Universidade de São Paulo
Instituto de Ciências Matemáticas e de Computação

Estudo sobre Bitcoin: escalabilidade da blockchain

Elias Italiano Rodrigues
elias.rodrigues@usp.br

20 de junho de 2016
São Carlos – SP, Brasil

Sumário

- Introdução
  - Motivação
  - Objetivos do Projeto
- Bitcoin e Criptomoedas
- Escalabilidade da Blockchain
  - Principais Implementações: Core, Classic, Unlimited
  - Tamanho Máximo do Bloco: Fee Market
  - Inovações para Escalabilidade: SegWit, Lightning Network
- Conclusão

Introdução

- **Motivação**:
  - O Bitcoin surgiu de maneira privada e independente;
  - Descentralizou e desestatizou a moeda;
  - Teve **adoção voluntária** e consequente valorização;
  - 2009-2011:
    - pequeno grupo de hackers e entusiatas;
    - 1 BTC = entre zero e poucas dezenas de reais [1];
  - 2012-2016:
    - interesse mundial de empresas e governos;
    - 1 BTC ~ R$ 2.900,00 [2].

Introdução

- **Motivação**:
  - Tecnologia com grande potencial disruptivo;
  - Sistemas distribuídos, P2P; Escola Austríaca de Economia;
  - Maior inovação em TI desde a criação da Internet;
  - Ou seria apenas mais um “hype” dos tecnologistas? Veremos nas próximas décadas.

Introdução

- **Objetivos do Projeto**:
  - Estudar o cenário atual sobre Bitcoin e criptomoedas;
  - Aprender sobre as tecnologias envolvidas;
  - Entender o problema da escalabilidade da blockchain;
  - Contribuir como material em português.

Bitcoin e Criptomoedas

- **Criptomoeda**:
  - Moeda digital e sistema de pagamento online;
  - P2P, *open-source* e descentralizada;
  - Baseada em técnicas de criptografia.
- **Bitcoin**:
  - Primeira criptomoeda de sucesso;
  - Criada pelo anônimo cientista Satoshi Nakamoto em 2008 [3]; colocada em operação em janeiro de 2009.

Bitcoin e Criptomoedas

- **Endereço**:
  - *Hash* de uma chave pública;
  - chave privada → chave pública → *hash()* → endereço
  - Ex: 17NJGu7kMncocFEKfLDwmGwvTSgPjMqpHF
- **Carteira**:
  - Guarda chaves privadas;
  - Gerencia o conjunto de endereços;
  - Confere saldos, cria, assina e envia transações.

Bitcoin e Criptomoedas

- **Blockchain**:
  - Banco de dados público do histórico das transações;
  - Cada nó da rede possui uma cópia idêntica;
  - Estrutura de dados em que blocos são ligados por ponteiros *hash*;
  - Cada bloco contém um conjunto de transações assegurados por uma Merkle Tree (árvore *hash*).

Bitcoin e Criptomoedas

- **Mineração**:
  - Processo que emite novas unidades da moeda (recompensa por bloco);
  - Adiciona blocos à blockchain;
  - Valida e consolida as transações (recebendo taxas);
  - Define o consenso sobre a blockchain;
  - Poder computacional protege a rede contra fraudes.

