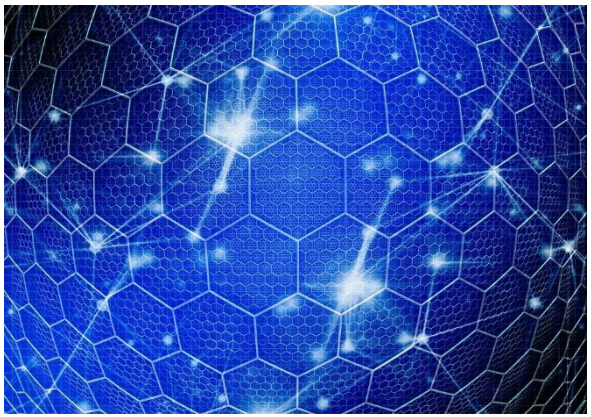


Blockchain, Criptomoedas & Tecnologias Descentralizadas

Blockchain sem o hype:

Aplicações

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

Objetivos

- Responder à questão: “Quando usar um Blockchain?”
- Discutir aplicações potenciais de blockchain
  - Sem qualquer pretensão de ser exaustivo
  - Mostrar alguns exemplos de plataformas

Blockchain: quando usar?

- Lembrando o início deste módulo:
- **Blockchain**: mecanismo distribuído **muito** interessante
- Porém, cuidado com o hype: um blockchain "completo" é
  - **Muito útil** em um cenário: **ordenação de eventos** em sistema **totalmente distribuído** e **sem confiança** entre as partes, mas há **incentivo** para sua participação no sistema
    - Obs.: "Incentivo" nem sempre é essencial, mas costuma ser interessante -- por que usuários irão participar do processo de consenso e replicação de dados, essencial para o funcionamento de um "blockchain completo"? Interesse deve ser claro!
  - **Pouco (ou nada) interessante** quando no cenário alvo:
    - Há **entidades totalmente confiáveis** no sistema; ou
    - É **desnecessário ordenar** eventos (e.g., basta sua existência); ou
    - A ordem relativa de eventos não basta (e.g., requer **instantes exatos de tempo**)
    - Ataques envolvem **eventos que podem não ser registrados** no blockchain (e.g., atacante age no mundo real, sem benefício/exigência de divulgar ações)

Blockchain: quando usar?

- Blockchain substitui **ACT**, com abordagem distribuída
  - Logo: se uma solução para o problema for uma ACT, então Blockchain também é uma potencial solução
- Sugestão de procedimento:
  - Defina bem o seu **problema**
    - Ex.: “preciso de uma base ordenada de eventos para verificar se houve duplicação ou supressão de algum evento”
    - Identifique os **requisitos** que justificam um blockchain
  - Modele uma solução **usando ACT**:
    - Ex.: ACT pode assinar ID dos eventos com seu timestamp, e publicar resultados em banco de dados aberto -- todos os interessados podem replicar (parte do) banco
  - Substitua a ACT pelo **Blockchain**
    - Preferencialmente, defina **incentivo** para participação no consenso (“pelo bem do sistema” pode ou não ser suficiente)

Blockchain: aplicações potenciais

- **Transferência de ativos (virtuais)**: **killer app**
  - **Ordenação de eventos**: necessário para saber quem é o dono atual do ativo
    - Não são necessários **instantes exatos de tempo**: em geral, não importa se o ativo foi recebido há anos ou há segundos, mas apenas quem é o dono atual
  - Sistema **totalmente distribuído**: sem intermediários
    - Eliminar **entidade confiável** permite aumentar resistência a falhas e disponibilidade, além de potencialmente evitar taxas
  - **Sem confiança**: usuários podem tentar cometer fraudes
    - Consenso previne que a "visão de mundo" fraudulenta prevaleça: apenas uma instância do ativo no sistema
  - Ex.: moedas (**Bitcoin**, **Ethereum**, **Ripple XRP, Solana, ...**)
    - **Incentivo:** moedas e/ou "pelo bem da economia"

Blockchain: pagamentos

- Transferência de ativos: moedas
  - Cenário de aplicação plausível: necessidade de ACT para solucionar “gasto duplo”.
  - Vantagem: agilizar sistemas de pagamentos...

Transações internas a bancos já são simples...

Alice	Bob
500 → 400	-20 → 80

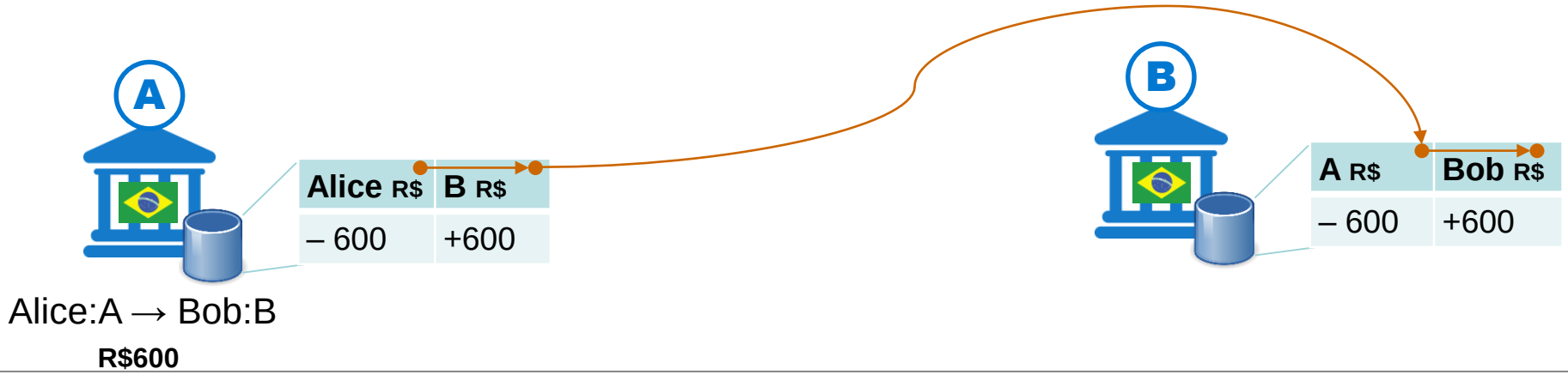
Alice → Bob

R$100

Blockchain: pagamentos

- Transferência de ativos: moedas
  - Vantagem: agilizar sistemas de pagamentos...

