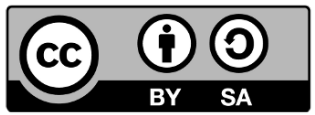
Bitcoin: Sonho e Realidade

Jorge Stolfi

Departamento de Ciênca da Computação
Universidade Estadual de Campinas - UNICAMP

2017-09-06

Seminários do IC-UNICAMP
Campinas, SP - Brasil



Pré-história:

- **1974–1978**: Criptografia de chave pública (Diffie-Hellman, Rivest-Shamir-Adleman):
  - Duas chaves, pú**b**lica B e pri**v**ada 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.

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_i.

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

- **1979-1984**: Assinatura digital (Goldwasser-Micali-Rivest e outros):
  - Duas chaves, pú**b**lica B e pri**v**ada V.
  - Chaves B, V são geradas por Alice.
  - Alice distribui só B.
  - Alice quer publicar un 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.

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.

- **1985–2007**: Sistemas decentralizado de pagamentos (acadêmicos, cypherpunks):
  - Duas chaves, pú**b**lica B e pri**v**ada V.
  - 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.

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).

Centistas perderam o interesse.

Cypherpunks continuaram sonhando.

- **2008**: Bitcoin (Satoshi Nakamoto):
  - Base pública distribuída de cheques **ordenados**.
  - Comunidade de *mineradores* atualiza essa base.
  - Usuários mandam "cheques" (*transações*) pros mineradores.
  - Mineradores validam cheques e decidem a ordem.
  - Mineradores votam com *prova de trabalho*.
  - Mineradores são recompensados com bitcoins.
  - Mineradores lucram mais cooperando do que fraudando.
  - Todo mundo confia na maioria dos mineradores.

Resumo (*hash*) criptográfico:

- Função que dado um texto T devolve um resumo $h(T) = H$.
- O resumo H tem algumas dúzias 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.

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

- Registo R_2 inclui o resumo H_1 do registro R_1:

R_1

Blablabla Bleble

$h(R_1) =$ `02fa 34b9 ... f03c`

R_2

Bliblibli
`02fa 34b9 ... f03c`
Bloblo

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

Cadeia de blocos do Bitcoin (*blockchain*):

- Lista de blocos $R_1, R_2, \ldots, R_n$.
- 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

- 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 $600 \times 6 \times 10^{18}$ tentativas por bloco.

Mineração de bitcoins é o maior supercomputador do mundo (e o maior desperdício de computação do mundo).

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 consegue publica o bloco e avisa os outros.
- Os outros imediatamente passsam para o bloco seguinte.

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

- **2009–06/2010**: Satoshi e os cypherpunks:
  - 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.

- **07/2010–12/2010**: Crime e especulação:
  - Bolsa MtGOX (Mark Karpelès) começa a funcionar.
  - Pessoas usam bitcoin para especular.
  - Criminosos "descobrem" bitcoin.
  - Valor chega a 0.01 USD
  - Mineração por lucro com GPUs.
  - Satoshi desaparece.

- **2011–2012**: Mais crime e especulação:
  - 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.
  - Valor chega a 15 USD/BTC.

- **2013**: A grande bolha e o grande colapso:
  - Milionários "descobrem" bitcoin (Andreessen, Winklevoss, ...).
  - Várias outras bolsas aparecem pelo mundo.
  - Bolsas OKCoin e Huobi abrem em Pequim.
  - Governo dos EUA fecha Silk Road.
  - Preço sobe a mais de 1100 USD/BTC (Nov/2013).
  - Banco Central da China intervém.
  - Preço desaba, recupera em parte.

- **2014**: Fim das “certezas”
  - Bolsa MtGOX admite“sumiço” de 600’000 BTC (400 M USD).
  - Preço decai de 800 para 250 USD/BTC.
  - 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 contracst” (Vitalik Buterin).

- **2015**: Ano da crise
  - Preço fica em 200 USD/BTC quase todo ano.
  - Uso de bitcoin no comércio não “pega”.
  - As *altcoins* continuam crescendo.
  - Rede bitcoin fica saturada com “spam”.
  - Bancos ficam interessados em “tecnologia blockchain”.