Escalabilidade da Blockchain

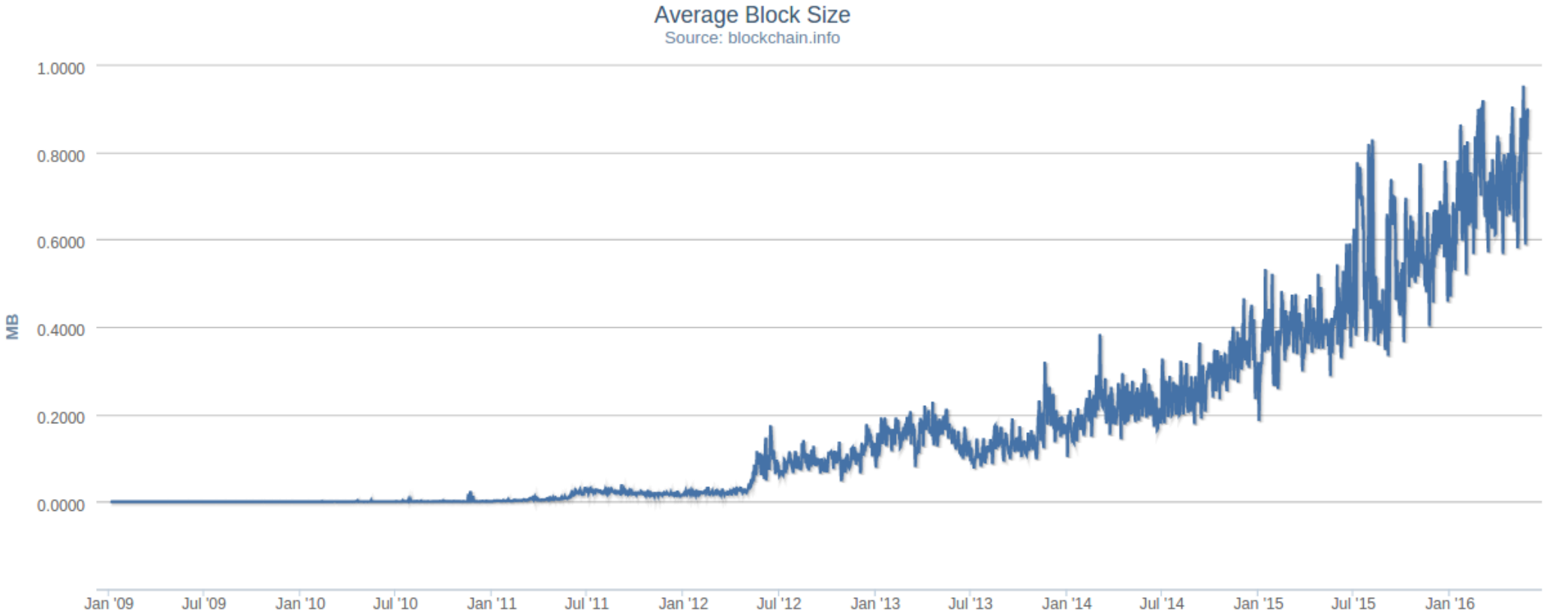
- Atualmente, problema de escalabilidade:
  - Liquidez está estagnada a uma pequena circulação;
  - *Blocksize limit* (1 MB) e intervalo (10min) **≈ 7 tx/s**;
  - Comparação: Visa Inc. máximo de 56000 tx/s [4].

Escalabilidade da Blockchain

- **Fato**: aprimoramentos tecnológicos não são suficientes para aumentar a escalabilidade:
  - Lei de Moore ainda é satisfatória;
  - Logo, são necessárias **mudanças no protocolo**.

Escalabilidade da Blockchain

- **Fato**: blocos cada vez mais cheios* [5].



Fonte: https://blockchain.info/charts/avg-block-size

* **e** existe uma atividade econômica

Principais Implementações

- **Bitcoin Core**:
  - Cliente de referência;
  - 1 MB *blocksize limit;*
  - Desenvolvedores experientes;
  - Atualmente, a implementação mais executada pelos mineradores (~ 80%) [6].

Principais Implementações

- **Bitcoin Classic**:
  - 2 MB *blocksize limit*;
  - Governança: decisões em modelo de votação entre as entidades envolvidas;
  - Tem crescido e ganhado suporte de importantes desenvolvedores e de empresas.
  - Atualmente, a segunda implementação mais executada pelos mineradores (~ 14%) [6].

Principais Implementações

- **Bitcoin Unlimited**:
  - Liberdade: Bitcoin deve ser o que os seus usuários definem pelo código que escolhem executar;
  - Configurações facilitadas: cada minerador pode escolher o *blocksize limit* que deseja;
  - Atualmente, a terceira implementação mais executada pelos mineradores (~ 2%) [6].