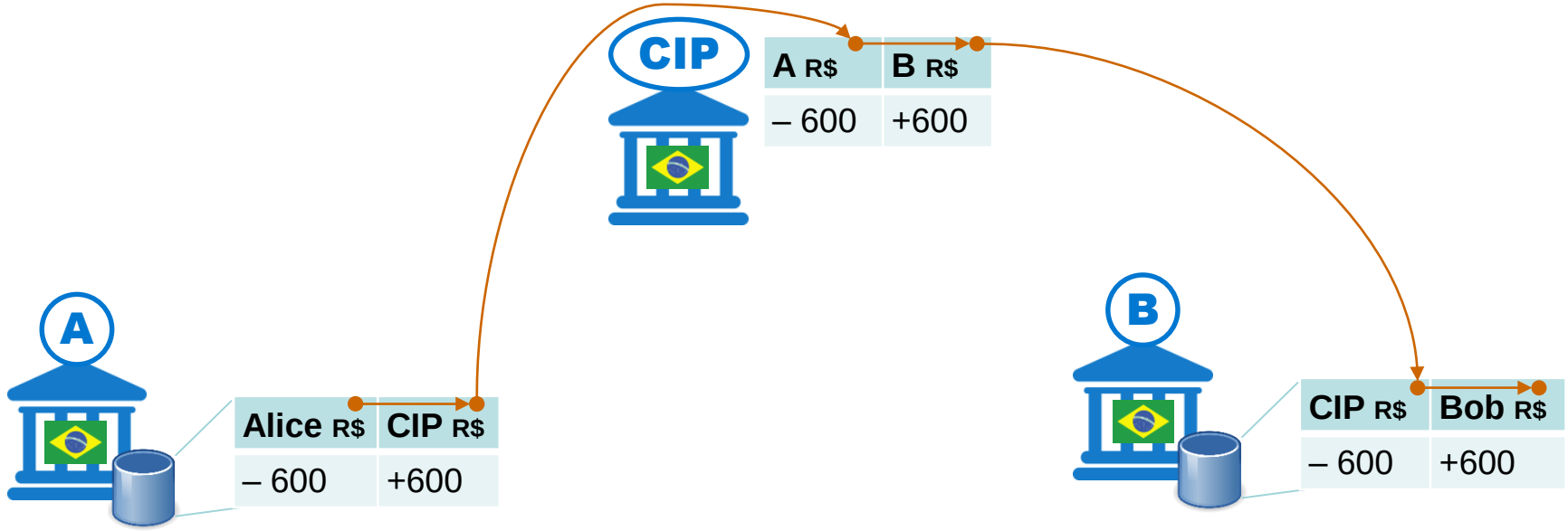
Já transações entre bancos não são tão simples...
➔ Banco A teria que manter liquidez em vários bancos...



Blockchain: pagamentos

- Transferência de ativos: moedas
  - Vantagem: agilizar sistemas de pagamentos...

Já transações entre bancos não são tão simples...
➔ Facilitador confiável: Câmara Interbancária de Pagamentos (CIP), auditado pelo Banco Central

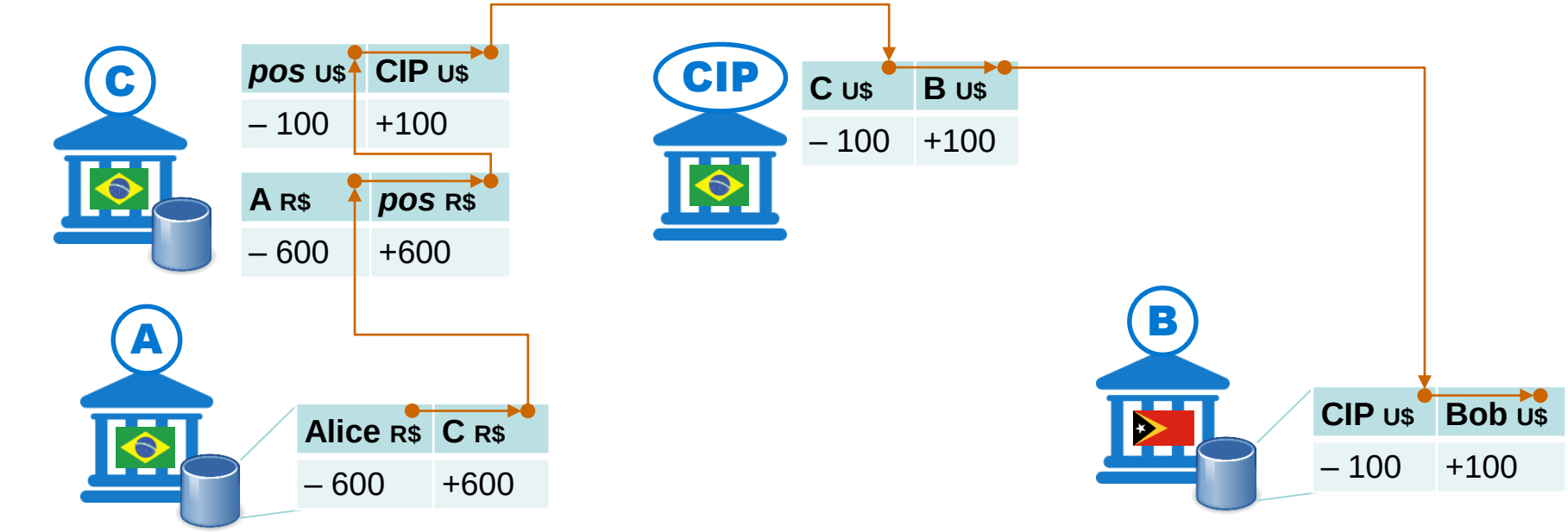


Alice:A → Bob:B
R$600

Blockchain: pagamentos

- Transferência de ativos: moedas
  - Vantagem: agilizar sistemas de pagamentos...