- **2016–2017**: Ressureição
  - 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, Coréia do Sul, Índia.
  - Preço tem outra "bolha" (quase 5000 USD/BTC).

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

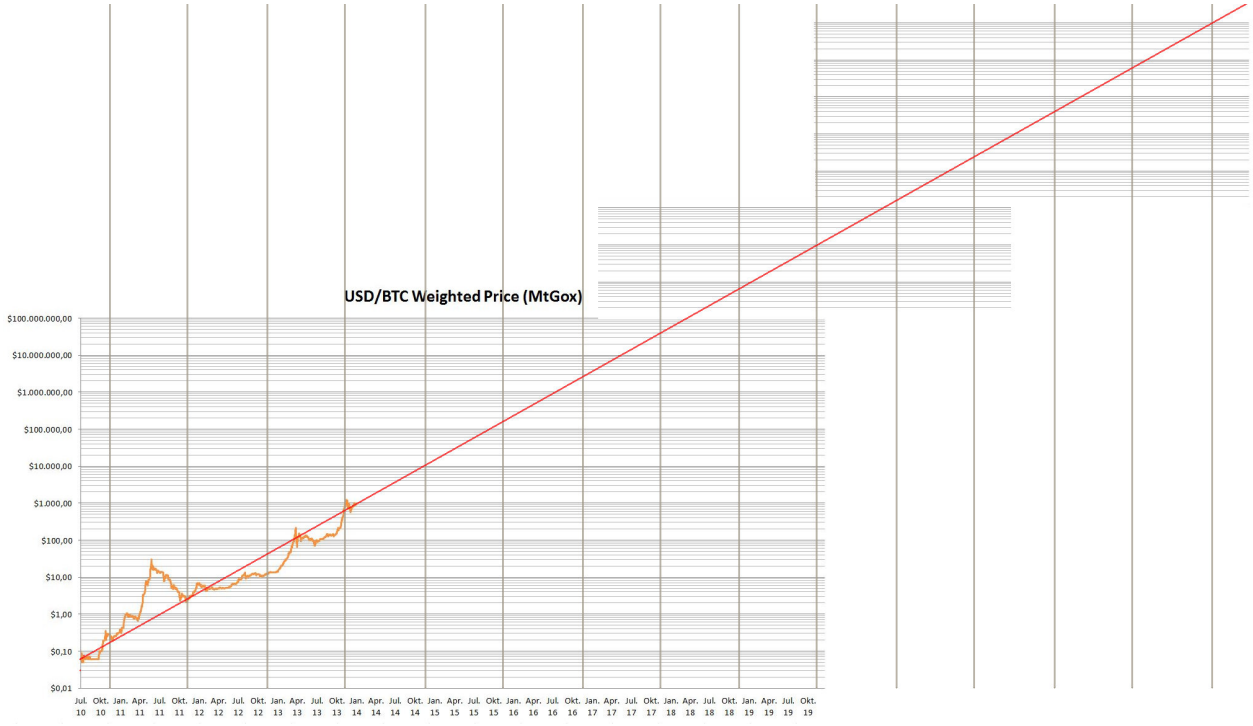
- **2017**: Bitoin racha
  - Blockstream tenta forçar adoção de suas mudanças (SegWit).
  - **08-01**: Moeda racha em Bitcoin-Core (BTC) e Bitcoin-Cash (BCH).
  - Mineradores oscilam entre BTC e BCH.
  - **11-18**: Moeda deve rachar de novo (SegWit2X).

