Criptomoedas após o *hype*

Rafael Bianchini Abreu Paiva

Bacharel em economia (Unicamp) e Direito (USP).
Mestre e Doutorando em Direito Comercial (USP).
Analista do Banco Central

Maio.2019

Disclaimer

As afirmações e ideias contidas nesta apresentação são opiniões do expositor e de sua exclusiva responsabilidade, não representado a opinião oficial do Banco Central do Brasil (BCB)

Programação

I. Tecnologia

II. Visão geral

III. Criptomoedas como meio de pagamento

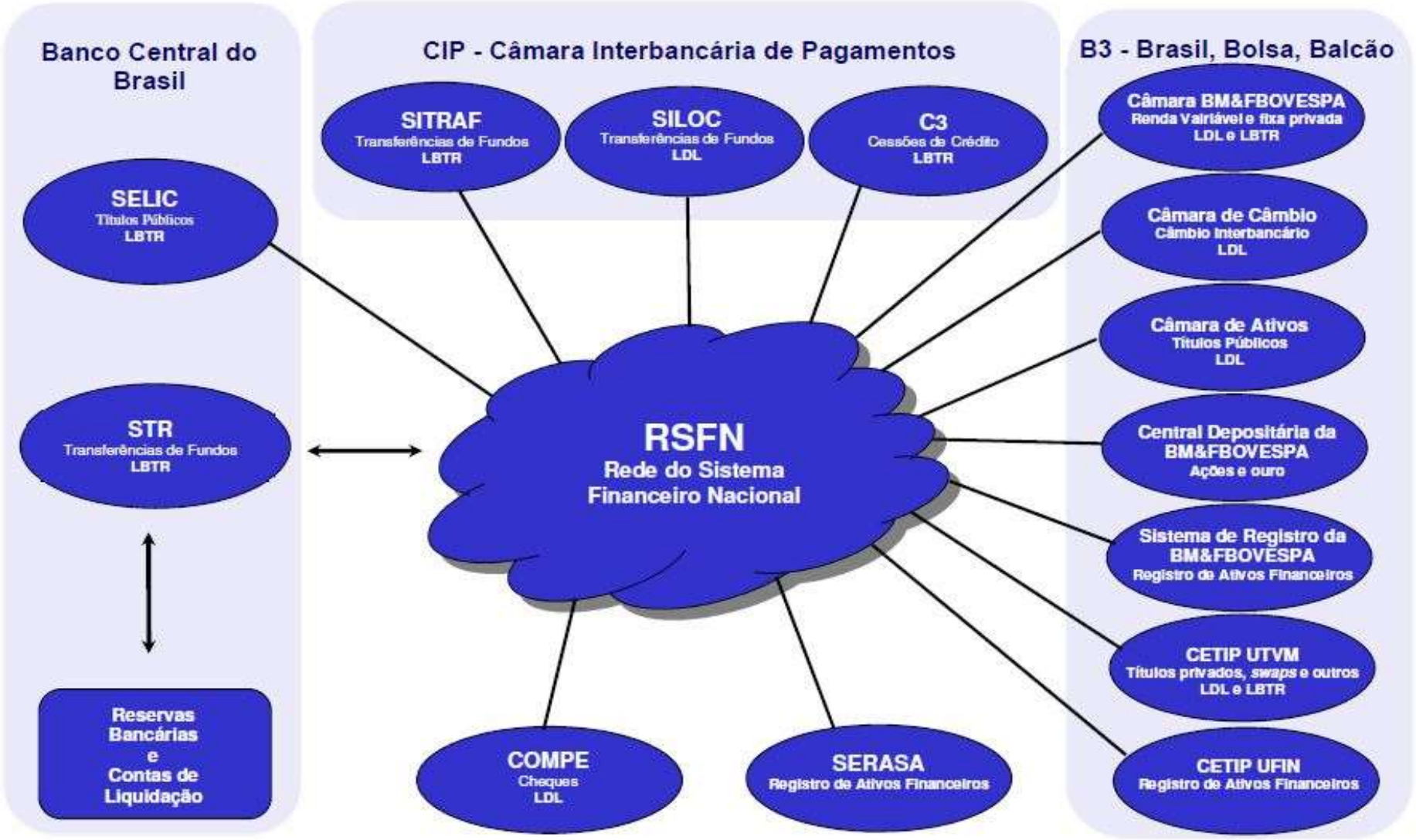
IV. Criptomoedas como alternativa de investimento

V. China

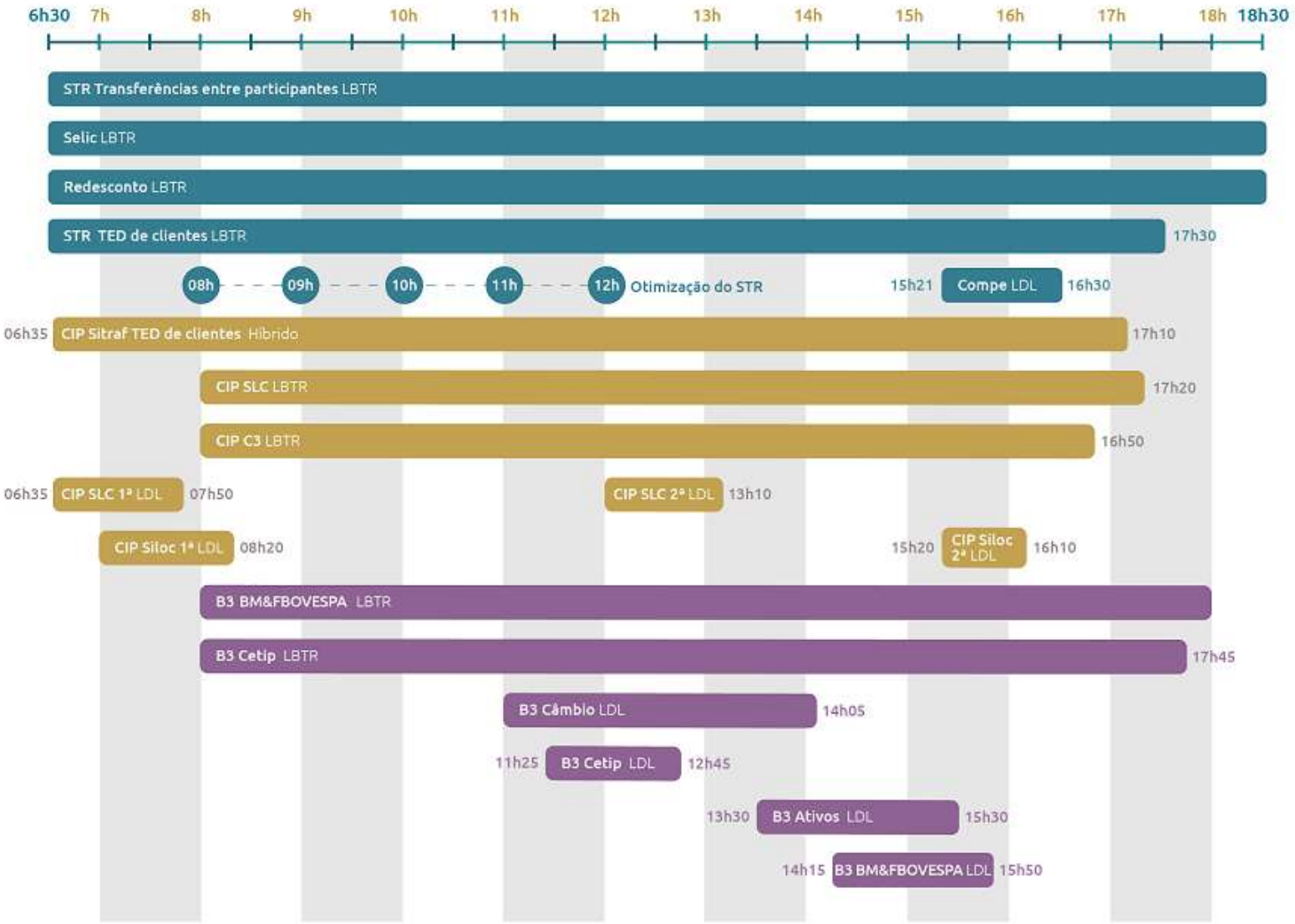
I. A tecnologia
Sistema de pagamentos

- **Meio circulante (papel moeda e moedas metálicas): transações anônimas e entre partes (*peer-to-peer*, P2P)**
  - **Entidade emissora: Estado**
  - **Riscos e custos de armazenamento**
  - **Acessível a pessoas sem acesso à internet e ao Sistema Financeiro**
- **Sistema de Pagamentos Brasileiro (SPB): transações performadas por bancos, infraestruturas do mercado financeiro e/ou arranjos de pagamentos**
  - **Sigilo garantido pelos intermediários envolvidos, de acordo com Lei Complementar 105/2001**
  - **Liquidação pelo saldo multilateral ou pelo valor bruto**
  - **Em geral, eletrônicas, mas ainda há uso de documentos físicos (p. ex. cheques)**
  - **Alguns tipos de transações têm limites de horários**
  - **Conversibilidade na moeda estatal**