E transações internacionais são ainda pior



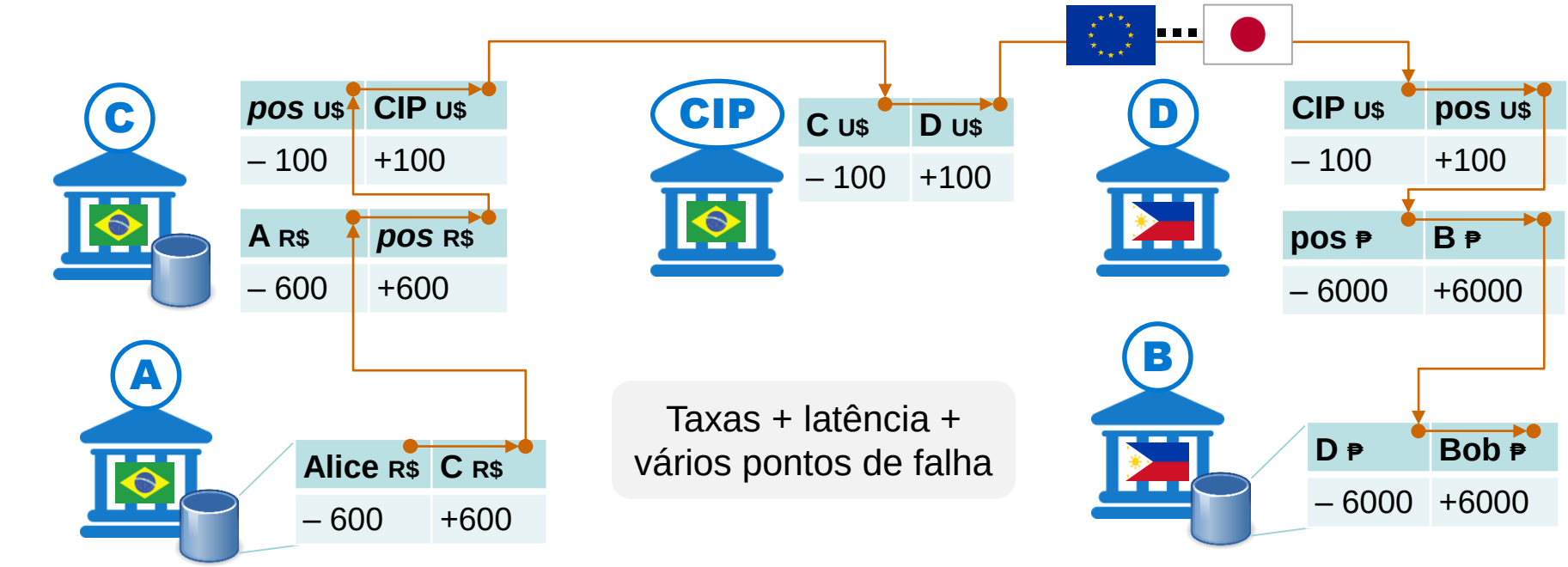
Alice:A → Bob:B

R$600

Blockchain: pagamentos

- Transferência de ativos: moedas
  - Vantagem: agilizar sistemas de pagamentos...

E podem piorar ainda ainda mais

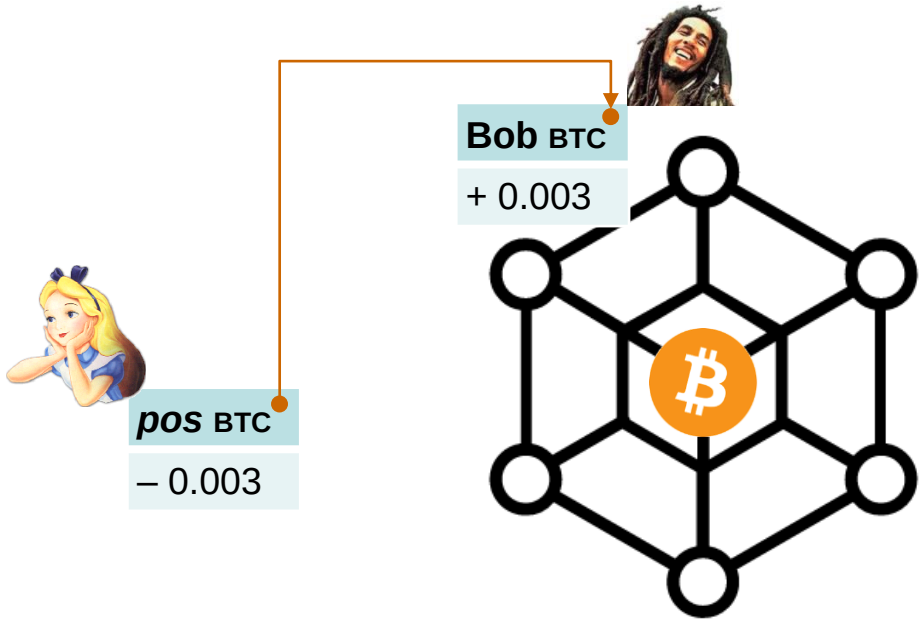


Alice:A → Bob:B

R$600

Blockchain: pagamentos

- Transferência de ativos: moedas
  - Vantagem: agilizar sistemas de pagamentos...



