

Bitcoin: Sonho e Realidade

Jorge Stolfi

Instituto de Computação
Universidade Estadual de Campinas - UNICAMP

2018-08-16

Apresentada no Instituto de Economia, Unicamp
Campinas, SP - Brasil



Pré-história

Criptografia de chave pública e assinatura digital

Bitcoin

Sonho: Pagamento sem bancos

A revelação de Satoshi

Histórico das criptomoedas

Os pioneiros

Crime e especulação

Duas Bolhas e o Grande Colapso

A longa crise e a Ressureição

A Guerra do Block Size

Perspectivas

Bitcoin pode dar certo?

Investir em bitcoin?

Conclusões

Pré-história

Função de mão única

Função de mão única (Diffie-Hellman; ≈ 1976):

- ▶ Uma função f que é fácil de calcular mas difícil de inverter.
- ▶ Dado x , pode-se calcular $y = f(x)$ em tempo e custo razoável.
- ▶ Porém, dado y , não é viável encontrar um x tal que $f(x) = y$.

Exemplo:

- ▶ x é par (x_1, x_2) de primos, $y = f(x) = x_1 \times x_2$.
- ▶ Se x_1, x_2 tem 100 algarismos, calcular $y = f(x_1, x_2)$ é trivial.
- ▶ Dado y de 200 algarismos, encontrar x_1, x_2 é inviável.

Resumo criptográfico

Resumo (*hash*) criptográfico
(Diffie-Helman, Rabin; 1976–1979):

- ▶ Uma função de mão única h de textos arbitrários para cadeias de tamanho fixo.
- ▶ Dado um texto T de qualquer tamanho, pode-se calcular $H = h(T)$ rapidamente.
- ▶ O resumo H tem poucas centenas de bits.
- ▶ É “impossível” determinar um T com um dado H .
- ▶ É “impossível” modificar T sem alterar H .
- ▶ É “impossível” gerar dois textos T_1, T_2 com mesmo H .

Portanto: O resumo H identifica “unicamente” o texto T .

Resumo criptográfico (2)

Exemplo: SHA256 (resumo de 32 bytes)

▶ "Independencia ou Morte"

32af5a53 3fb57933 abb28758 9a24ab5d
f54da4a9 552b8489 f28bbd0b 669d1ac7

▶ "Independencia ou Marte"

0b0d462f ee7ace62 06999a77 e02e7b35
ebe19447 3de73fbd a1faf789 be73c19d

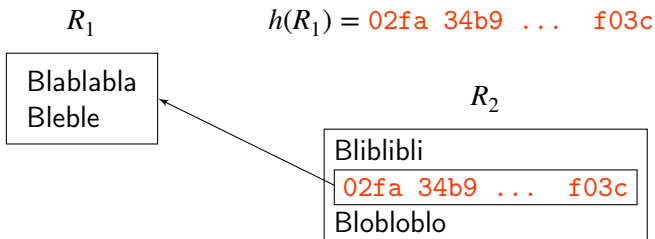
▶ "Se e para o bem de todos e felicidade geral
da Nacao, estou pronto! Digam ao povo que fico"

a72c93fd 0187fa7d 9ffa174a b05c95fa
7cd79cd2 b109d0da 36d16494 545d004b

Laço de Merkle

Laço (apontador, ponteiro, *link*) de Merkle
(Merkle, 1979):

O registro R_2 inclui o resumo H_1 do registro R_1 :



O laço de Merkle especifica R_1 pelo conteúdo, não pelo endereço.

Criptografia de chave pública

Criptografia de chave pública
(Diffie-Hellman, Rivest-Shamir-Adleman; 1974–1978):

- ▶ Duas chaves, pública B e privada V .
- ▶ Chaves B , V são geradas por Alice.
- ▶ Alice distribui só B .
- ▶ Beto quer mandar um texto T para Alice.
- ▶ Beto codifica o texto T com B .
- ▶ Beto manda o texto cifrado C para Alice.
- ▶ Alice decodifica C usando a chave V .