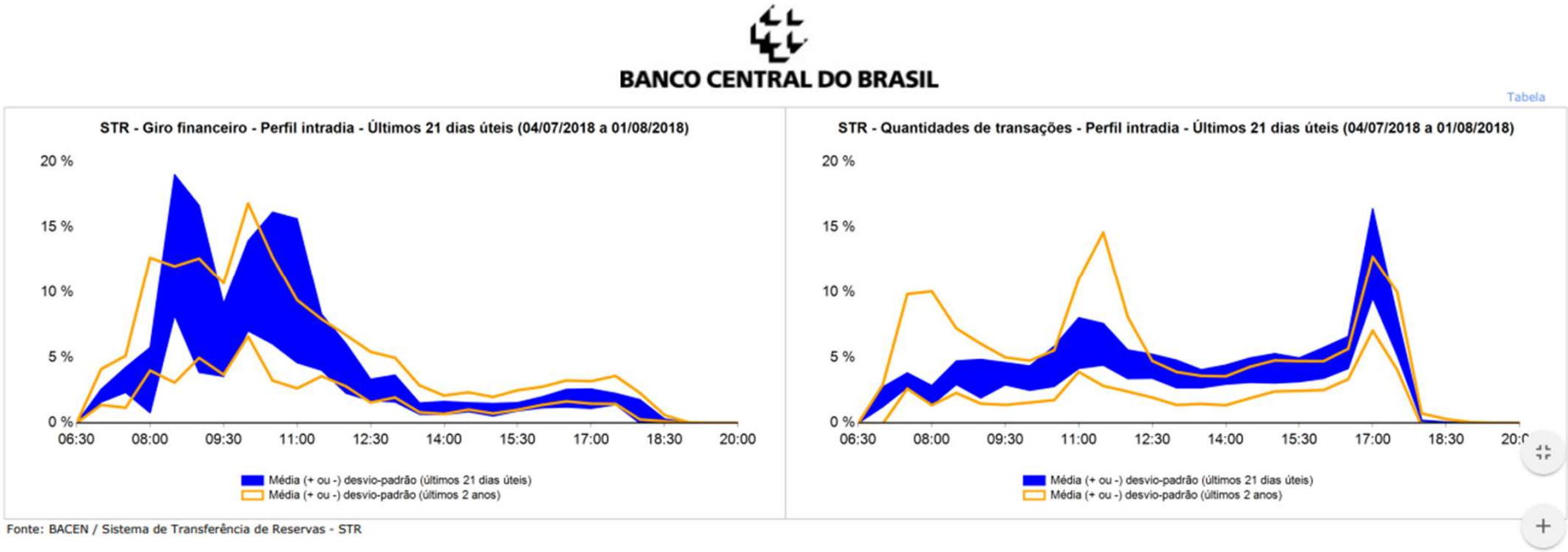
I. A tecnologia
Visão geral do SPB



I. A tecnologia
Grade do STR



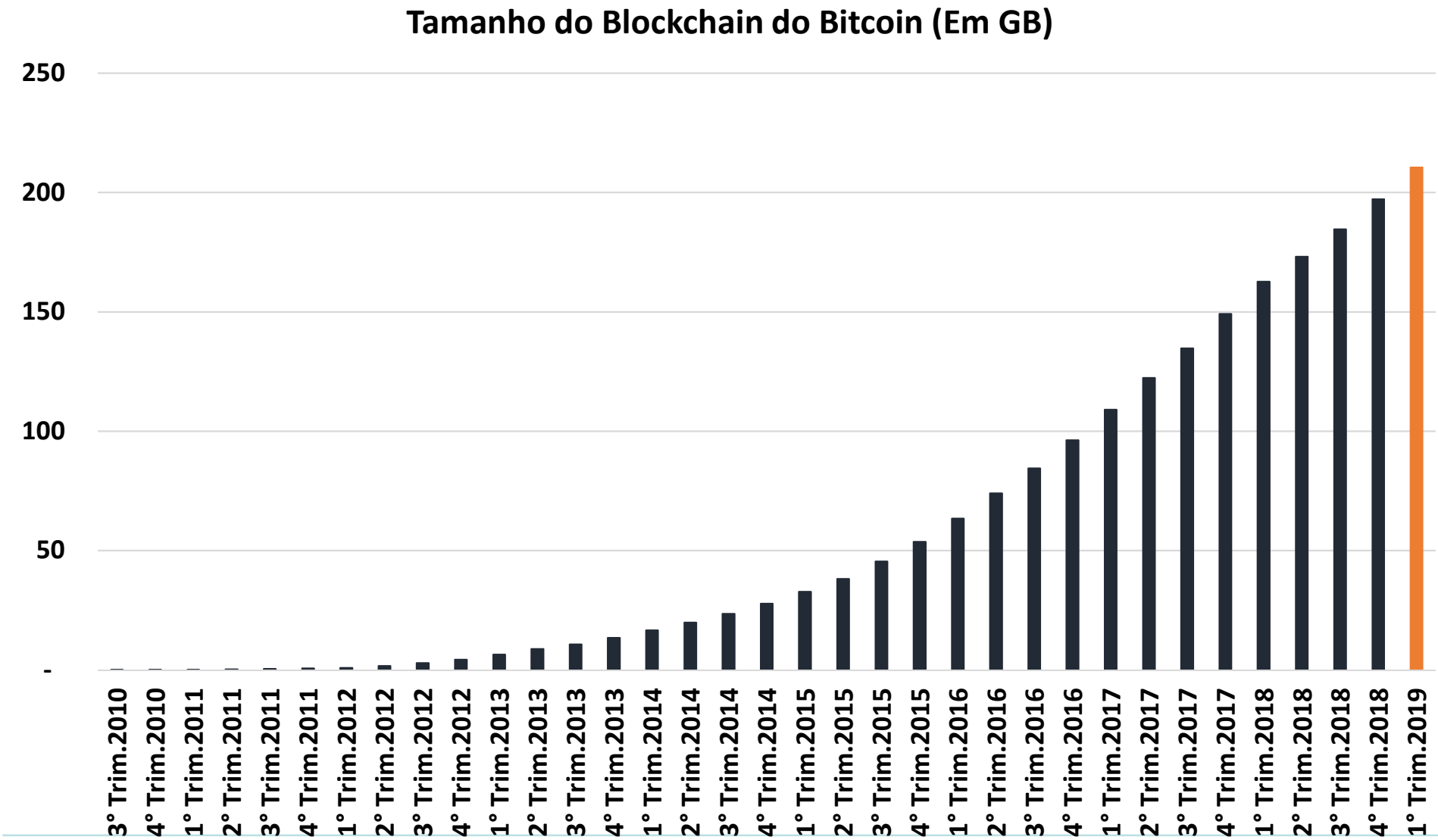
I. A tecnologia STR



STR: Média diária (2018) > R$ 1,4 trilhão e 310 mil operações em grade de 12X5 (7,2/segundo)

- **Criptomoedas**
  - Acesso universal
  - Totalmente eletrônicas
  - Ausência de emissor*
  - Liquidação descentralizada*
  - Diretamente entre partes (*Peer-to-peer*, P2P)*
  - Transações públicas, identidades (chaves públicas) anônimas
  - Identificação de pares de transações em vez de endereços individuais: p. ex: A-B = 1, A-C = 2, A-D = 4, A-E = 5, B-C = 6, B-D = 7, B-E = 8, C-D = 9, C-E = 10
  - Semi-anonimato
  - BCB considerou tecnologia inviável para operar como contingência do Sistema de Transferências de Reservas (STR) por infringir sigilo bancário

- Criptografia: segurança e integridade das transações (pagador, recebedor, valor)
- "Carimbos do Tempo": verificação precisa e confiável da data e hora em que um determinado documento foi assinado ou produzido
  - Sem entidade certificadora de carimbos de tempo
- Armazenamento distribuído entre "nós" da rede – *Distributed Ledger Technology* (DLT)
- Novas transações adicionadas a um bloco de transações (blockchain), transações antigas compactadas
  - Baixa necessidade de armazenamento
- Validação descentralizada baseada em incentivos dos participantes (nós)


Tamanho do Blockchain do Bitcoin (Em GB)
250
200
150
100
50
-
3° Trim.2010
4° Trim.2010
1° Trim.2011
2° Trim.2011
3° Trim.2011
4° Trim.2011
1° Trim.2012
2° Trim.2012
3° Trim.2012
4° Trim.2012
1° Trim.2013
2° Trim.2013
3° Trim.2013
4° Trim.2013
1° Trim.2014
2° Trim.2014
3° Trim.2014
4° Trim.2014
1° Trim.2015
2° Trim.2015
3° Trim.2015
4° Trim.2015
1° Trim.2016
2° Trim.2016
3° Trim.2016
4° Trim.2016
1° Trim.2017
2° Trim.2017
3° Trim.2017
4° Trim.2017
1° Trim.2018
2° Trim.2018
3° Trim.2018
4° Trim.2018
1° Trim.2019

- **Prova de trabalho: um CPU, um voto**
  - Validação de transações por nós na rede
  - Integridade quando mais da metade das CPUs é honesta
  - Participantes competem por inserir novo bloco à cadeia de transações
  - Identificação da "resposta certa" por tentativa e erro
  - Bloco validado é adicionado à cadeia e transmitido à rede
  - Bloco mais longo é o verdadeiro
  - Garante elevado grau de segurança contra *hackers*
  - Recompensa: novas unidades e tarifas