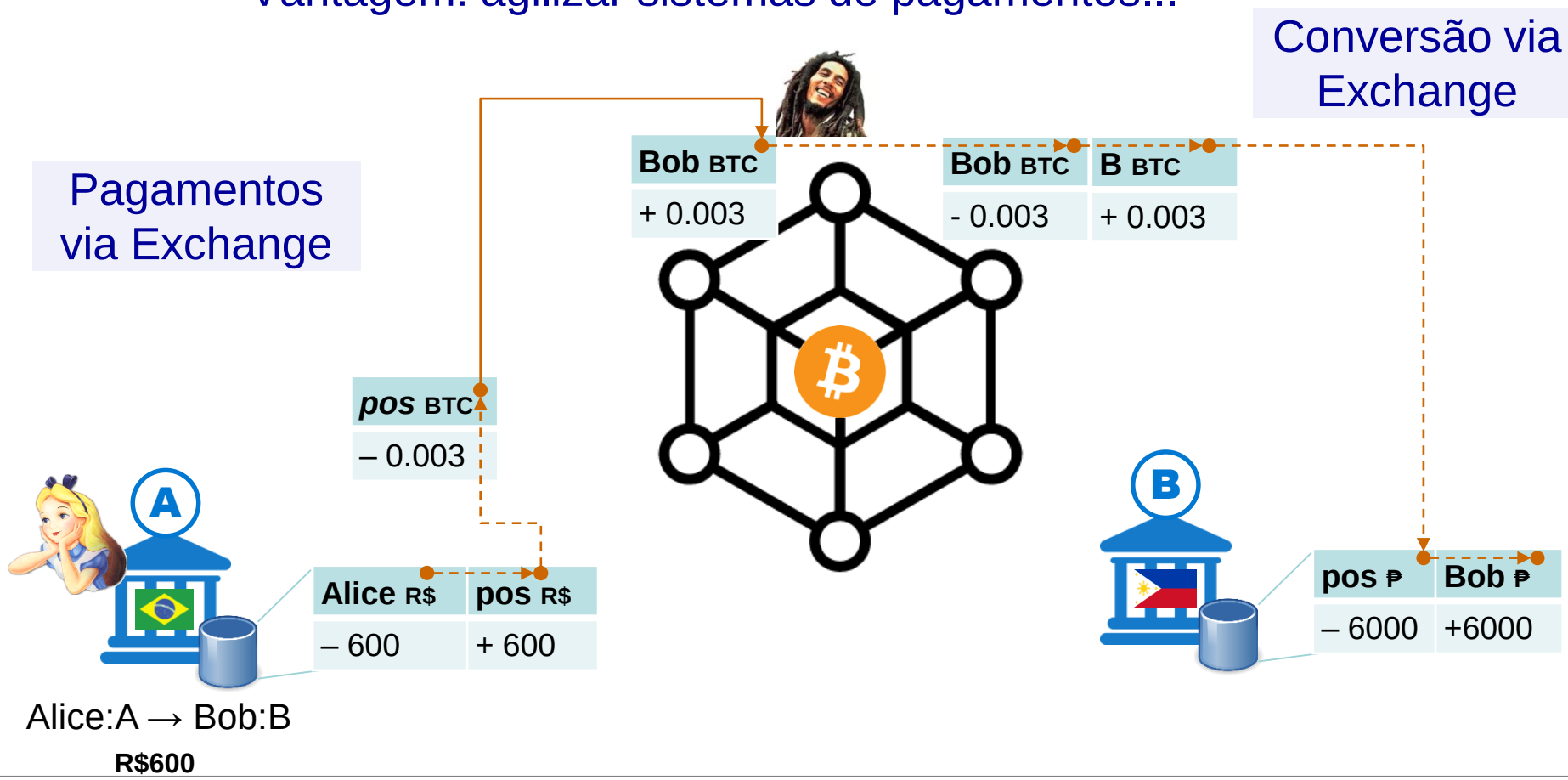
Pagamentos diretos: como “intra-banco”

