Blockchain: muito mais que o bitcoin

Agenda

- Passado: criptografia, função hash, assinaturas digitais, *proof of work* e *bittorrent*
- Presente: bitcoin, ethereum, mineração
- Futuro: DAG, federações, outros usos e desafios
- FS2: como estamos contribuindo para o ecossistema

Antes de mais nada:
o que é um blockchain?

Blockchain é uma estrutura de armazenamento de dados cujas propriedades matemáticas tornam alterações (praticamente) impossíveis de serem realizadas.

A tecnologia do blockchain é o resultado de **décadas** de pesquisa em *criptografia*, *estruturas de dados* e *protocolos de redes*.

Criptografia de chave pública

- Você usa todo dia!
  - É o cadeadinho do Chrome (HTTPS)
- Resolve o problema de compartilhar o segredo de uma informação encriptada.
- Cria duas chaves:
  - **Chave pública:** Só encripta, então você pode divulgar a vontade.
  - **Chave privada:** A chave mestra que abre todas suas chaves públicas.
- Primeira ideia em 1874, por William Stanley Jevons:

> *Can the reader say what two numbers multiplied together will produce the number 8.616.460.799? I think it unlikely that anyone but myself will ever know.*

Função de hash criptográfico

- Indexa qualquer informação a um número entre zero e muito grande.
  - SHA256, usada pelo bitcoin, indexa em 2^{256} posições.
- É uma função unidirecional, caótica e equiprovável:
  - Você obtém o número, mas do número você não obtém a informação.
  - Qualquer mínima alteração da informação causa efeitos imensos: efeito borboleta.
  - A chance de obter qualquer valor é a mesma.
- Exemplos em SHA256:

A aranha arranha o jarro.

D8AD8E4734ACE960FDB3992D2DCD3B0D
319ADC134536BF912368B2B18EBC4D1F

662A829F1B19F4E48912253826E7E66C
343ABD0CFEA646FC0F103487CA4268BA

A aranha arranha o iarro.

1C3E926B0CE1E99EAFECFAAB9F4A3D95
B26859E5F756686D89148933B4F1A4C1

Assinaturas digitais

- Utiliza princípios da criptografia de chave pública.
- Tem sido utilizada já há alguns anos: e-CPF e e-CNPJ

Proof or work (prova de trabalho)

- Publicado por Cynthia Dwork e Moni Naor em 1993

- Consiste em provar que você realizou trabalho (processamento) ao cumprir um desafio
  - O cumprimento do desafio permite que alguma ação seja realizada

- Existem diversos desafios possíveis, mas vamos nos focar no baseado em funções de hash criptográfico
  - Largamente utilizado desde antes do blockchain do bitcoin

DESAFIO:

Só vou ler mensagens cujo valor de hash SHA256 comece com 6 zeros.
Todas as que não cumprirem esse quesito, serão ignoradas.

Desafio *proof of work*

MENSAGEM: Rick, vamos comer panquecas?
VALOR DE HASH: 7ADEF438AEF09DB32808702041FDA29697F0D18E9EA4570BF60A3B00D26F7880

MENSAGEM: Conheça nossas promoções! http://promocao.com.br
VALOR DE HASH: 193FB03FBC908421D260F8C5AB80DBC767FC4646DA630B711F1A426475D9EC4D

MENSAGEM: Rick, vamos comer panquecas? 6470157
VALOR DE HASH: 000000ED2A51CE731EDA32C1407CF4E5767628EFCAECA4A6F3538EEB5363735F
Tempo de processamento: 8.3 segundos