Criptografia de chave pública (2)

Propriedades do esquema:

- ▶ Cada chave tem algumas centenas de bits.
- ▶ É “impossível” que duas pessoas gerem a mesma chave.
- ▶ É “impossível” decodificar C sem a chave privada V .
- ▶ É “impossível” descobrir V dado B e T_i, C_j .

Portanto: Beto e Alice tem “certeza” de que ninguém vai ler T .

Assinatura digital

- ▶ Assinatura digital
(Goldwasser-Micali-Rivest e outros; 1979–1984):
 - ▶ Duas chaves, pública B e privada V .
 - ▶ Chaves B , V são geradas por Alice.
 - ▶ Alice distribui só B .
 - ▶ Alice quer publicar um texto T .
 - ▶ Alice calcula uma assinatura S usando T e V .
 - ▶ Alice publica o texto T e assinatura S .
 - ▶ Beto verifica a assinatura S usando T e B .

Assinatura digital (2)

Propriedades do esquema:

- ▶ Cada chave tem algumas centenas de bits.
- ▶ É “impossível” que duas pessoas gerem a mesma chave.
- ▶ É “impossível” criar a assinatura S para T sem saber V .
- ▶ É “impossível” descobrir V dado B e T_i, S_i .
- ▶ É “impossível” modificar T sem invalidar S .

Portanto: Beto tem “certeza” de que Alice escreveu T .

Bitcoin

Sonho: Pagamentos sem bancos

Pagamentos sem bancos

(acadêmicos, cypherpunks; 1985–2007):

- ▶ Chaves B_1 , V_1 são geradas por Alice para sua “conta”.
- ▶ Chaves B_2 , V_2 são geradas por Beto para sua “conta”.
- ▶ Alice quer mandar dinheiro para Beto.
- ▶ Alice junta ao cheque T_1 uma assinatura S_1 usando V_1 .
- ▶ Beto verifica a assinatura S_1 usando T_1 e B_1 .
- ▶ Beto quer usar esse dinheiro para pagar Clarice.
- ▶ Beto junta ao cheque T_2 uma assinatura S_2 usando V_2 .
- ▶ Clarice verifica a assinatura S_2 usando T_2 e B_2 .

Sonho: Pagamentos sem bancos (2)

Problemas:

- ▶ Verificar que o dinheiro existe: **fácil**
(base pública distribuída de cheques, cadeia de pagamentos).
- ▶ Verificar que Alice é a dona do dinheiro: **fácil**
(assinatura digital).
- ▶ Verificar que Alice ainda não gastou o dinheiro: **impossível?**
(problema dos Generais Bizantinos).

Cientistas perderam o interesse.

Cypherpunks continuaram sonhando.

A revelação de Satoshi

Bitcoin

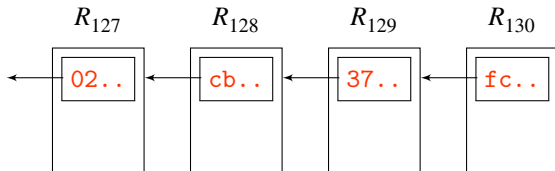
(Satoshi Nakamoto, 2008):

- ▶ Base pública distribuída de cheques **ordenados**.
- ▶ Comunidade de *mineradores* atualiza essa base.
- ▶ Mineradores são anônimos e voluntários.
- ▶ Usuários mandam “cheques” (*transações*) pros mineradores.
- ▶ Mineradores validam cheques e decidem a ordem.
- ▶ Mineradores votam com *prova de trabalho*.
- ▶ Todo mundo confia na maioria dos mineradores.
- ▶ Mineradores são recompensados com bitcoins.
- ▶ Minerador que não coopera só perde seu trabalho.

Blockchain

Cadeia de blocos do Bitcoin (*blockchain*):

- ▶ Lista de blocos R_1, R_2, \dots, R_n .
- ▶ Cada bloco contém um lote de cheques confirmados.
- ▶ Cada bloco contém um laço de Merkle para o anterior.