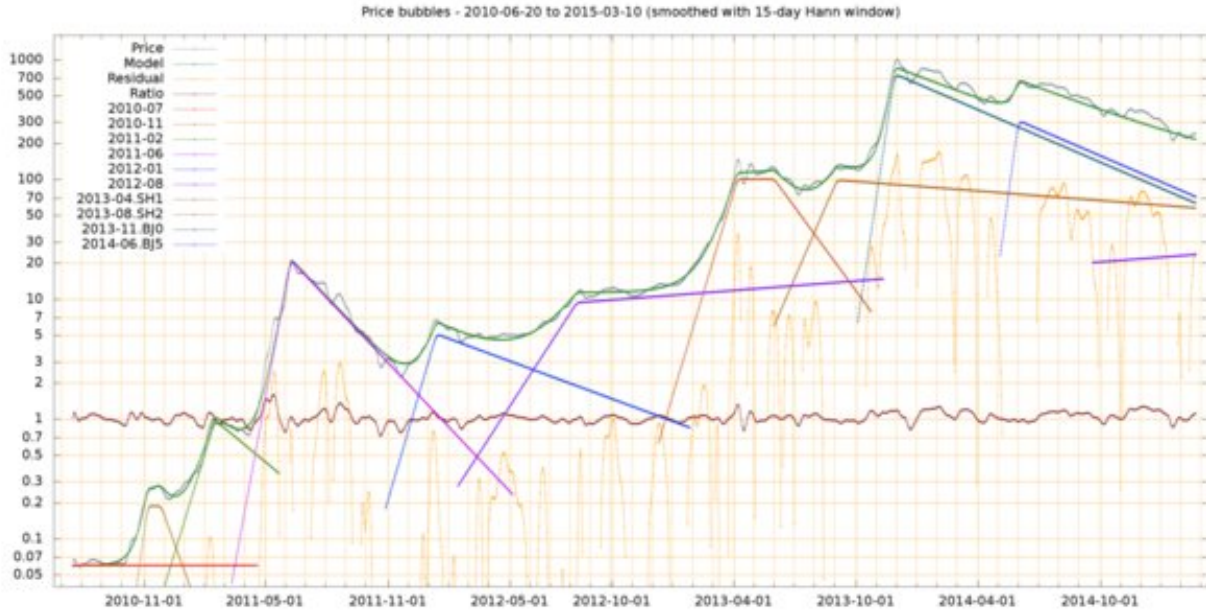
Bitcoin vai dar certo?

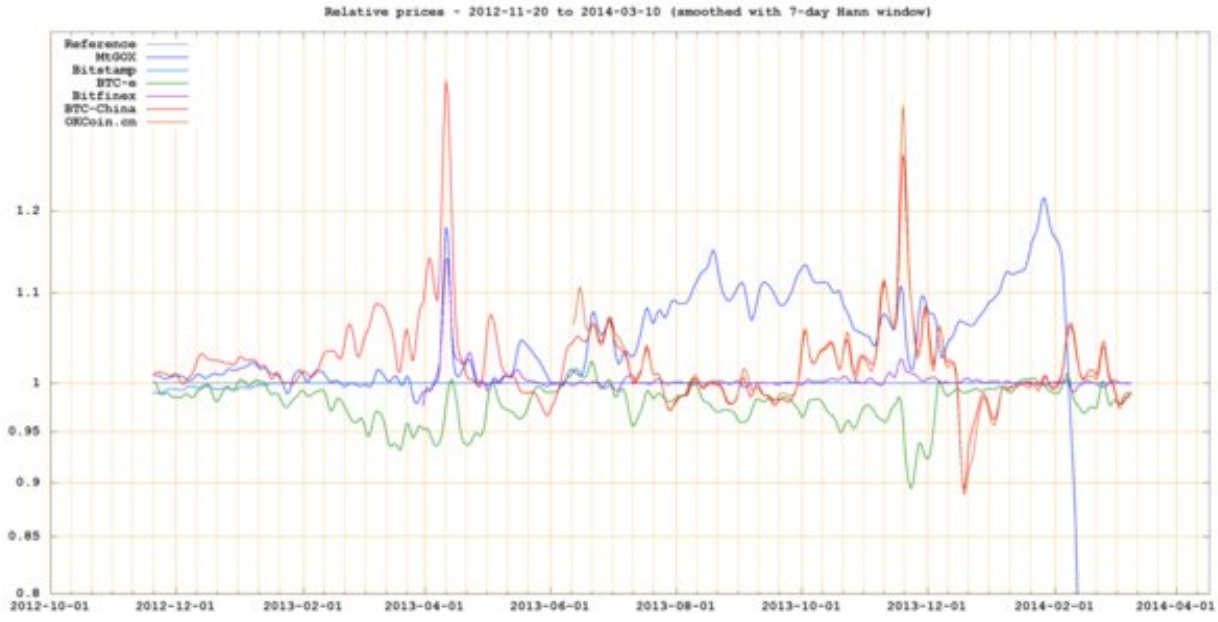
- Cadeia de blocos é muito grande.
- Mineração é muito cara.
- Tempo de confirmação é muito longo e variável.
- Mineração será inevitavelmente concentrada.
- Decentralização só tem vantagem para crimes.
- Falta de inflação gera volatilidade.
- Volatilidade impede uso como moeda.
- Posse ficou muito concentrada.
- Falta governança para evolução.