- **Transparência nas transações a todos os participantes (nós) e "imutabilidade"**
  - Tecnicamente mutável, mas probabilidade tende a zero

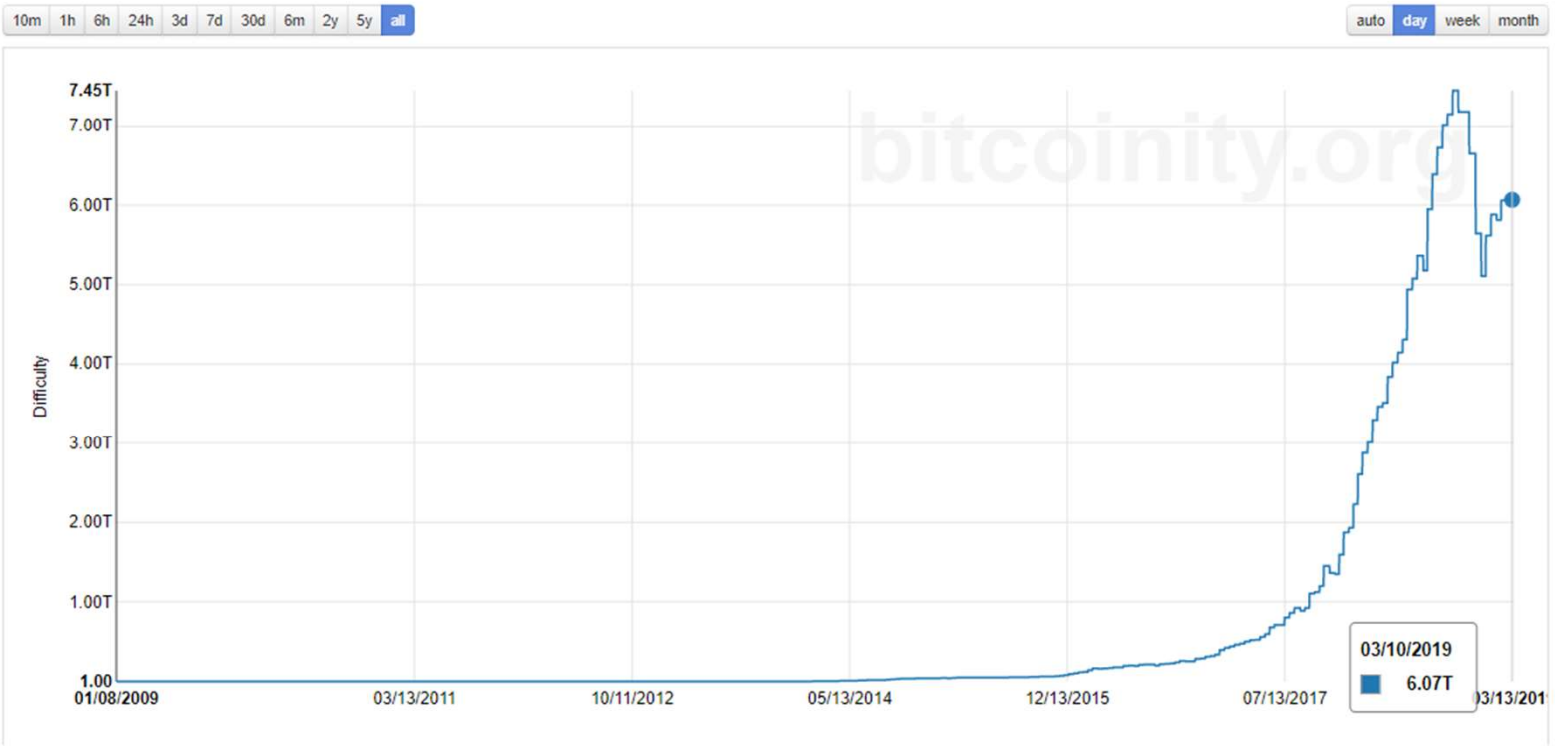
I. A tecnologia
Dificuldade de mineração (2008 =1)

data.bitcoinity.org (beta version)

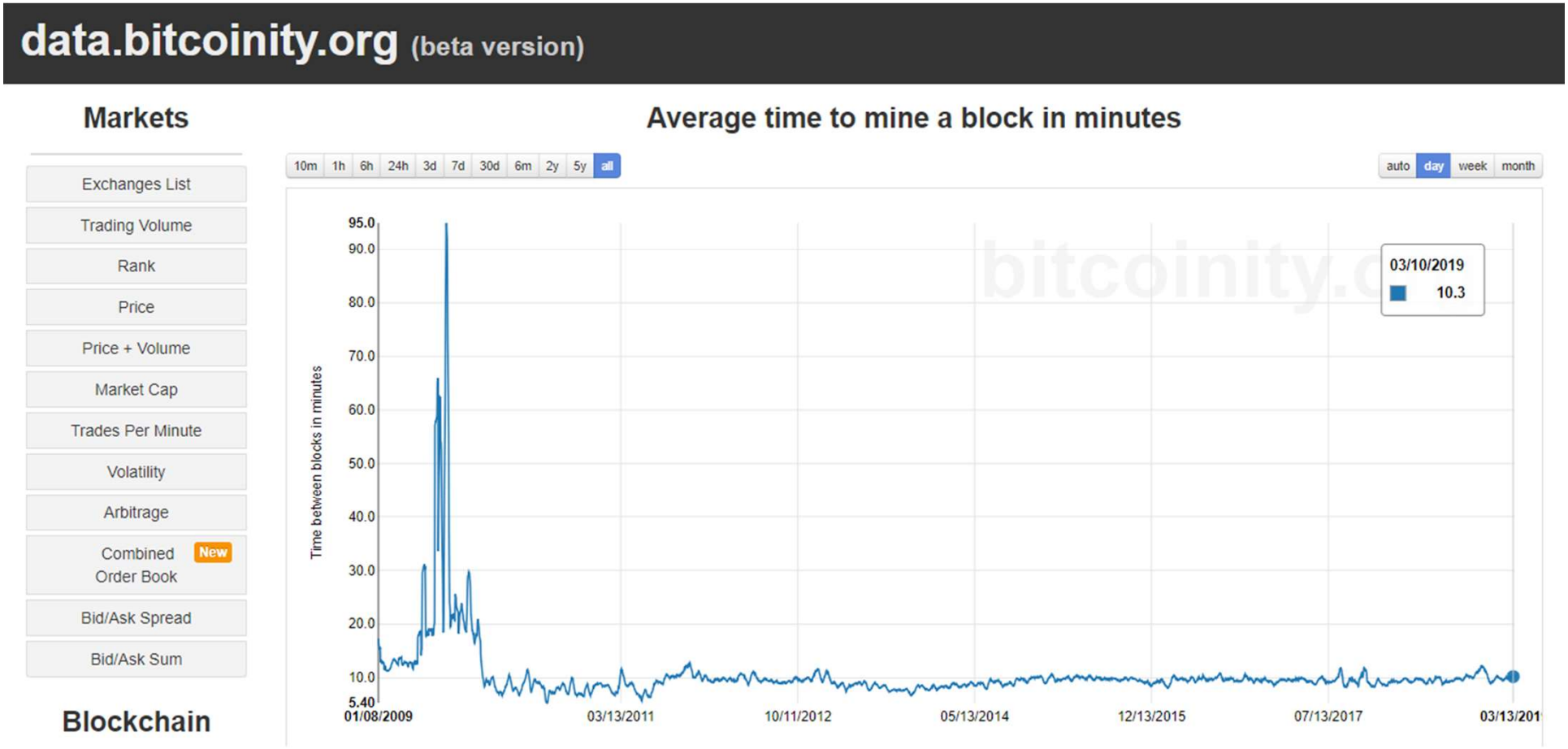
Markets

- Exchanges List
- Trading Volume
- Rank
- Price
- Price + Volume
- Market Cap
- Trades Per Minute
- Volatility
- Arbitrage
- Combined Order Book (New)
- Bid/Ask Spread
- Bid/Ask Sum