Bittorrent

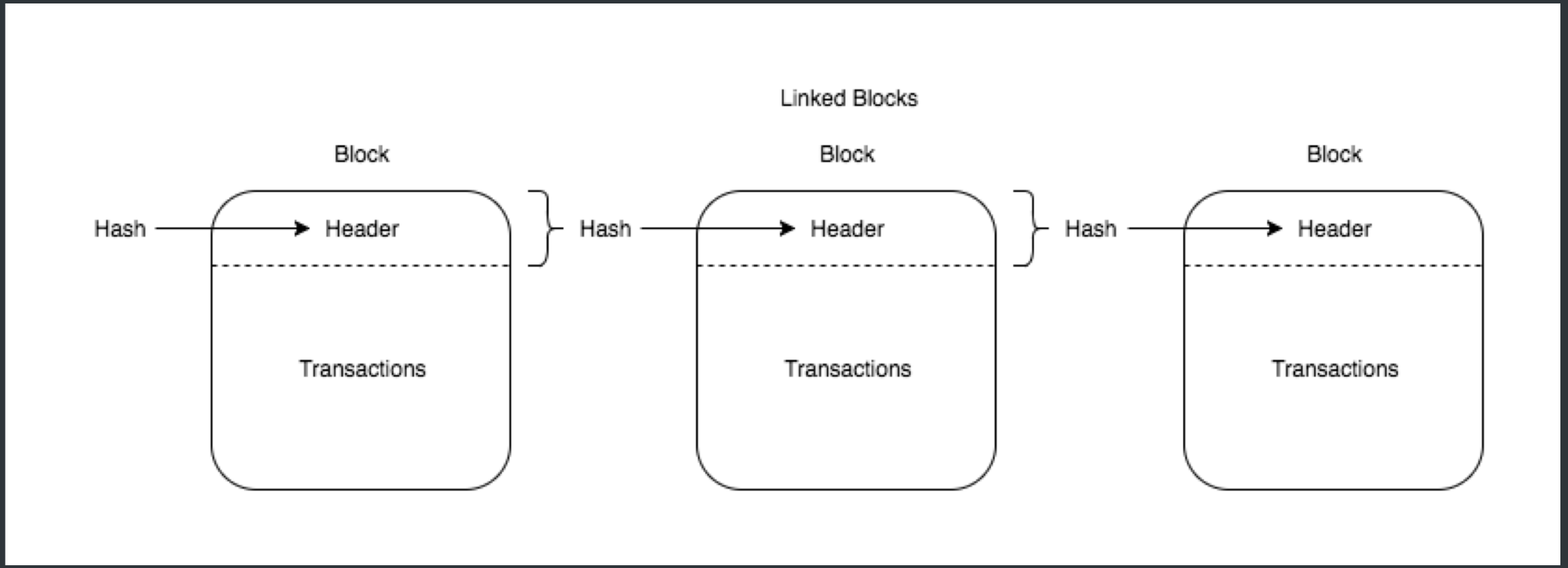
- Você usa e talvez nem saiba
  - A Blizzard usa para distribuir World of Warcraft, StarCraft, Diablo e outros conteúdos.
- É um sistema de distribuição de arquivos descentralizado
- Fatia-se o(s) arquivo(s) em centenas ou milhares de pequenos pedaços (ou blocos) e envia-se esses pedaços um de cada vez
- O arquivo .torrent contém informações a respeito do que se está sendo enviado:
  - Valor de hash de todos os arquivos juntos
  - A quantidade de pedaços e o valor de hash de cada um
- O software de download envia e recebe pedaços em qualquer ordem que se queira
- Os valores de hash asseguram que o que você baixou era o que você esperava

Presente (desde 2008):
Era Blockchain

Blockchain

- Agora temos todos os elementos que precisamos para montar um blockchain!
  - Um sistema seguro para trocar e verificar informações
    (Criptografia de chave pública e assinaturas digitais)
  - Uma ferramenta para verificar se a informação não foi alterada
    (Função de hash)
  - Um desafio que dificulta alterações
    (Proof-of-work)
  - Uma maneira de distribuir pedaços de informação entre muitos atores
    (Tecnologia do bittorrent)

Blockchain


Linked Blocks
Block
Hash
Header
Transactions
Block
Hash
Header
Transactions
Block
Hash
Header
Transactions

Bitcoin

- Criado em 2008 pela misteriosa figura de Satoshi Nakamoto
- Carteiras bitcoin são chaves privadas
- Endereços bitcoin são chaves públicas
- Transações ocorrem enviando uma mensagem para a rede:

  "Transfira 0.5 bitcoin do endereço A para o endereço B."

  A mensagem é assinada digitalmente com a minha chave privada

  O endereço A é minha chave pública

  O endereço B é a chave pública de quem vai receber

- Os outros participantes da rede irão verificar se a transação é válida

  A assinatura da mensagem bate com a chave pública de quem está enviando?

  O endereço A tem esse saldo para enviar?

- Se for válida, será incluída num bloco a ser minerado

FS2

Mineração

- Mineração é o ato de reunir transações enviadas para a rede bitcoin e organizá-las em um bloco válido
  - O bloco contém também o valor de hash do bloco anterior
- Um bloco é válido se o valor de hash dele começar com uma certa quantidade de zeros
  - Encontrar isso é muito difícil, principalmente hoje em dia
- Quem encontra, recebe uma recompensa!
  - 12.5 BTC atualmente
  - Começou com 50 BTC, após quatro anos, caiu para 25 BTC, etc.
- Uma transação é considerada confirmada se estiver dentro de um bloco válido
  - Cada novo bloco após o que contém a transação, adiciona uma nova confirmação
  - É comum uma transação ser aceita pelo destinatário somente após um certo número de confirmações, tipicamente entre 3 e 6

Mineração

- Evita que se gaste duas vezes a mesma moeda
- Força que haja consenso na rede
- Impede a alteração de registros
- É a responsável pela emissão de bitcoins
- O primeiro bloco foi escrito por Satoshi Nakamoto em 03 de janeiro de 2009

  A primeira transação do primeiro bloco traz junto consigo a manchete do The Times daquele dia: "Chancellor on brink of second bailout for banks"