Alice:A → Bob:B

R$600

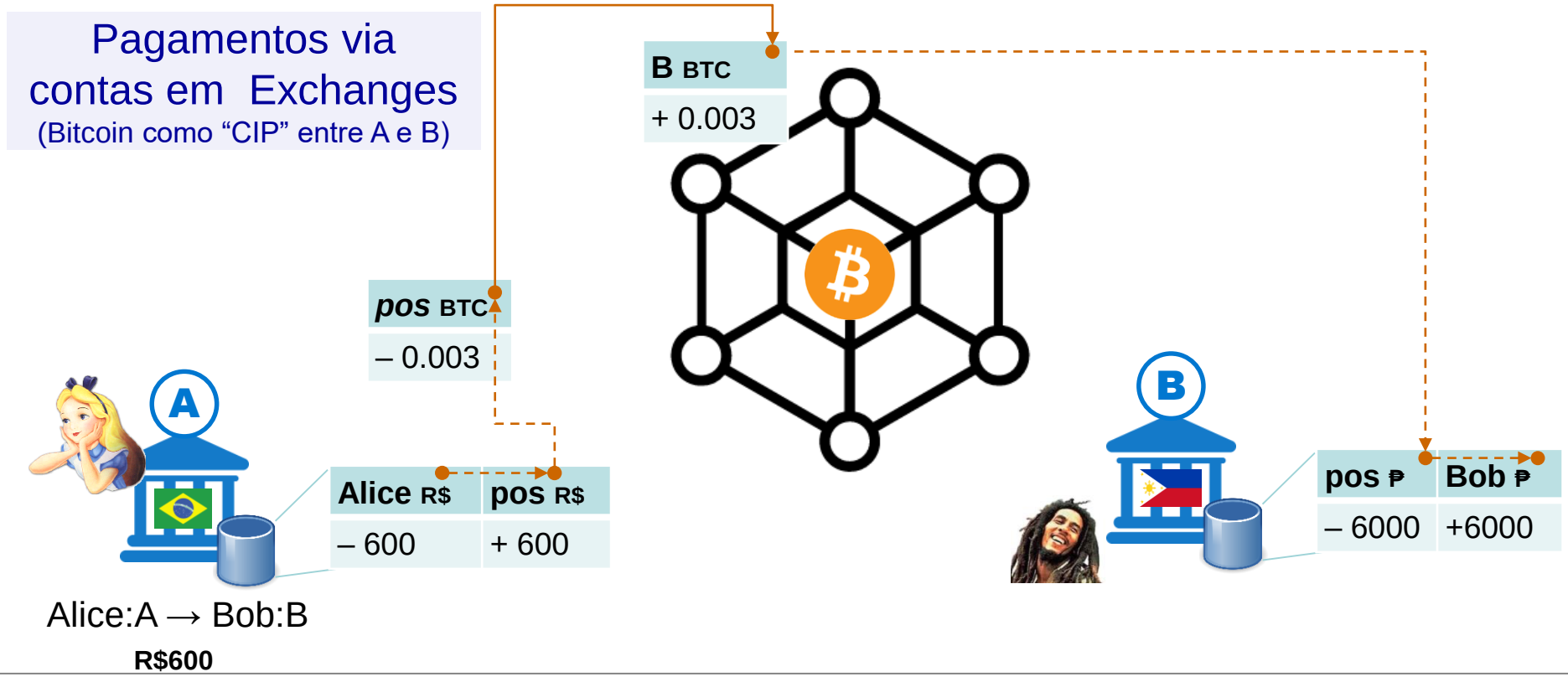
Blockchain: pagamentos

- Transferência de ativos: moedas
  - Vantagem: agilizar sistemas de pagamentos...



Blockchain: pagamentos

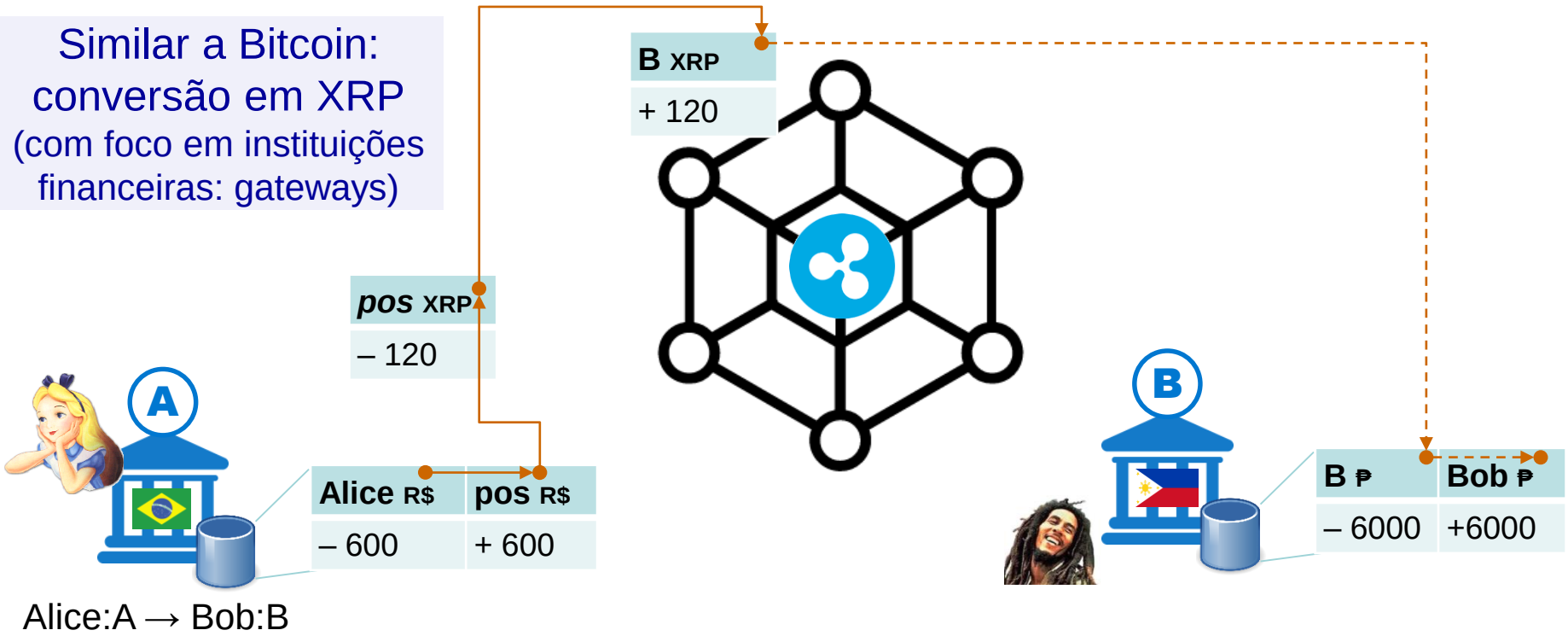
- Transferência de ativos: moedas
  - Vantagem: agilizar sistemas de pagamentos...



Blockchain: pagamentos

- Transferência de ativos: moedas
  - Vantagem: agilizar sistemas de pagamentos... em especial no caso da RippleNet (https://ripple.com/xrp/)!