Blockchain



I. A tecnologia
Tempo de processamento de um bloco



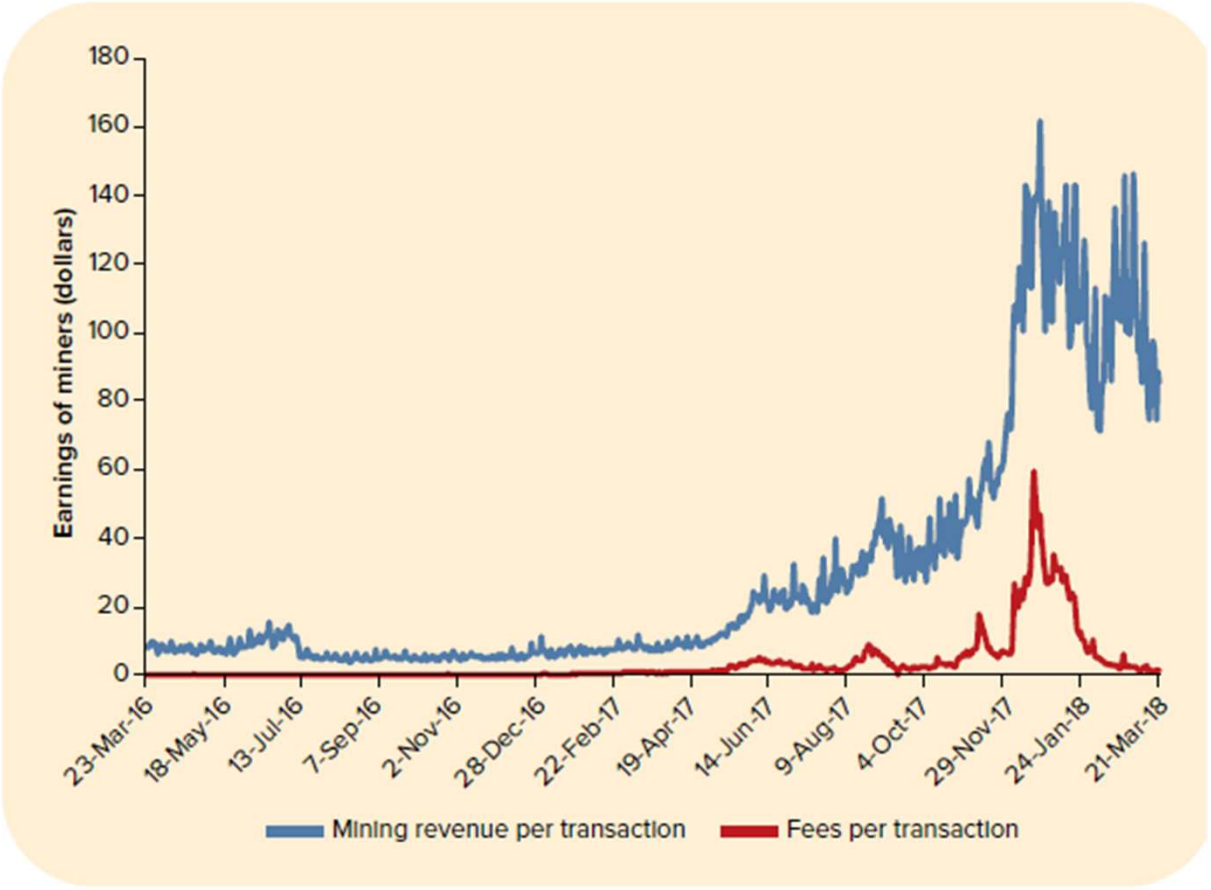
Bloco ≈ 2 mil transações

- **Protocolos**
  - Oferta inicial – ICO (Vide Itens II e IV)
  - Regras de emissão com ou sem limite quantitativo absoluto
  - Bitcoin: limite de 21 milhões de unidades (Em 2019 > 17,6 milhões)

- **Incentivo para criação de novas unidades**
  - Remuneração por CPU e energia consumidos
  - Similar à mineração
  - Desincentiva hackers

- **Quando não houver mais unidades a serem criadas, tarifas**

FIGURE 2.3 Most mining revenue comes from the seignorage (block reward) of the network



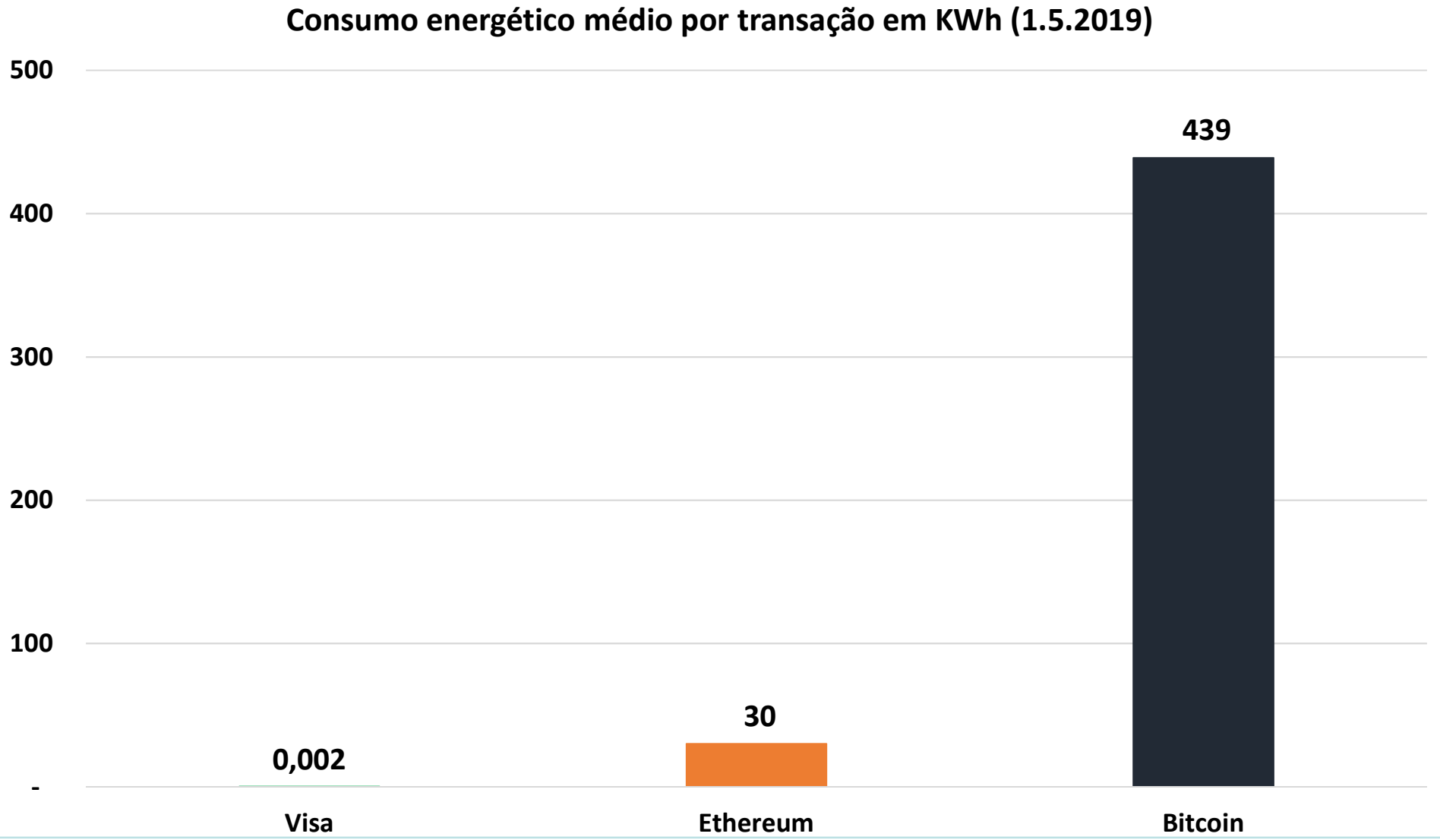
Source: blockchain.info.

I. A tecnologia
Da prova de trabalho à prova de conceito

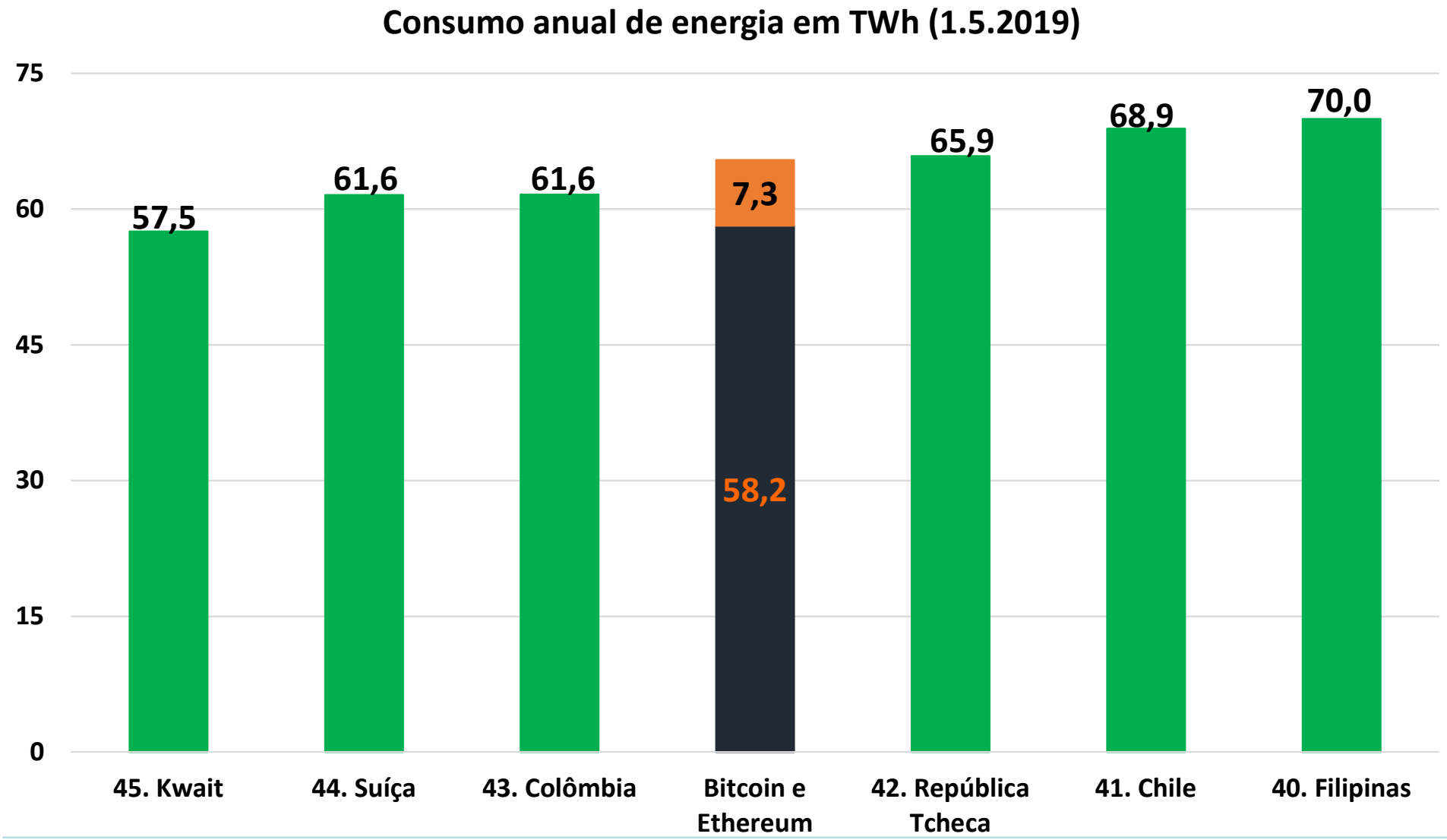
- **Prova de trabalho (Bitcoin): elevado consumo de energia e dificuldade de escalabilidade**
  - Blocos: em média 2 mil transações
  - Tempo de processamento dos blocos > 9 minutos
  - Dificuldade ajustada periodicamente