- ▶ Um novo bloco é acrescentado a cada 10 min em média.
- ▶ “Todo mundo” recebe, confere e guarda a lista toda.
- ▶ Se dois cheques conflitam, no máximo um é confirmado.

Portanto: Ninguém consegue gastar duas vezes o mesmo dinheiro.

Prova de trabalho

Prova de trabalho:

- ▶ Para cada bloco R_i existe uma *dificuldade* D_i
- ▶ Um bloco R_i só é válido se $h(R_i) < D_i$.
- ▶ Cada bloco tem um campo arbitrário X .
- ▶ Problema: encontrar X para satisfazer $h(R_i) < D_i$.
- ▶ Tem que ser por tentativa e erro.
- ▶ D_i é ajustada para que leve 10 minutos.
- ▶ Hoje exige 43×10^{18} tentativas por bloco.

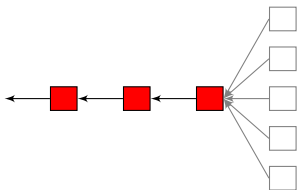
Mineração de bitcoins é o maior supercomputador do mundo
e o maior desperdício de computação do mundo:
10 milhões de USD/dia, 7.3GW.

Correção posterior à palestra: são 43×10^{18} tentativas por **segundo**, ou
 26×10^{21} por bloco, em média.

Mineração competitiva (1)

Mineração competitiva:

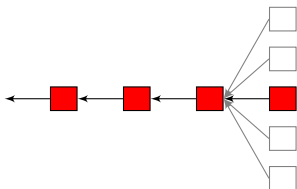
- ▶ Mineradores trabalham em *pools*.
- ▶ Cada pool monta um bloco candidato.
- ▶ Cada pool tenta resolver o quebra-cabeça do seu bloco.



Mineração competitiva (2)

Mineração competitiva:

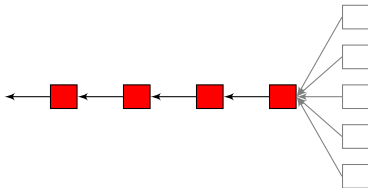
- ▶ Mineradores trabalham em *pools*.
- ▶ Cada pool monta um bloco candidato.
- ▶ Cada pool tenta resolver o quebra-cabeça do seu bloco.
- ▶ O primeiro que resolve publica o bloco e avisa os outros.



Mineração competitiva (3)

Mineração competitiva:

- ▶ Mineradores trabalham em *pools*.
- ▶ Cada pool monta um bloco candidato.
- ▶ Cada pool tenta resolver o quebra-cabeça do seu bloco.
- ▶ O primeiro que resolve publica o bloco e avisa os outros.
- ▶ Os outros imediatamente passam para o bloco seguinte.



É do interesse de cada minerador conferir a validade dos cheques e dos blocos minerados pelos outros.

Histórico das criptomoedas

Os pioneiros

2009–06/2010: Os pioneiros

- ▶ Satoshi minerou um milhão de bitcoins.
- ▶ Alguns cypherpunks adotaram.
- ▶ “Bitcoin vai acabar com governos e bancos.”
- ▶ Valor monetário irrisório.
- ▶ Primeira compra: duas pizzas por 10'000 BTC.

Crime e especulação (1)

07/2010–12/2010: Especulação

- ▶ Bolsa MtGOX (Mark Karpelès) começa a funcionar.
- ▶ Pessoas usam bitcoin para especular.
- ▶ Valor chega a 0.01 USD
- ▶ Mineração por lucro com GPUs.
- ▶ Criminosos “descobrem” bitcoin.
- ▶ Satoshi desaparece.

Crime e especulação (2)

2011–2012: Crimes e China

- ▶ Mercados “dark net” adotam bitcoin (Ross Ulbricht).
- ▶ Casinos online adotam bitcoin (Eric Vorheess).
- ▶ Primeira concorrente, Litecoin (Charlie Lee).
- ▶ Bolsa BTC-China abre em Xangai (Bobby Lee).
- ▶ Mineradores usam FPGAs e ASICs.
- ▶ Velha guarda do bitcoin cria rede de relays.
- ▶ Primeira grande bolha: preço chega a 15 USD/BTC.