Similar a Bitcoin: conversão em XRP (com foco em instituições financeiras: gateways)



Blockchain: pagamentos

- Transferência de ativos: moedas
  - Vantagem: agilizar sistemas de pagamentos... em especial no caso da RippleNet (https://ripple.com/xrp/)!

	Ripple XRP	Bitcoin (BTC)
Tempo p/ confirmação de transações	~3s	~1h (6 blocos)
Taxa média por transação	~U$0.0002	U$1-4* (picos de 60...)
#Transações/segundo	1500	~4**
Consumo energético por transação (kWh)	0.0079‡	2265†
Mecanismo de Consenso	Consensus	Proof-of-Work

* Considerando anos 2021 a 2022: https://ycharts.com/indicators/bitcoin_average_transaction_fee
** Média considerando 2019 a 2022: https://www.blockchain.com/charts/n-transactions
‡ TRG Datacenters (2021) https://www.trgdatacenters.com/most-environment-friendly-cryptocurrencies/
† Valor fornecido em https://www.statista.com/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/.

- Obs.: Consumo energético do Bitcoin em Fev/2022 era de 132 TWh/ano[a], equivalente ao consumo anual de ~5 cidades de São Paulo em 2020[b]

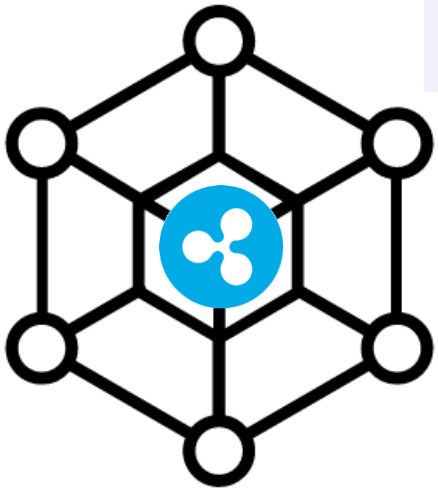
a. Cambridge Bitcoin Electricity Consumption Index: https://ccaf.io/cbeci/index
b. Anuário de Energéticos por Municípios do Estado de São Paulo, 2021 - ano base 2020: https://dadosenergeticos.energia.sp.gov.br/portalcev2/intranet/BiblioVirtual/diversos/anuario_energetico_municipio.pdf

Blockchain: pagamentos

- Transferência de ativos: moedas
  - Vantagem: agilizar sistemas de pagamentos... em especial no caso da RippleNet (https://ripple.com/xrp/)!

Linhas de crédito (*trust line*) diretas entre gateways, com valores máximos devidos e em quais moedas: promessas de pagamento (IOU: "*I owe you*")

Câmbio: ofertas de compra/venda de moedas registradas no Blockchain (com valores mantidos fora dele)



Cheques, permitindo verificar fundos e recusar pagamentos

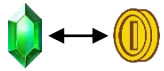
Conta com saldo pré-carregado, p/ pagamentos a terceiros (que podem sacar valor recebido)

Blockchain: outros ativos

- Variantes de **transferência de ativos (virtuais)**:
  - **Contratos** diversos, como posse ou promessa de dívida

    - Substituição de cartório físico, que tem estrutura (semi-)centralizada
    - **Importante**: eventos no blockchain não são facilmente confrontados com eventos registrados fora do blockchain (e.g., em cartórios físicos) ➔ ordenação exata exigiria **instantes exatos de tempo**
    - Inclui **contratos inteligentes** (“programa executável”): que não precisam ser sempre vinculados a blockchains (basta assinaturas digitais das partes)

  - Em jogos: **contas**, **itens colecionáveis**, **ouro/gemas**, ...
    - Ex.: figurinhas, cartas em jogos de colecionáveis

    - Comumente implementado com arquiteturas centralizadas controladas pelo gerador dos itens (**entidade confiável**): **descentralizar** pode **reduzir custos**, e aumentar **interoperabilidade** entre diferentes plataformas 

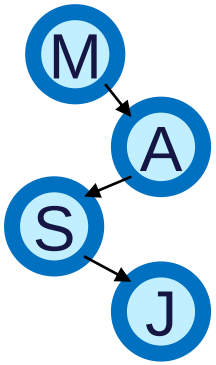
- **Desafio**: como convencer usuários a investir recursos computacionais no processo de consenso (“**incentivo**”)?

Blockchain: outros ativos

- Cuidados com **transferência de ativos reais**:
  - É necessário "**tokenizar**" ativos: como garantir que a representação digital de um ativo de fato corresponde a um ativo real?
    - Conceito também conhecido como "digital twins"
  - Alguns casos **mais fáceis**: veículos (chassis, renavam); casas (número de matrícula); pessoas (CPF+foto+digitais); obras de arte (únicas, com atestado de autenticidade feito por perito);
    - Nota: sistema cartorial atual garante **posse inicial**

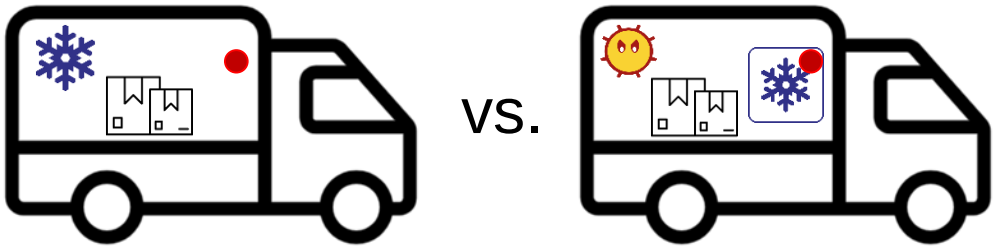
  - Alguns **mais difíceis**: produtos agropecuários (testes de DNA?); produtos químicos (???); objetos sem identificador único (???)
    - Nota: difícil impedir **geração, duplicação ou substituição** de ativos
  - **Desafio difícil** p/ algumas aplicações de **cadeia logística**