- **Prova de conceito (Ethereum): menor consumo de energia**
  - Eleição de bloco em função da quantidade de moedas próprias que o participante adiciona ao bloco
  - Eleição probabilística – participantes mais ricos com maior probabilidade de aceitação
  - Análogo a colocar recursos próprios em garantia para performar transações e ganhar comissões
  - Movimento em direção à intermediação

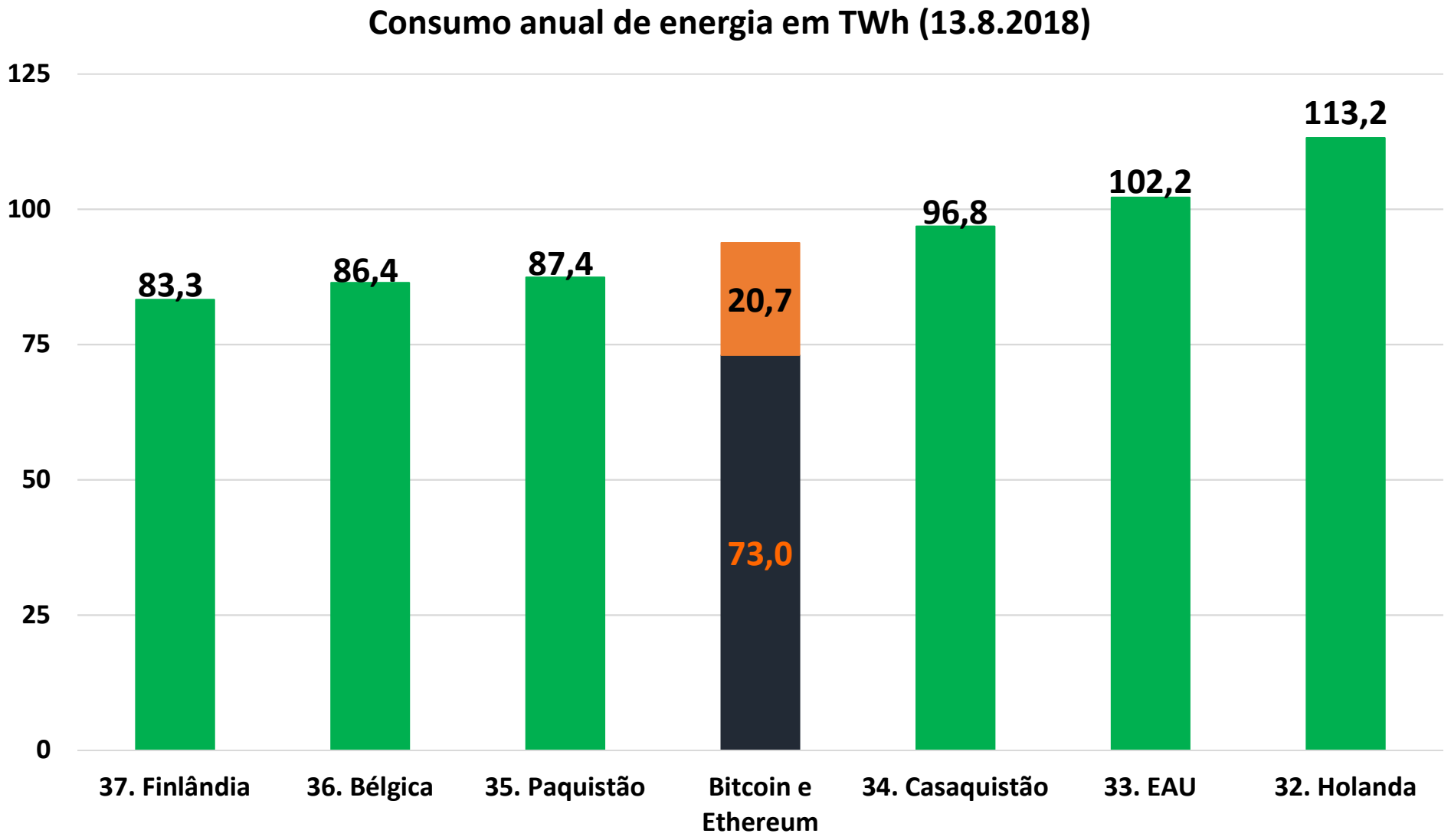
I. A Tecnologia
Consumo energético por transação



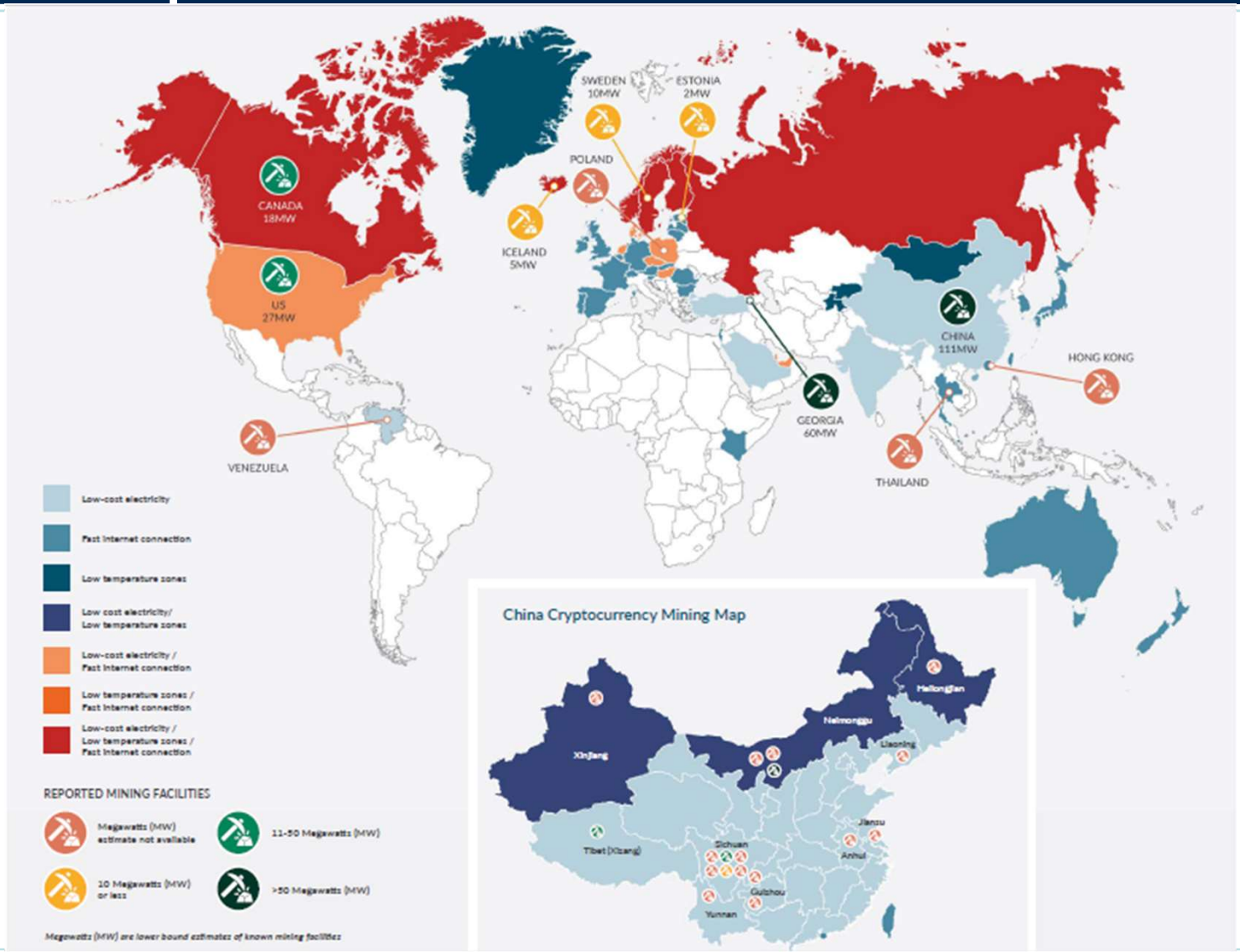
I. A Tecnologia
Consumo energético da mineração



