Insper

Ativos Digitais e Blockchain

Ricardo Rocha
Raul Ikeda

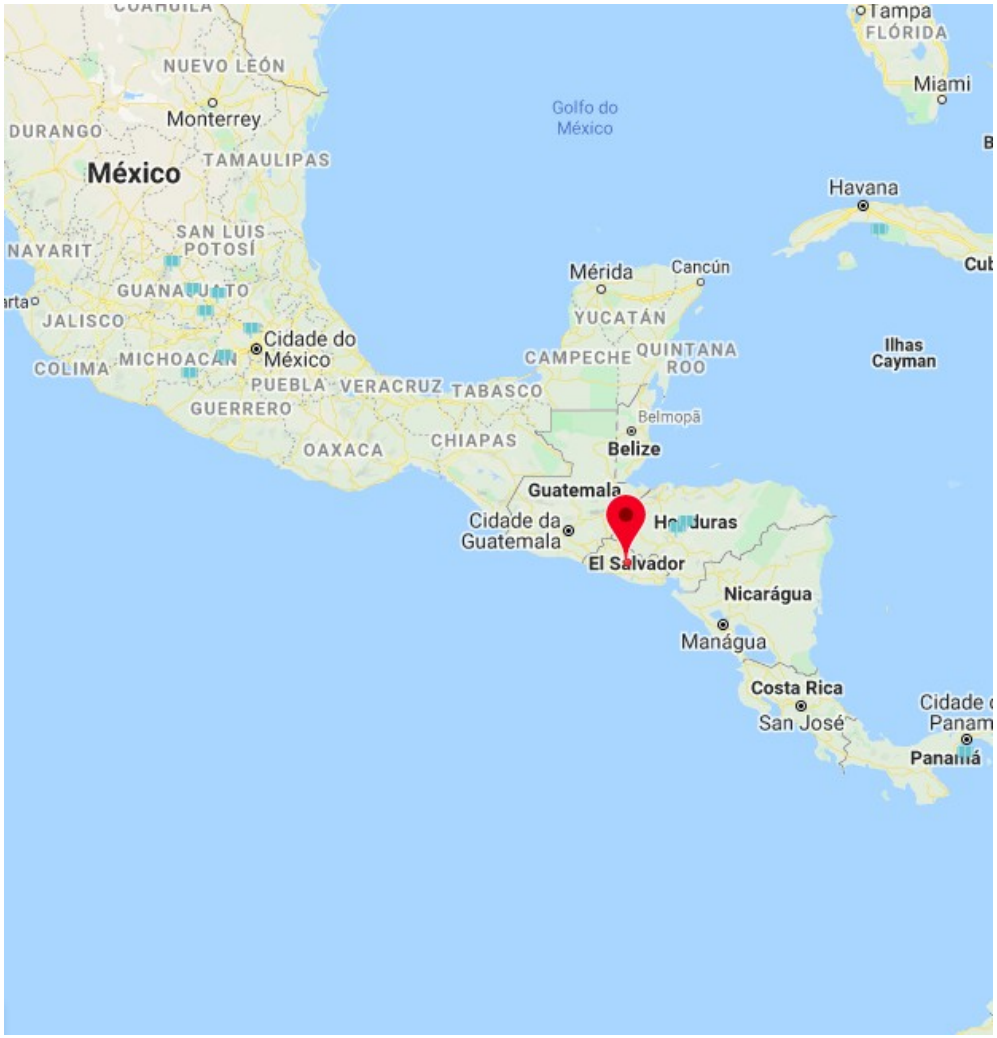
Relembrando:

- Bitcoin: caro (0.0005BTC) + lento (10 minutos)
- Ethereum: supercomputer + Smart Contracts + GAS
- Tokens & NFT

Objetivo

- Explorar alternativas aos principais problemas das redes

Case El Salvador



Fonte: Google Maps

- Dados Socioeconômicos:

- PIB: US$ 54 Bilhões (101º)
- Per capita: US$ 8.388,00 (111º)
- População: 6,83 milhões (107º)
- Área: 21 mil km²
- Moeda: USD e **BTC**
- Fonte: Wikipedia

Insper

BTC?

- Primeiro país a adotar oficialmente BTC como moeda corrente.
- Aprovado pelo congresso salvadorenho em 09/Jun/2021.
- Fez a primeira compra no dia 07/Set. 400 BTC.
- Muitos problemas técnicos durante a implantação.
- Distribuiu cerca de $30 para os cidadãos via carteira Chivo.

- Como as pessoas transacionam valores se as taxas são altas de as confirmações demoradas?