Blockchain: outros ativos

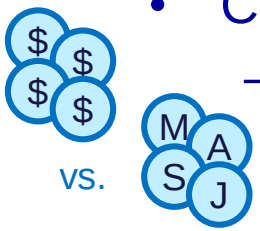


- Cuidados com **transferência de ativos reais**:
  - Mesmo **após tokenizar**: como garantir que **ações** sobre ativos reais se refletem na sua representação no blockchain?
    - Também parte do conceito de “digital twins”
  - Normalmente, é preciso recorrer a **auditoria por entidade confiável**
    - **Assinatura digital** sobre a ação é registrada no Blockchain: manutenção de equipamento, vacinação de rebanho, temperatura de transporte, ...
    - **Desafio difícil** p/ aplicações de **cadeias logísticas**: omissão, falsificação,...
      - Blockchain ou log transparente: dificulta “apagar rastros” de falhas ou auditorias fraudulentas (preserva histórico)
      - Mas não previne falhas, mesmo se auditor honesto: e.g., **dispositivo de IoT** com módulo anti-adulteração (*tamper proof*) **pode ser enganado**

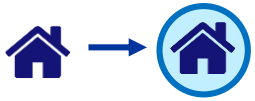
sensor temperatura

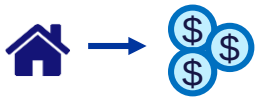


Blockchain: outros ativos



- Considerações extras sobre **ativos (reais ou virtuais)**:
  - **Fungibilidade** dos ativos tokenizados
    - Atributo que dita se tokens podem ser substituídos por outros da mesma espécie, qualidade e quantidade
  - Ex.: **bem tokenizado** em Blockchain como garantia de empréstimo
    - Alternativa 1: registro como NFT (*non-fungible token*), atribuído a emprestador segundo termos de contrato inteligente
      - Potencial desvantagem: operação atômica (tudo ou nada)
    - Alternativa 2: **conversão em FTs** (*fungible token*), de acordo com **avaliação** de seu valor no momento do registro
      - Contrato inteligente dita regras do empréstimo, como juros em #tokens e tratamento para eventual (des)valorização do token
    - Alternativa 3: registro como **NFT de referência**, e **conversão em FTs** p/ empréstimo de “pedaços” (conforme **avaliação** do NFT e FTs no registro do empréstimo)



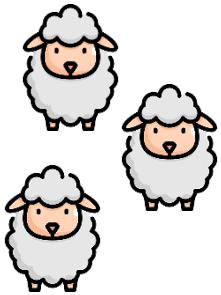


➔ Estratégias conferem maior liquidez a bens com baixa liquidez!

Blockchain: exemplos de ativos

- Outro exemplo de tokenização:
  - Itens para os quais é **difícil confirmar data de criação**: produções artísticas (e.g., música ou pintura); ideias inovadoras (patentes)
    - Risco: roubo de autoria

  - Soluções: registro em **cartório** ou em **ACT** (tradicional); **tokenização do ativo e seu dono** em blockchain (NFT)
    - Vantagem de blockchain é a **visibilidade** e menor necessidade de **confiança** no dono do cartório/ACT
    - Plataformas de **NFT**: OpenSea, Rarible, ...
  - Nota: NFT **não garante "unicidade"/"raridade"**
    - Melhor das hipóteses: com ferramentas automatizadas de detecção de similaridade, NFT é "único" por plataforma...
    - ... mas nada (exceto honestidade?) impede registro de um mesmo item em mais de uma plataforma!!!
    - Casos de apropriação indevida, falsificações, plágio... (Fev/22): https://edition.cnn.com/2022/02/13/tech/nft-marketplace-plagiarism/index.html



Blockchain: exemplos de ativos

- Mais exemplos (longe de exaustivos) de tokenização:
  - **Tempo de atenção** de usuários assistindo propaganda: Brave (navegador)
    - Nota: abordagem comum em jogos móveis gratuitos (sem blockchain)
  - **Conteúdo** gerado por usuários em redes sociais, ou jogos: Social.Network, Minds, soluções do “metaverso” (*Second Life*-like)
  - **Ativos ambientais**, como áreas de floresta (Moss, Tree Cycle, Carbon 21), ou biodiversidade na forma DNA extraído de espécies em regiões de difícil acesso (Biobanco da Amazônia)
  - **Indexação de dados** espalhados em blockchains: TheGraph
  - **Participação societária** em empresas (*equity tokens*, ou *security tokens*) : várias Exchanges no mundo todo, USP Coin
  - **Recursos computacionais** de usuários: Filecoin, BitTorrentSpeed**,** Torrente

@USP

Blockchain: exemplos de ativos

- Tokenização: não é só hype...
  - Valor normalmente relacionado com sua **utilidade** (e.g., uso em plataforma virtual, ou ter direito reconhecido sobre ativos reais) e/ou interesse potencial por terceiros (i.e., **liquidez** do investimento)

Qual o preço justo de um NFT da Mona Lisa...?

https://medium.datadriveninvestor.com/why-nfts-dont-have-a-screenshot-problem-4e8b284051b9

https://www.vix.com/pt/mundo/538712/como-um-dos-maiores-mentirosos-da-humanidade-conseguiu-vender-a-torre-eiffel

Victor Lustig: o homem que "vendeu" a Torre Eiffel (1925)...