I. A Tecnologia
Consumo energético da mineração



I. A Tecnologia
Geografia da mineração



I. A Tecnologia
Impacto da mineração na Geórgia

Consumo de energia elétrica na Geórgia: KWh per capita

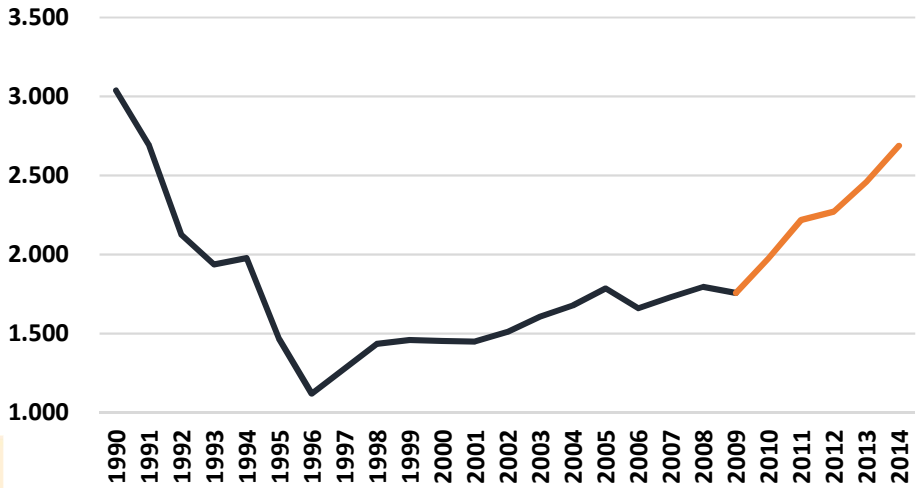
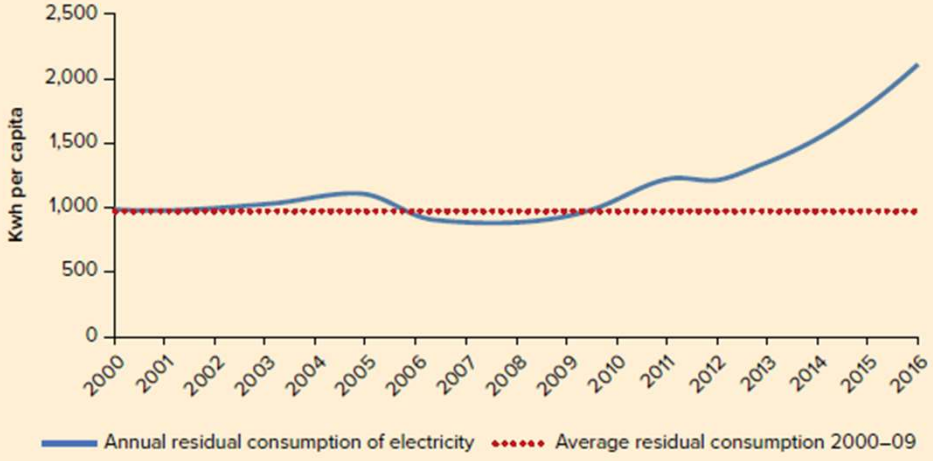


FIGURE B2.3.2 Unexplained electricity demand in Georgia has risen rapidly since 2009



Source: Data for 2000–14 are from World Development Indicators and the International Energy Agency. Data for 2015 and 2016 are from Georgia's energy services company.

- ***Blockchain*** **restrito a um número restrito de participantes (Ripple)**
  - **Reintroduz intermediários**

- ***Lightning network***
  - **Contratos inteligentes**
  - **Rede descentralizada**
  - **Pequenos pagamentos agrupados**
  - **Benefício: maior escalabilidade do Bitcoin**
  - **Maior risco**

a) Meio de pagamento

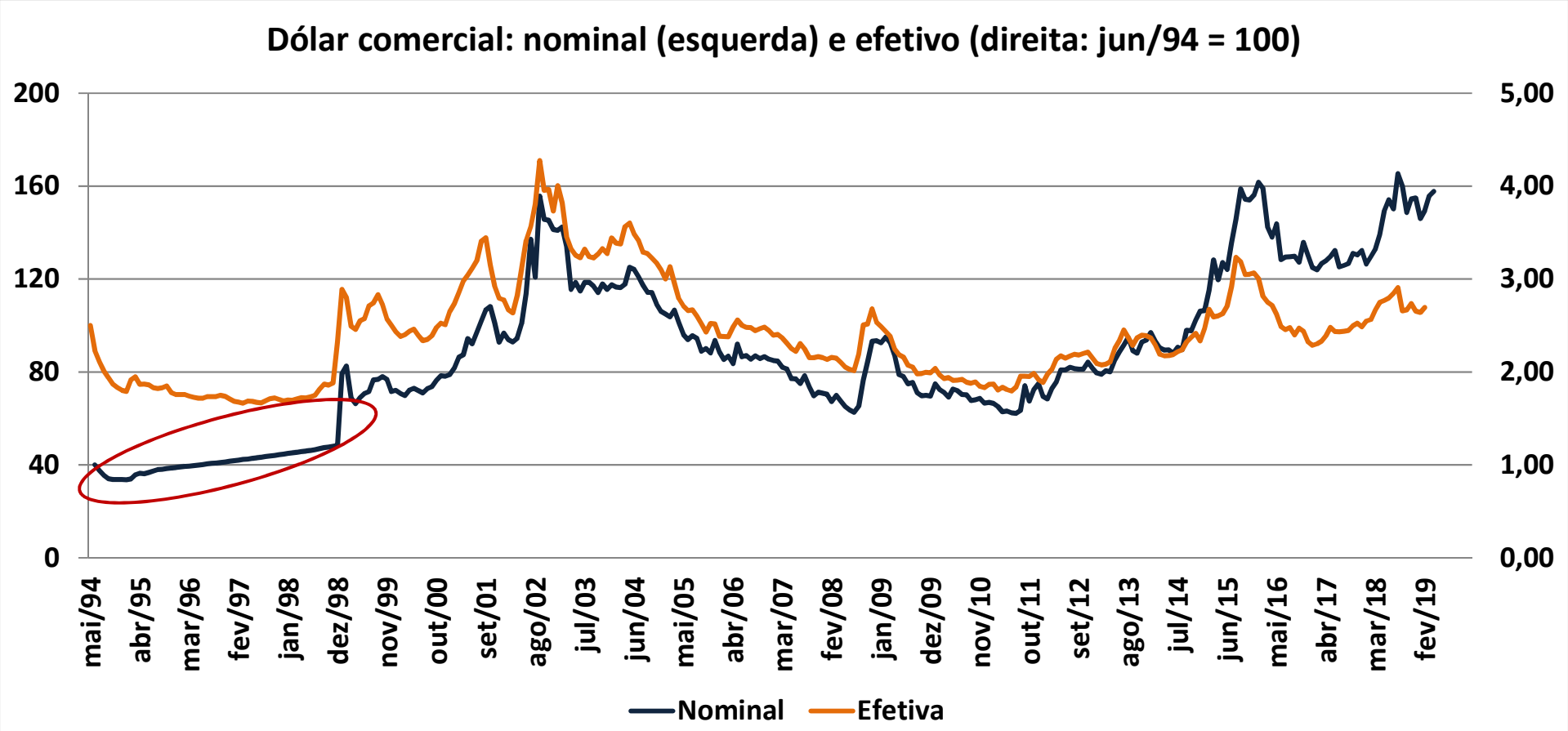
- Decreto-Lei 857/69 c/c Lei 9.069/95, art. 1º: curso forçado do Real
- CTN, art. 162: pagamento de tributos em Real
- Criptomoedas: aceitação voluntária – 200 mil varejistas em jul/18

b) Unidade de conta

- Lei 9.069/95, art. 5º: Real como unidade de conta para *"(...) demonstrações contábeis e financeiras, os balanços, os cheques, os títulos, os preços, os precatórios, os valores de contratos e todas as demais expressões pecuniárias que se possam traduzir em moeda nacional."*
- *Criptomoedas: Ineficiência da descoberta de preços em uma economia baseada em Bitcoins – Vídeo Porta dos Fundos*