Lightning Network

- Decentralizado
- Rede tipo Layer 2 que age sobre a rede do Bitcoin
- Tecnicamente pode agir sobre qualquer rede blockchain
- Permite transacionar bitcoins com uma taxa muito baixa e instantaneamente
- Não realiza transações realmente na rede bitcoin

- Mais detalhes: http://lightning.network/docs/

Lightning Network

- A ideia é ter uma rede p2p própria com seus próprios nós
- Uma pessoa cria um canal multisig com outra pessoa depositando bitcoins oriundos da rede bitcoin
- Como os nós são interligados pelos canais, é possível enviar e receber para qualquer conta da rede, passando pelos diversos nós. Algoritmo análogo ao da Internet
- É preciso pagar apenas 1 transação da rede para começar a realizar os pagamentos e 1 transação para transferir de volta para rede

Lightning Network

- Não há mineração
- Qualquer pessoa pode ser um node
- Um node pode rodar em equipamentos muito baratos ($50) e que consomem pouquíssima energia
- Não há incentivos financeiros claros

- Por que alguém seria nó da rede?

Ripple

- Protocolo de meio de pagamento
- Empresa privada
- Possui uma moeda (XRP), mas permite a criação de moedas customizadas
- Foi criado para concorrer com métodos tradicionais de wire (SWIFT por exemplo)
- NÃO usa Blockchain, mas usa uma rede e tem mecanismo de consenso (RPCA - https://ripple.com/files/ripple_consensus_whitepaper.pdf).

- XRP é uma cryptomoeda?

Altcoins ou Tokens?

- Altcoins: moedas com rede própria derivada de certa forma do Bitcoin. Cada uma possui suas próprias características, adicionando funcionalidades que gerariam forks na rede.
  - Exemplos: Litecoin, Dogecoin, Monero, Dash, etc
- Tokens: São apenas representações de algum objeto dentro de um Smart Contract que rege o ownership dos tokens. Normalmente implementado no Ethereum (ERC-20) ou outra plataforma que suporta Dapps. (https://coinmarketcap.com/tokens/views/all/)

Outros Termos

- Stablecoins: moedas baseadas em algum ativo, normalmente com lastro. Procuram diminuir a volatilidade. Normalmente é token based. Exemplo: USDT, BUSD, USDC, etc.
- NFT: Non-Fungible Tokens, tokens que representam algo único, colecionável.
- DeFi: Decentralized Finance, termo designado para representar todo ecossistema de serviços financeiros em cima de blockchains.
  - Geralmente tokens emitidos por Smart Contracts
  - Podem possuir encadeamento entre eles
  - Um fork no Ethereum poderia causar um grande estrago
  - https://medium.com/dragonfly-research/ethereum-is-now-unforkable-thanks-to-defi-9818b967738f

- Um grande zoológico: https://coinmarketcap.com/cryptocurrency-category/
- Ou cemitério: https://99bitcoins.com/deadcoins/

Reflexão

- Por que você começaria um novo projeto usando Blockchain?

Blockchain – Quando usar

Pense na sua solução e nas partes envolvidos, respondendo as seguintes perguntas:

- Os recursos e/ou dados são compartilhados entre as partes?
- Sua solução precisa de um intermediário para auditoria?
- Há problemas de confiança entre as partes envolvidas?
- Você abre mão de desempenho computacional?
- Você não precisa de uma solução distribuída?
- Está disposto a pagar mais caro que uma solução tradicional?

Se você respondeu **SIM** a todas as questões, estaria elegível a utilizar Blockchain como plataforma da solução.

Se as informações precisam ser públicas, utilize Blockchain Pública, senão utilize Blockchain Privada.

Essay (Ensaio)

- Texto curto de autoria própria sobre a pesquisa de um determinado tema
- Objetivo: Pesquisar e dissertar sobre uma cryptomoeda
- Sugestão de pauta: Origem, motivação, acontecimentos relevantes e planos futuros
- Concluir o texto com a opinião sobre o futuro das cryptomoedas em geral e da tecnologia Blockchain
- Lista de Moedas: Link no Blackboard
- Cada moeda só pode ser escolhida uma vez (first come, first serve)
- Individual – Ao final vou publicar todos os essays.
- **Modelo no Blackboard**
- Esperado cerca de 1 página em PDF
- Entrega: 11/Mai às 23:59 via Blackboard. Após esse prazo valerá no máximo C (5,0).

Recapitulando

- Layer 2 como solução de problemas das redes
- Nem tudo é como o Bitcoin ou Ethereum
- Tokens são simples e baratos, mas podem ser um grande problema
- Ecossistema diverso, complexo e muito frágil

Próxima aula

- Modelos de Negócio com Smart Contracts