Segunda bolha

01/2013–07/2013: A segunda bolha

- ▶ Milionários “descobrem” bitcoin (Andreessen, Winklevoss, ...).
- ▶ Preço chega a 200 USD.
- ▶ Várias outras bolsas aparecem pelo mundo.
- ▶ Bolsas OKCoin e Huobi abrem em Pequim.
- ▶ Governo dos EUA fecha Silk Road.

Terceira bolha e o grande colapso

08/2013–02/2014: Terceira bolha e o grande colapso

- ▶ Preço sobe a mais de 1100 USD (11/2013).
- ▶ Banco Central da China intervém.
- ▶ Preço desaba para 400 USD.
- ▶ Bolsa MtGOX admite “sumiço” de 600'000 BTC (400 M USD).

O ano da incerteza

03/2014–02/2015: O ano da incerteza

- ▶ Preço recupera para 800 USD.
- ▶ 400 M USD investidos em empresas de bitcoin.
- ▶ Empresa Blockstream é fundada, quer reformar bitcoin.
- ▶ Governo EUA leiloa bitcoins da Silk Road.
- ▶ Mineração é centralizada na China.
- ▶ Moedas alternativas (*altcoins*) proliferam.
- ▶ Ethereum e “smart contracts” (Vitalik Buterin).
- ▶ Preço decai gradualmente para 200 USD.

A grande depressão

03/2015–10/2015: A grande depressão

- ▶ Preço fica em 200 USD por 8 meses.
- ▶ Uso de bitcoin no comércio não “pega”.
- ▶ As *altcoins* continuam crescendo.
- ▶ Rede bitcoin fica saturada com “spam”.
- ▶ Bancos ficam interessados em “tecnologia blockchain”.

A quarta bolha e o grande racha

11/2015–11/2017: A quarta bolha e o grande racha

- ▶ Ransomware explode graças a bitcoin.
- ▶ Ethereum vira veículo de golpes financeiros (DAO, ICOs).
- ▶ Congestão da rede causa explosão de tarifas e demora.
- ▶ CVM dos EUA rejeita criação de fundo de Bitcoin.
- ▶ Novos mercados: Japão, Coreia do Sul, Índia.
- ▶ Bitcoin racha em duas moedas, BTC e BCH (08/2017).
- ▶ Preço cresce sem parar e chega a 22'000 USD (11/2017).

O novo colapso

12/2017–08/2018: O novo colapso

- ▶ Preço de BTC cai para 6000 USD.
- ▶ Todas as criptomoedas caem 70%.
- ▶ Bitcoin perde prestígio para outras moedas.
- ▶ Índia reprime criptomoedas.
- ▶ Interesse por tecnologia blockchain esfria.

A Guerra do Block Size

Cronograma da guerra

2013–2016: Guerra fria

- ▶ **2013**: Gavin Andresen propõe aumentar tamanho dos blocos.
- ▶ **02/2013**: Greg Maxwell propõe rede de dois níveis.
- ▶ **2014**: Blockstream é fundada (70 M USD).
- ▶ **10/2014**: Proposta “sidechains”.
- ▶ **2014–2015** Blockstream assume controle de Core.
- ▶ **2015**: proposta do Lightning Network (Poon, Dryja).
- ▶ **11/2015**: Blockstream propõe SegWit.
- ▶ **2015**: Comunidade racha em pro e contra Blockstream.