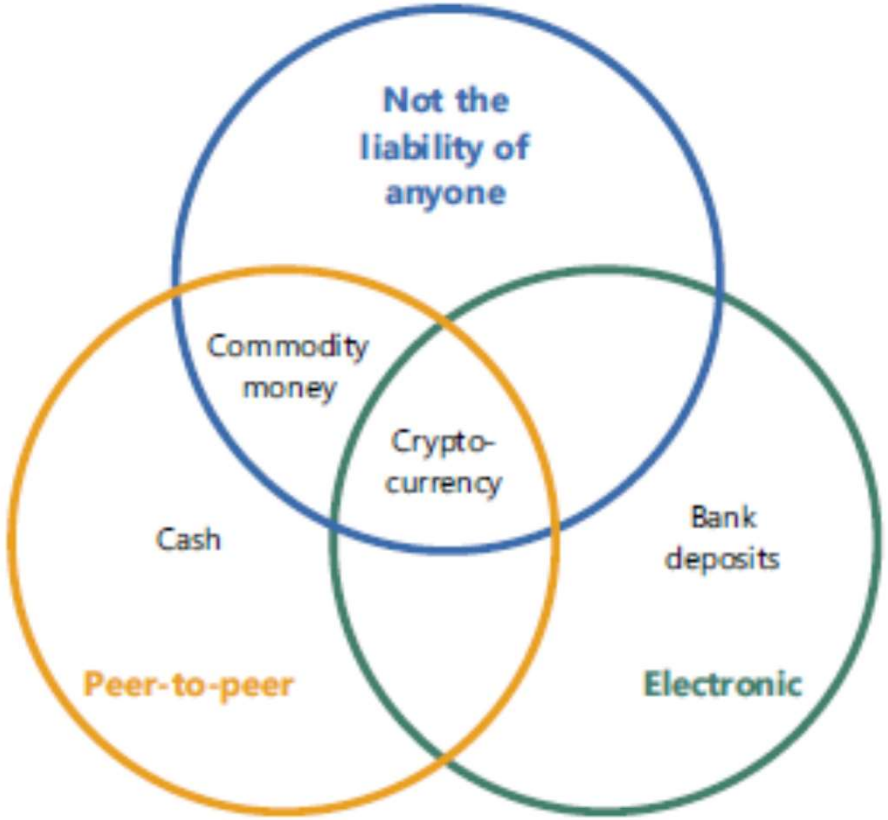
c) Reserva de valor (jul/1994 a jan/1999)

- Lei 9.069/95, arts. 3º e 4º - lastro em reservas e regras de emissão do Real

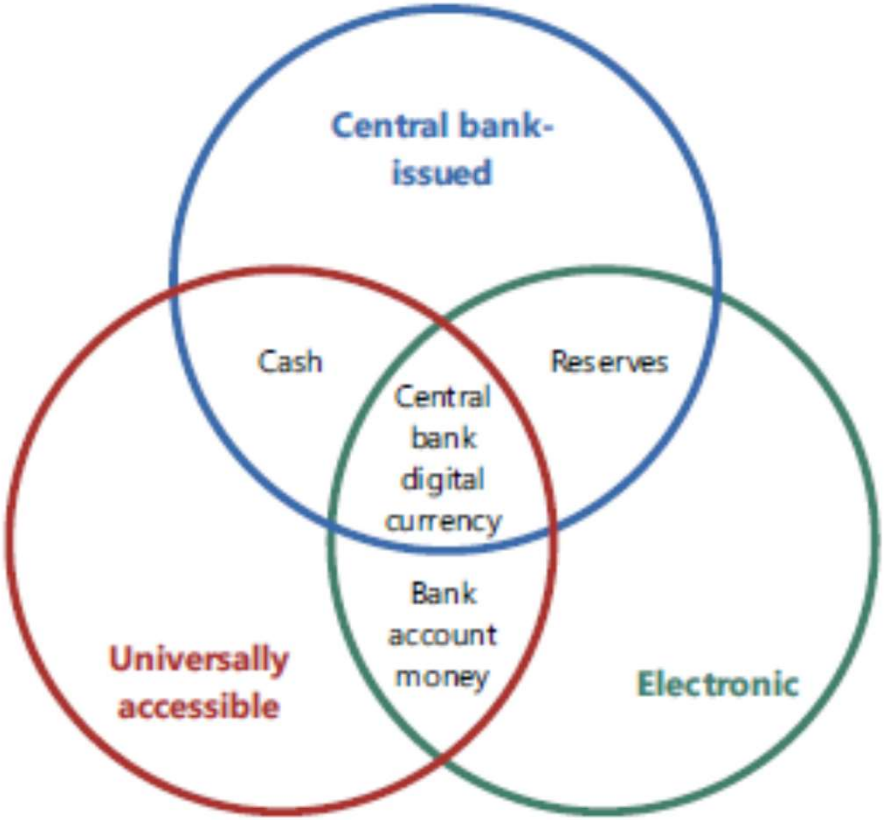


II. Visão geral
Criptomoedas x Moedas

Cryptocurrency, CPMI (2015)



Central bank digital currency, Bjerg (2017)



II. Visão geral
Criptomoedas x Categorias jurídicas

	Semelhança	Distinção
Meio circulante	P2P	Não existem na forma física, não têm autoridade central e semi-anonimato
Moeda estatal Lei 9.069/95	Funções de meio de pagamento e reserva de valor	Não têm poder liberatório determinado por lei e não têm autoridade central*
Moeda eletrônica (e-Money) Lei 12.865/13	Transferência e depósito de valores puramente eletrônico e 24x7	Não existe obrigatoriedade de conversibilidade na moeda estatal
Valores Mobiliários Lei 6.385/76	Captação de recursos junto ao público (ICOs > USD 22,5 bilhões até 2018), intermediários e funções de investimento	Não estão no rol de valores mobiliários

Art. 1º Esta lei dispõe sobre Criptoativos, que englobam ativos utilizados como meio de pagamento, reserva de valor, utilidade e valor mobiliário, e sobre o aumento de pena para o crime de "pirâmide financeira", bem como para crimes relacionados ao uso fraudulento de Criptoativos.

- **Definição ampla, mas não define competências regulatórias**

Art. 2º, (...) Parágrafo único. Considera-se intermediador de Criptoativos a pessoa jurídica prestadora de serviços de intermediação, negociação, pósnegociação e custódia de Criptoativos.

- **Definição tautológia e incompleta (e consultoria / recomendação?)**
- **Quem regula intermediários?**

Art. 4º, (...) § 2º A emissão de criptoativos que, por sua natureza ou pela natureza dos bens, serviços ou direitos subjacentes, estejam sujeitos à regulação específica a ela devem se submeter.

- **Comunicado CVM sobre ICO**
- **Aplica-se a ativos financeiros (BCB)?**

2.5.2019

Capitalização de mercado < USD 180 bilhões (Máximo > USD 800 bilhões)

Número de criptomoedas e tokens > 2100

Market share do Bitcoin < 55% (Até 2016 > 80%)

Cotação do Bitcoin < USD 5,5 mil (Máxima > USD 19,2 mil)

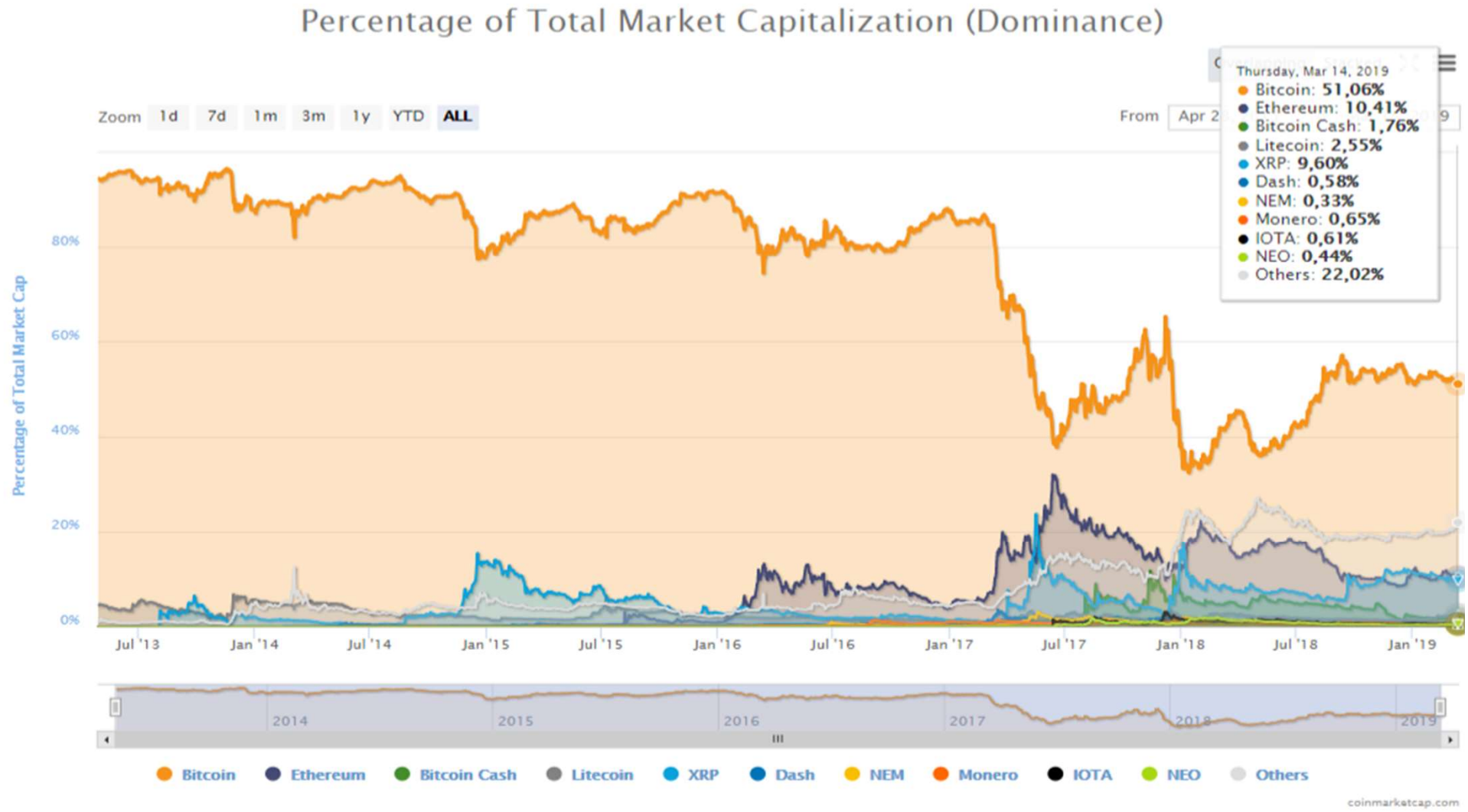
BTC em circulação > 17,6 milhões (Limite de 21 milhões)

