Insper

Ativos Digitais e Blockchain

Ricardo Rocha
Raul Ikeda

Relembrando: Bitcoin

- Ledger (livro caixa) ou apenas registros de transações
- Meio de pagamentos
- Proof of work, ache o nonce primeiro
- Um bloco a cada 10 minutos em média
- Maior rede

Objetivo

- Aprofundar mais ainda sobre Blockchain via Ethereum

Decentralized World Post-Bitcoin

- Novas redes:
  - Namecoin – registro de nomes decentralizados
- Protocolos sobre o Bitcoin:
  - Colored coins – uma tentativa de criar outras digital currencies via o ancestral dos tokens (colors)
  - Metacoins – uma tentativa de ampliar as funcionalidades da Blockchain para além de transações

Quais os empecilhos?

- Novas redes: muito difícil de colocar no ar, depende de adesão dos nós.

- Protocolos sobre o Bitcoin: o bitcoin não foi projetado para isso e não permite o registro de informações adicionais às transações. Por exemplo: para realizar micro pagamentos, dependeria de aglutinar múltiplas transações que dependeriam de um agente centralizador temporário.

Fantasmas do Bitcoin

- Não conseguir provisionar valores para garantias (transações condicionadas)
- Ser Turing Incompleto (Não permite scripting com loops)

Solução: Ethereum

- Nova rede. Não poderia ser apenas top layer.
- Ao invés de apenas transações, vamos permitir rodar scripts (aka programas)

- Ethereum é um **MEGA** computador decentralizado que, além de transacionar valores, roda programas!

- Qual a implicação disso?

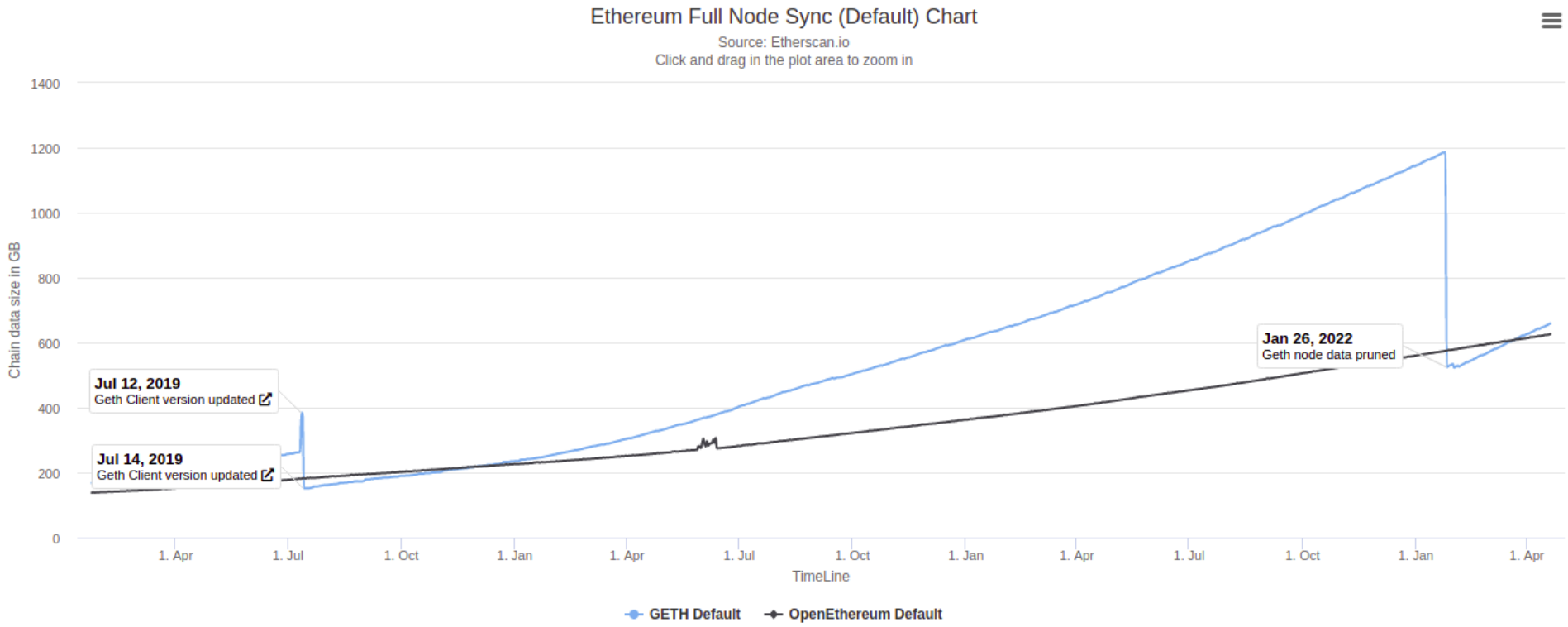
Blockchain by Ethereum (20/Out)