https://9gag.com/gag/a11PEXG

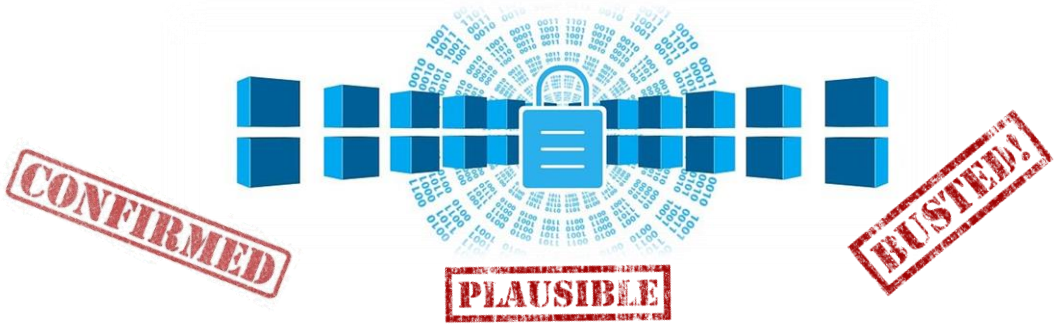
Même: dar a Putin um NFT da Ucrânia pararia a guerra

Logs transparentes e ativos: ?

- Possível também usar logs transparentes p/ transferência de ativos: evitam-se custos com consenso
  - **Servidor de Log**: entidade logicamente centralizada responsável por **ordenar** dados após **validação** (“Proof of Authority”)
  - **Auditores** verificam periodicamente: **validade de blocos** inseridos; **consistência** do blockchain (política de “**apenas adição**”)
    - Armazenam **estado global** da rede em vez de cópia de blockchain: posse atual de NFT; saldo atual de usuário em FTs
    - Em caso de **conduta indevida**: **avisar** usuários via protocolo próprio, redes sociais, ou qualquer outro meio conveniente
  - **Usuários**: podem obter estado junto a diferentes auditores, fazendo validação cruzada; podem verificar eles mesmos o blockchain
- Grau de confiança similar a Blockchain completo
  - Assumindo replicação do Servidor de Log: ponto crítico de falha!

Blockchain: exercício

- Tente imaginar o uso de blockchains nos cenários a seguir:
  - Plataforma substituta a cartórios em registros de pessoas físicas (nascimento, ..., casamento, falecimento)
  - Plataforma para registro de preços diversos de produtos
- Responda:
  - Blockchain seria útil, facilitando procedimentos e/ou adicionando funcionalidades?
  - Há limitações no cenário que ainda exijam entidades confiáveis?
  - Quais seriam incentivos razoáveis para a participação no sistema, seja como um nó mantenedor ou como um provedor de dados?
- Algumas considerações no apêndice
  - Nota: sem pretensão de ser “a resposta correta”, mas apenas discutir os conceitos aqui apresentados



Blockchain, Criptomoedas & Tecnologias Descentralizadas

Blockchain sem o hype:

Algumas lendas (?) sobre blockchains

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

Referências

- K. Wüst, A. Gervais (2017). "Do you need a Blockchain?" Cryptology ePrint Archive: Report 2017/375. URL: https://eprint.iacr.org/2017/375
- S. Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". Whitepaper, 2008. URL: https://bitcoin.org/bitcoin.pdf. Veja também (tradução paara português): https://cointimes.com.br/whitepaper-do-bitcoin-traduzido/
- D. Schwartz, N. Youngs, A. Britto (2018). “The Ripple Protocol Consensus Algorithm”. White paper. URL: https://ripple.com/files/ripple_consensus_whitepaper.pdf
- Ripple (2020). “The Future of CDBCs – Why all central banks must take action”. White paper. URL: https://ripple.com/wp-content/uploads/2021/01/cbdc-whitepaper-2020.pdf
- BCB (2021). "Lift Challenge - o Real digital". Banco Central do Brasil (online) URL:
- https://liftchallenge.bcb.gov.br/site/liftchallenge

Blockchain: “Lifechain”

- Variante de transferência de ativos
  - “Token de vida” criado no nascimento e destruído no falecimento
    - Certidões (**identidade**) emitidas por **entidade confiável** (e.g., cartório)
  - Eventos que dependem apenas dos usuários feitos de forma **totalmente distribuída**

    - Casamento ou divórcio consensual: cônjuges assinam o “eu aceito”
      - Não muito diferente de status de relacionamento no Facebook...
      - Mas divórcio litigioso pode exigir **entidade confiável**
    - Uso de nome social: usuário assina seu novo nome
  - Requer **ordenação de eventos**: previne duplo casamento, duplo nascimento, duplo nome, dupla morte, etc.
    - **Sem confiança** nos usuários: podem tentar praticar bigamia, fraudar seguros de vida, receber aposentadoria de falecidos, etc.
  - **Incentivo**: “pelo bem do sistema” ou política governamental (e.g., incentivos fiscais)

Blockchain: “PriceChain”

- Variante de transferência de ativos
  - **Eventos**: vendedores registram preços; compradores registram compras pelo preço do vendedor.
    - Útil para concorrências públicas e disputas sobre preço anunciado
  - Requer **ordenação de eventos**: compra por preço X só pode ocorrer após registro de preço X; listagem de preços para diversos concorrentes em certo instante de tempo
  - **Sem confiança** nos usuários: comprador pode tentar ignorar preços mais baixos (fraude em concorrência pública); vendedor pode se recusar a honrar preço de oferta (Procon, artigo 35)
  - Registros de forma **totalmente distribuída**:
    - Alternativa a **entidades confiáveis**: sites com histórico de preços (Black Friday...); sites de cotações (Buscapé, Zoom, MelhorCâmbio, ...)
    - Nota: identificar produtos idênticos pela sua descrição não é trivial...

Incentivo: créditos em compras (compradores); exigência para participação em concorrências e preferência em caso de preços idênticos (vendedores)