- Esses conceitos valem para todas as criptomoedas baseadas em Proof-of-Work

Ethereum e *smart contracts*

- Utiliza o Proof-of-Work
  - Existe uma forte iniciativa para mudar para Proof-of-Stake
- Imaginada por Vitalik Buterin em 2013, lançada em 2015
- Implementa uma linguagem de programação na blockchain
- Facilita a criação de smart contracts
  - São contratos auto-enforçáveis
  - A realização de uma ação causa automaticamente um efeito:
    - Uma troca de ativos
    - A emissão de um certificado
    - Uma distribuição de valores, etc.
- Permite a emissão de tokens na rede Ethereum
- Chamados tokens ERC20, utilizado por empresas como representação de valores ou ações
- Comunidade bastante ativa, diversas ferramentas disponíveis

Usos atuais do blockchain

- Agilizar transações internacionais
  - Banco do Brasil, Caixa e Santander estão utilizando para transações entre alguns países
- Microtransações entre partes
  - Valores menores que 1 centavo, por exemplo
  - Gorjetas (Dogecoin)
- Colecionáveis e jogos
  - CryptoKitties
  - Decentraland
- Pagamentos anônimos
  - DASH, Zcash, Monero
- Bolsas descentralizadas
  - Através de smart contracts
- Prova de existência e/ou autenticidade
  - LegalChain

Futuro:
Ao infinito e além?

Blockchain, só que não

- Grafos acíclicos direcionados (DAG)
  - IOTA
    - Estrutura de emaranhado
    - Alta capacidade de processamento
    - Elimina taxas de transação
- Federações
  - Stellar / Ripple
    - Passa de proof of work para consenso através de linhas de confiança
    - Taxas de transação bastante reduzidas
    - Entidades podem escolher em quem confiar

Lightning network (Bitcoin)

- Adiciona uma camada de pagamentos ao blockchain do bitcoin
- Muito parecido com federação
  - Linhas de confiança são criadas através de transações bitcoin comuns, com propriedades especiais
- Resolve os problemas de:
  - Escalabilidade
  - Valores de taxas
  - Tempo de processamento
- Críticos reclamam que remove a principal fortaleza do bitcoin: não precisar confiar em ninguém

Desafios

Escalabilidade

- Proof-of-work é bastante custoso
  - Muitos argumentam que é ecologicamente inviável a longo prazo
- Transações não são instantâneas
  - Imagine esperar 20 ou 30 minutos para sua transação confirmar, o café que você comprou estará frio
- A rede possui uma capacidade muito baixa de processamento
  - Bitcoin - 7 tx/segundo
  - Ethereum - 15 tx/segundo
  - VISA - 45000+ tx/segundo
- O blockchain inteiro é muito grande
  - A promessa da descentralização esbarra no custo de ter máquinas potentes o suficiente
  - Atualmente, está em cerca de 183 GB
- Lightning Network é a melhor aposta para solucionar

Identidade e autenticidade

- Seres humanos não são passíveis de serem aplicados uma função de hash criptográfico
  - Há uma dependência de serviços externos e centrais que verificam que certa chave pública corresponde a uma determinada pessoa
  - Isto causa preocupações com privacidade e rastreabilidade
- Produtos que queiram ser rastreados via blockchain podem ser alterados no meio do caminho
  - Se eu tenho um carregamento de maçãs que foi registrado na blockchain como “boas, vermelhas e suculentas”, nada impede que a caixa seja aberta e o carga trocada
  - A tecnologia que previa eliminar confiança acaba dependendo de agentes confiáveis nesta área

Complexidade

- Nem todos os problemas precisam de uma blockchain
  - Muitas vezes, é mais simples utilizar um banco de dados centralizado do que uma blockchain
    - Principalmente quando se fala em blockchain privada
  - Menos infraestrutura para se administrar e menos problemas insolúveis, como envio de transações para chaves erradas, que precisam ser revertidas
- Existe uma barreira alta de entrada
  - É necessário explicar claramente as implicações de utilizar sistemas de criptografia de chave pública
  - As contas Google, Facebook, Twitter não teriam a penetração que têm se a complexidade fosse maior
- Responsabilidade
  - Pessoas perdem senhas
  - Sistemas criptográficos implicam em uma grande responsabilidade de guardar as chaves de forma segura e permanente por parte do usuário
  - Sem a chave privada, não há nada que possa ser feito por ninguém para recuperar o acesso

Como estamos contribuindo para o ecossistema: Financial Services 2.0

Quem faz parte da FS2

Gorilainvest.com.br

Iporangainvest.com

Bxchain.io

BxChain

- Projetos em blockchain para a próxima geraçao de serviços digitais

- H3
  - Plataforma de negociação de criptomoedas (H3.exchange)

- Abakate
  - Invista de graça! (Abakate.com.br)

- Legal Chain
  - Plataforma de notarização de documentos em blockchain (Legalchain.com.br)

Agradecimentos, dúvidas, contatos

- Agradecimento a todo a equipe de desenvolvimento da FS2!
- Agradecimento a FGV e EESP pela oportunidade
- Agradecimento ao publico

Contatos

www.fs2.com.br

contact@fs2.com.br

11-3074-0490