- Apresentado em 2013 por Vitalik Buterin
- Atualmente 658Gb full e 625Gb pruned (openethereum)
- Cada bloco tem em média 92Kb
- 1 Bloco a cada 13 **segundos** em média
- Remuneração por bloco (London EIP-1559):
  - 2 ETH (Ethers) via mineração
  - 5 ETH via transaction fees em média
- 1250 mil Transações por dia em média
- Usa uma EVM (Ethereum virtual machine).
- Cada smart contract paga-se um fee para executar e/ou armazenar dados.
- ASIC & FPGA safe – desenhado para rodar em computadores reais, com muita memória.

Mais detalhes: https://etherscan.io/


Ether Daily Price (USD) Chart
Source: Etherscan.io
Click and drag in the plot area to zoom in
Ether Price (USD)
6 k
5 k
4 k
3 k
2 k
1 k
0
Jan '16
Jul '16
Jan '17
Jul '17
Jan '18
Jul '18
Jan '19
Jul '19
Jan '20
Jul '20
Jan '21
Jul '21
Jan '22

Insper


Ethereum Full Node Sync (Default) Chart
Source: Etherscan.io
Click and drag in the plot area to zoom in
Chain data size in GB
1400
1200
1000
800
600
400
200
0
Jul 12, 2019
Geth Client version updated
Jul 14, 2019
Geth Client version updated
Jan 26, 2022
Geth node data pruned
1. Apr
1. Jul
1. Oct
1. Jan
1. Apr
1. Jul
1. Oct
1. Jan
1. Apr
1. Jul
1. Oct
1. Jan
1. Apr
TimeLine
GETH Default
OpenEthereum Default

Insper

Implementação

- Comunidade extremamente organizada
- Site: https://ethereum.org
- Documentação: https://ethereum.org/en/developers/docs/

Networks

- Mainnet (Eth1 – London)
- Testnets
  - Görli (Proof-of-Authority – multiple clients)
  - Kovan (Proof-of-Authority – OpenEthereum clients)
  - Rinkeby (Proof-of-Authority – Geth clients)
  - Ropstein (Proof-of-Work – espelho da Mainnet)
- Redes privadas

- Proof-of-Authority: apenas alguns mineradores são autorizados a minerar na rede. O ether dessas redes não possuem valor agregado e podem ser solicitados via faucets

- https://ethereum.org/en/developers/docs/networks/

Eth1 vs Eth2

- Hoje mainnet contém o que é chamado de Eth1
  - O protocolo de consenso é Proof-of-Work (igual ao Bitcoin)
  - Diversos EIPs (Ethereum Improvement Proposal) foram implantados, o mais recente é o London
  - No ar desde 05/Ago, ele altera a forma de remuneração dos mineradores
- Há perspectivas de implantar a versão Eth2 em 2022
  - Principal mudança: Proof-of-Stake

