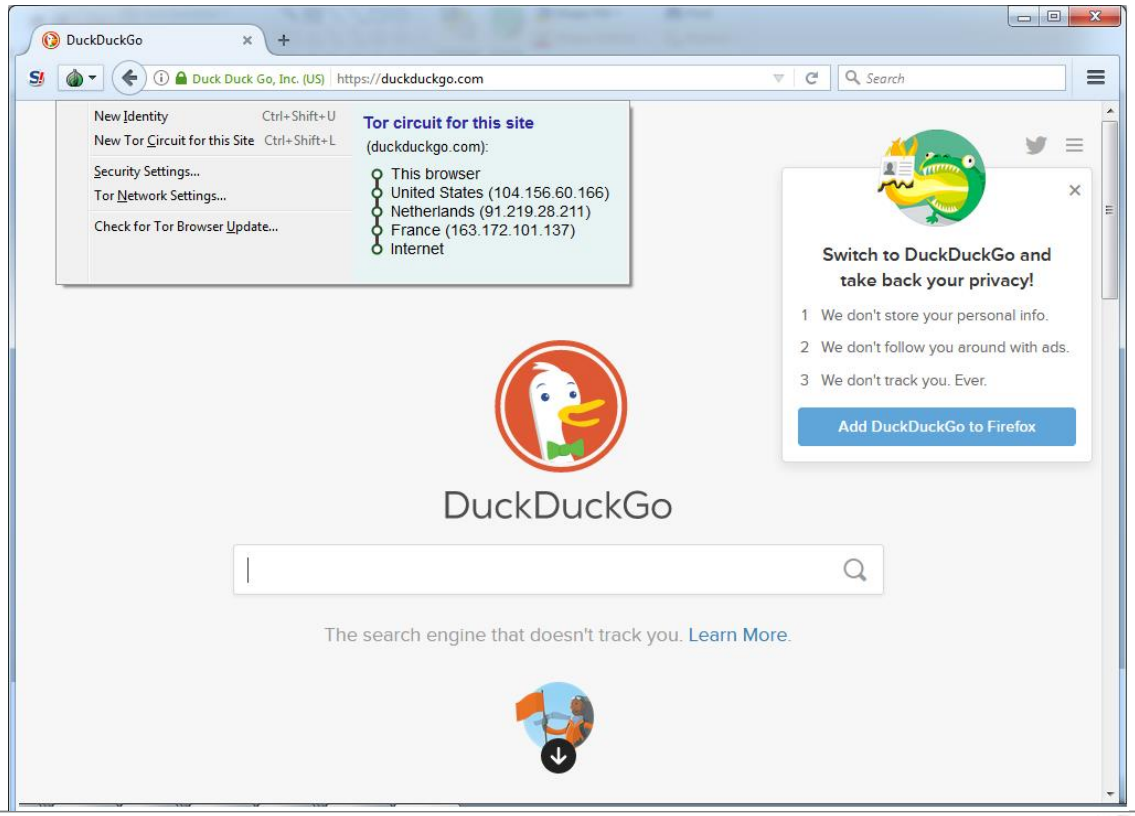
Termo às vezes usado (de modo simplista) como "conteúdo ilegal"

Tor Browser: teste você mesm@!

- Página oficial: https://www.torproject.org/
  - Ex. de "hidden wiki": https://thehiddenwiki.org/
  - http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page







Blockchain, Criptomoedas & Tecnologias Descentralizadas

Tecnologias descentralizadas:
Tor e Privacidade

Prof. Dr. Marcos A. Simplicio Jr. – mjunior@larc.usp.br
Escola Politécnica, Universidade de São Paulo

Apoio financeiro: d24n.org <https://d24n.org>
ripple impact | university blockchain research initiative