2017: Bitcoin racha em duas moedas

- ▶ Blockstream tenta forçar adoção de suas mudanças (SegWit).
- ▶ Dissidentes propõem mudança alternativa (SegWit2X).
- ▶ Amaury Séchet propõe rachar a moeda (BitcoinABC).
- ▶ **08/2017**: Moeda racha em Bitcoin-Core (BTC) e Bitcoin-Cash (BCH).
- ▶ Mineradores oscilam entre BTC e BCH.
- ▶ **11/2017**: Reforma de BCH encerra oscilação.
- ▶ Preço de BCH estabiliza em ≈ 0.1 BTC

Perspectivas

Não tem conserto à vista

Não há perspectivas de que criptomoedas:

- ▶ tenham essas falhas consertadas.
- ▶ cumpram seus objetivos iniciais.
- ▶ sejam adotadas em escala significativa.
- ▶ sejam úteis para alguma coisa.
- ▶ sejam regulamentadas e legalizadas.

Quem ganha com criptomoedas?

Quem ganha:

- ▶ Mineradores (10 milhões de USD por dia).
- ▶ Fabricantes de equipamento de mineração (2 bilhões de USD).
- ▶ Bolsas de criptomoedas (tarifas e fraudes).
- ▶ Fundos de bitcoin (tarifas e sobrevalorização).
- ▶ Serviços diversos (tarifas)
- ▶ Golpes e fraudes.
- ▶ Empresas de bitcoins.
- ▶ Criminosos (traficantes, sonegadores, hackers, ...).
- ▶ Alguns “investidores” e traders.

Quem perde com criptomoedas?

Quem perde:

- ▶ Maioria dos “investidores” e traders ($\gg 10$ milhões USD/dia).
- ▶ Investidores de “venture capital”.
- ▶ Vítimas de fraudes, ransomware.

Sobrevivencia não prova valor

“Mas já não é um sucesso?”

- ▶ Preço prova apenas que há quem compra por esse preço.
- ▶ Quanto mais durar, mais os investidores vão perder.
- ▶ Quanto mais o preço subir, mais rápido eles vão perder.
- ▶ Porque continuam existindo:
 - ▶ Única opção para pagamentos ilegais via internet.
 - ▶ Muita gente está ganhando muito dinheiro.
 - ▶ Tecnologia é complexa e potencial difícil de avaliar.
 - ▶ Sucesso comercial prometido para “algum dia”.

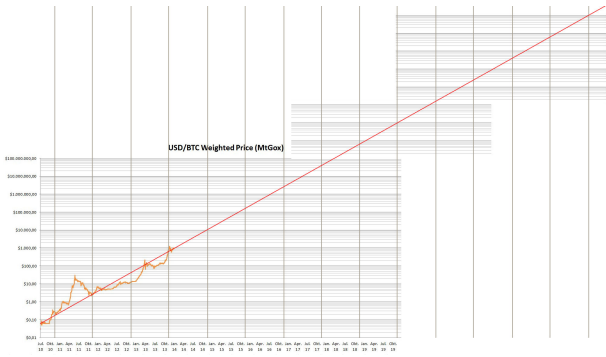
Conclusões

Conclusões:

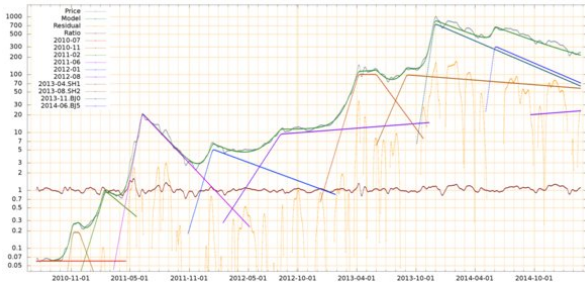
- ▶ Tecnicamente, bitcoin é muito interessante...
- ▶ Mas ainda não resolveu o problema original!
- ▶ Ainda sobrevive por razões erradas.
- ▶ Concorrência crescente de outras criptomoedas.
- ▶ Concorrência de sistemas centralizados.
- ▶ Fundamentalmente ilegal.
- ▶ Investimento é fraude financeira.
- ▶ Blockchain é fraude tecnológica.



(CC) BY-ND



Price bubbles - 2010-06-20 to 2015-03-10 (smoothed with 15-day Hann window)



Relative prices - 2012-11-20 to 2014-03-10 (smoothed with 7-day Hann window)