Tamanho Máximo do Bloco

- **Fee Market**:
  - Proposta por Peter R. Rizun [7];
  - Não deve existir um *blocksize limit*: ele será melhor definido pelo mercado de taxas de transação;
  - **Proposição**: um minerador racional toma decisões quanto as transações e o *blocksize* para maximizar o seu lucro e minimizar o seu prejuízo;

Tamanho Máximo do Bloco

- **Fee Market**:
  - Equação do lucro do minerador:

Lucro = (Recompensa + *Fees*) * (*hashPower* / *hashPower*Rede) *** (1 - $P_{orfão}$)**

  - **Objetivo**: maximizar a equação;
  - **Porém,** quanto maior o *blocksize*, maior o $P_{orfão}$.
  - **Logo**, buscar pelo melhor *blocksize*.

Tamanho Máximo do Bloco

- **Fee Market**:
  - Curva *fee* por bloco:
    - O minerador ordena sua *mempool* de acordo com a densidade das transações (*fee*/byte).
  - Curva custo por bloco:
    - Caso neutro: bloco vazio* ;
    - Serve como comparação para determinar até que ponto compensa inserir transações no bloco ou quais transações deve-se inserir.

* existência de uma recompensa por bloco

Tamanho Máximo do Bloco

- **Fee Market**:
  - Existe um mercado:
    - Caso contrário não existiria uma rede, não existiriam mineradores investindo recursos.
  - O tamanho do bloco será finito:
    - Fisicamente infactível um bloco infinito;
    - Existe prejuízo por um bloco muito grande.
  - Um mercado de taxas de transações surgirá.

Inovações para Escalabilidade

- **SegWit**:
  - Apresentado por Pieter Wuille [8];
  - Somente nós completos de validação precisam de todas assinaturas (~60% da *blockchain*);
  - Separar as assinaturas das transações;
  - Otimização de espaço => melhor aproveitamento do *blocksize*;
  - A mais factível de ser implementada em breve.

Inovações para Escalabilidade

- **Lightning Network**:
  - Proposta por Joseph Poon e Thaddeus Dryja [9].
  - Canais de pagamentos *off-blockchain*;
  - A e B criam um “canal” com respaldo na *blockchain* e por meio desse canal várias transações podem ser executadas;
  - Indo além: uma camada de canais de pagamentos em cima da rede de Bitcoin;
    - Usuários mantém uma pequena quantidade de canais abertos formando uma rede de pagamentos;
    - Torna-se possível o roteamento de pagamentos pelos canais existentes;

Conclusão

- Bitcoin **é** Unlimited:
  - *Open-source* + Consenso => Unlimited;
  - Conforme a oferta de profissionais capacitados na área aumentar, isso se tornará mais evidente.
- Unlimited => livre mercado => sem *blocksize limit* ;
- SegWit + Lightning Network + demais soluções:
  - Para resolver o atual problema de escalabilidade;
  - Vale lembrar que escalabilidade é um **problema recorrente.** A Internet é um exemplo disso.

Referências

[1] BITCOIN HISTORY. The Complete History of Bitcoin [Timeline]. 2016. Disponível em: <http://historyofbitcoin.org>. Acesso em: 16 jun. 2016.

[2] Disponível em: <http://exchangewar.info/coinprice?BTC_BRL>. Acesso em: 17 jun. 2016.

[3] NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 17 jun. 2016.

[4] Disponível em: <https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf>. Acesso em: 16 jun. 2016.

[5] Disponível em: <https://blockchain.info/charts/avg-block-size>. Acesso em: 27 mai. 2016.

[6] Disponível em: <https://coin.dance/nodes> e <http://nodecounter.com>. Acesso em 27 mai. 2016.

[7] RIZUN, P. R. A Transaction Fee Market Exists Without a Block Size Limit. 2015. Disponível em: <https://scalingbitcoin.org/papers/feemarket.pdf> e <https://www.youtube.com/watch?v=ad0Pjj_ms2k>. Acesso em: 27 mai. 2016.

[8] WUILLE, P. Segregated Witness for Bitcoin. Disponível em: <https://prezi.com/lyghixkrguao/segregated-witness-and-deploying-it-for-bitcoin> e <https://www.youtube.com/watch?v=fst1IK_mrng&t=37m12s>. Acesso em 30 mai. 2016.

[9] POON, J.; DRYJA, T. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. 2016. Disponível em: <https://lightning.network/lightning-network-paper.pdf> e <https://www.youtube.com/watch?v=8zVzw912wPo>. Acesso em: 30 mai. 2016.

Obrigado pela atenção!