PoW ou PoS

- Na aula passada foi apresentado o conceito de Proof-of-Work: o primeiro que descobrir o nonce do bloco, apresenta aos demais que validam o resultado.
- Proof-of-Stake apresenta uma ideia diferente: candidatos a mineradores realizam depósitos e o próximo minerador é sorteado proporcionalmente ao valor depositado. Caso o minerador cometa uma fraude, a diferença é descontada do seu depósito.
- Isso reduz significativamente o custo de mineração, tanto em equipamento quanto em eletricidade.
- Reduz significativamente o risco de ataque 50% + 1, pois não há incentivos para criar mining pools.
- Porém pode ser um sistema injusto se poucos participantes realizarem um depósito muito superior aos demais.
- Ethereum pretende migrar de PoW para PoS devido a problemas de congestionamento na rede.

Smart Contracts

- Bitcoin suporta apenas o registro de transações de moedas.
- Ethereum, por outro lado, permite a execução de programas com variáveis, loops, funções e eventos.
- É considerado um super computador decentralizado que armazena e modifica os estados de cada programa a medida em que as funções são chamadas.
- Esses programas são chamados de Smart Contracts.
- As aplicações formadas por smart contracts são chamadas de **DApps** (**Decentralized Applications**)
- DApps abrem uma nova gama de aplicações com modelos de negócios diferentes, reinventando os processos sobretudo no que tange a transações financeiras. Essa transformação digital tem sido chamada de WEB3.
- No Ethereum é necessário utilizar uma moeda chamada GAS para executar diversos comandos. GAS pode ser comprado com Ethers.

GAS?

- É unidade de medida da quantidade de esforço computacional necessário para rodar um programa na rede
- É possível estimar quanto GAS será necessário para executar alguma operação de um contrato. Algumas operações são gratuitas
- O Valor do GAS é descrito em ETH e o valor pago por depende da prioridade com que deseja ter na execução das tarefas:

https://ethgas.watch/

https://youtu.be/AJvzNICwcwc

Insper

ERC-20 & ERC-721

- Ethereum é tão poderoso que permitiria rodar sistemas complexos (com certo custo)
- É possível criar um Smart Contract para a emissão, compra e venda de tokens
- Tokens são objetos que representam outro objeto. Incluindo algum ativo, tíquetes, ouro ou dinheiro (moedas).
- Esses Tokens são comumente usados para representar cryptomoedas que não possuem rede própria.
- Existem 2 ERCs (Ethereum Request for Comments) que estabelecem padrões para tokens como valor:
  - ERC-20: para token de cryptomoedas em geral. Evoluiu para ERC-777.
  - ERC-721: para tokens NFT (Non-Fungible Tokens – aka colecionáveis, ou itens únicos).

https://ethereum.org/en/developers/docs/standards/#token-standards

Como começar a programar?

Site: http://ethereum.org/developers/

- Smart Contracts:
  - Solidity
  - Vyper
  - etc
- Frameworks:
  - Truffle
  - Waffle
  - Brownie
  - etc
- Network:
  - Testnets
  - Ganache
  - Ethnode
  - Infura
  - etc

ETH ou ETC

- Em 2016 um fundo chamado The DAO, Decentralized Autonomous Organization, uma espécie de Kickstarter para Dapps, sofreu um grande ataque perdendo $150 milhões devido a vulnerabilidade dos seus smart contracts
- Após uma grande discussão, optou-se por reverter os blocos até o momento do início do ataque
- Alguns membros achavam que modificar a Blockchain tiraria a sua credibilidade
- Houve então um hard fork e criou-se a rede Ethereum Classic (ETC), que manteve a Blockchain intocada
- Depois desse fork, já houve mais duas reversões de ataques

Recapitulando

- Ethereum é um super computador
- Ele roda programas (Smart Contracts) na Blockchain
- Smart Contracts são parte de Decentralized Apps (DApps)
- Não foi desenhado para ser rápido ou barato e sim confiável.
- Possui uma gama de aplicações mais amplas que o Bitcoin.
- Comunidade organizada e sempre em evolução

Próxima aula

- Outras redes e cryptomoedas