Mas já não é um sucesso?

- Preço prova apenas que há quem compra por esse preço.
- Razões para sobrevivência:
  - Única opção para pagamentos ilegais via internet.
  - Muita gente está ganhando muito dinheiro.
  - Tecnologia é complexa e potencial difícil de avaliar.
  - Sucesso comercial não tem data prevista.


USD/BTC Weighted Price (MtGox)
$100.000.000,00
$10.000.000,00
$1.000.000,00
$100.000,00
$10.000,00
$1.000,00
$100,00
$10,00
$1,00
$0,10
$0,01
Jul. 10
Okt. 10
Jan. 11
Apr. 11
Jul. 11
Okt. 11
Jan. 12
Apr. 12
Jul. 12
Okt. 12
Jan. 13
Apr. 13
Jul. 13
Okt. 13
Jan. 14
Apr. 14
Jul. 14
Okt. 14
Jan. 15
Apr. 15
Jul. 15
Okt. 15
Jan. 16
Apr. 16
Jul. 16
Okt. 16
Jan. 17
Apr. 17
Jul. 17
Okt. 17
Jan. 18
Apr. 18
Jul. 18
Okt. 18
Jan. 19
Apr. 19
Jul. 19
Okt. 19


Price bubbles - 2010-06-20 to 2015-03-10 (smoothed with 15-day Hann window)
Price
Model
Residual
Ratio
2010-07
2010-11
2011-02
2011-06
2012-01
2012-08
2013-04.SH1
2013-08.SH2
2013-11.BJ0
2014-06.Bj5
1000
700
500
300
200
100
70
50
30
20
10
7
5
3
2
1
0.7
0.5
0.3
0.2
0.1
0.07
0.05
2010-11-01
2011-05-01
2011-11-01
2012-05-01
2012-10-01
2013-04-01
2013-10-01
2014-04-01
2014-10-01


Relative prices - 2012-11-20 to 2014-03-10 (smoothed with 7-day Hann window)
Reference
MtGOX
Bitstamp
BTC-e
Bitfinex
BTC-China
OKCoin.cn
1.2
1.1
1
0.95
0.9
0.85
0.8
2012-10-01
2012-12-01
2013-02-01
2013-04-01
2013-06-01
2013-08-01
2013-10-01
2013-12-01
2014-02-01
2014-04-01

Quem ganha:

- Mineradores (8 milhões de USD por dia).
- Fabricantes e vendedores de equipamento de mineração.
- 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:

- Maioria dos “investidores” e traders ($\gg$8 milhões USD/dia).
- Investidores de “venture capital”.
- Vítimas de fraudes, ransomware.

Investir em Bitcoin?

- Bitcoins não tem valor intrínseco.
- Bitcoins não representam propriedade de nada.
- Bitcoins não tem consumidores finais.
- **Bitcoins não existem.**
- Todo lucro de um investidor é perda de outro.
- Mineradores tem lucro (bilhões de USD).
- Total de perdas vai ser maior que total de lucros.
- Lucro esperado é negativo.
- Colapso é inevitável mas imprevisível.
- Não tem receita para lucrar.

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.
- Crise de governança.


BELIEVED IN BITCOIN LOST EVERYTHING
HEY BRO! CAN YOU SPARE A DOGE?
T-STOLK
03-2014