Dados atualizados

Concentração - Credit Suisse: 4% dos endereços com 97% dos Bitcoins x 86% dos endereços com 0,6% dos Bitcoins

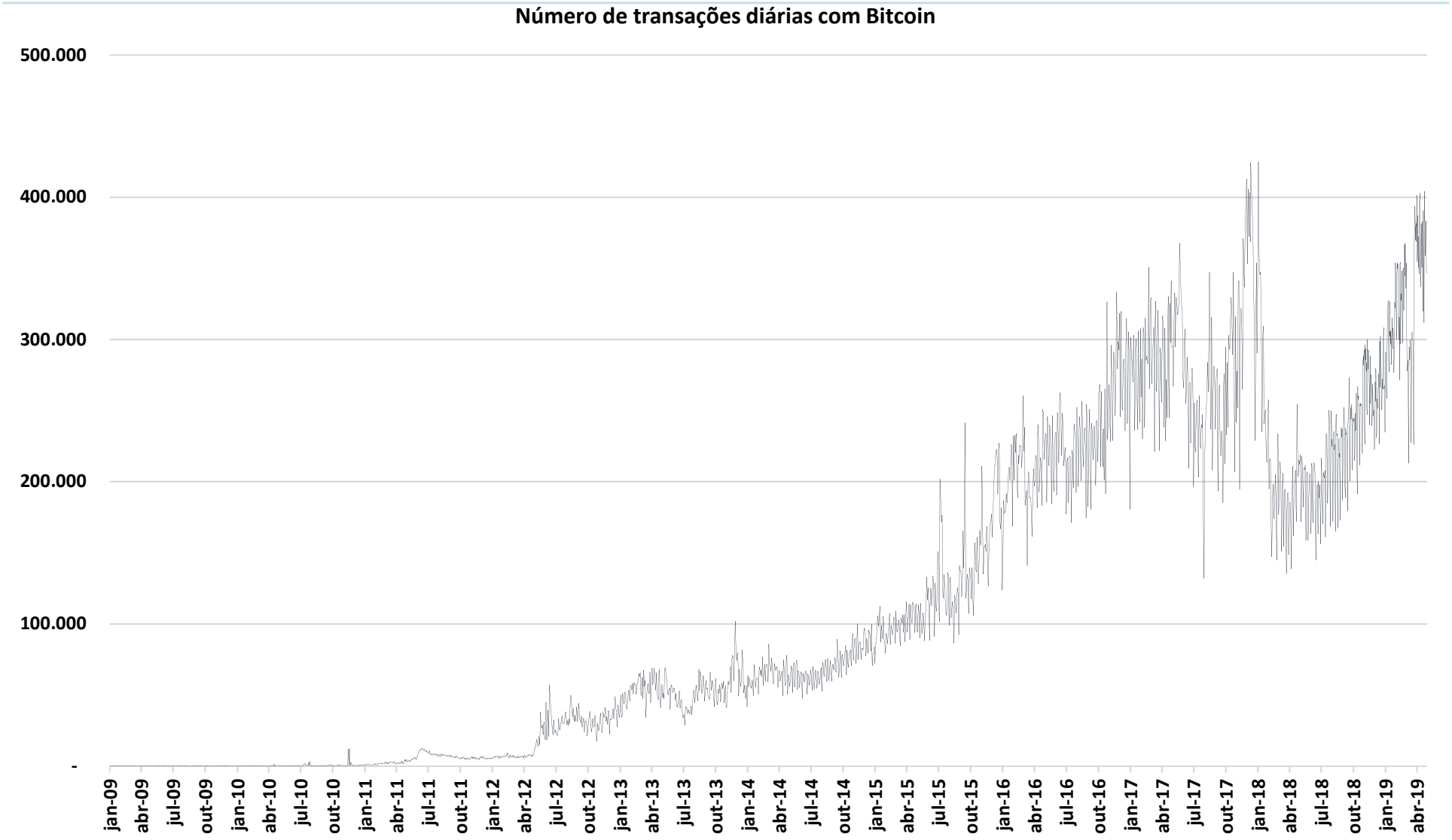
II. Visão geral

Market share das criptomoedas



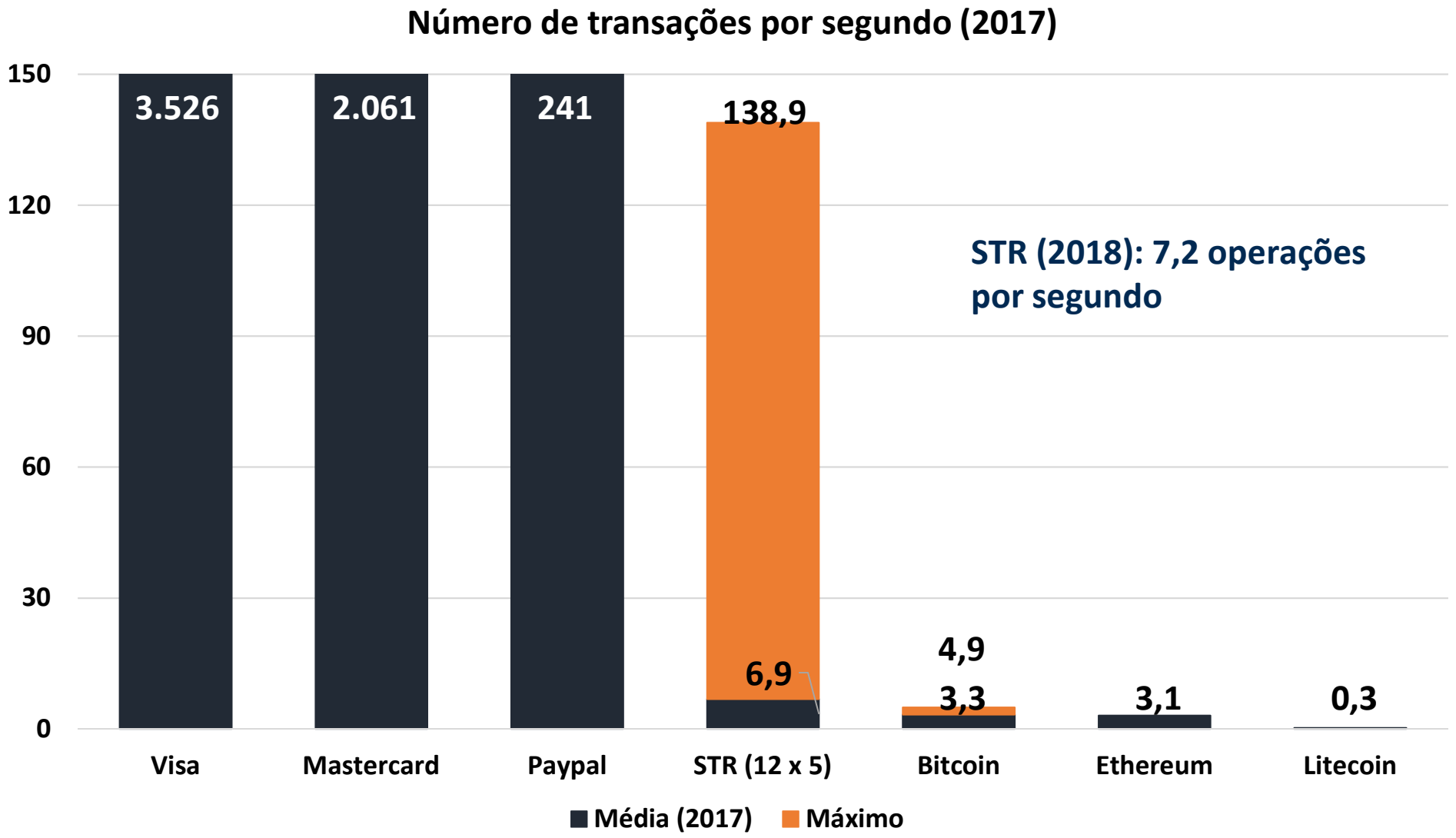
III. Criptomoedas como meio de pagamento

Número de transações diárias



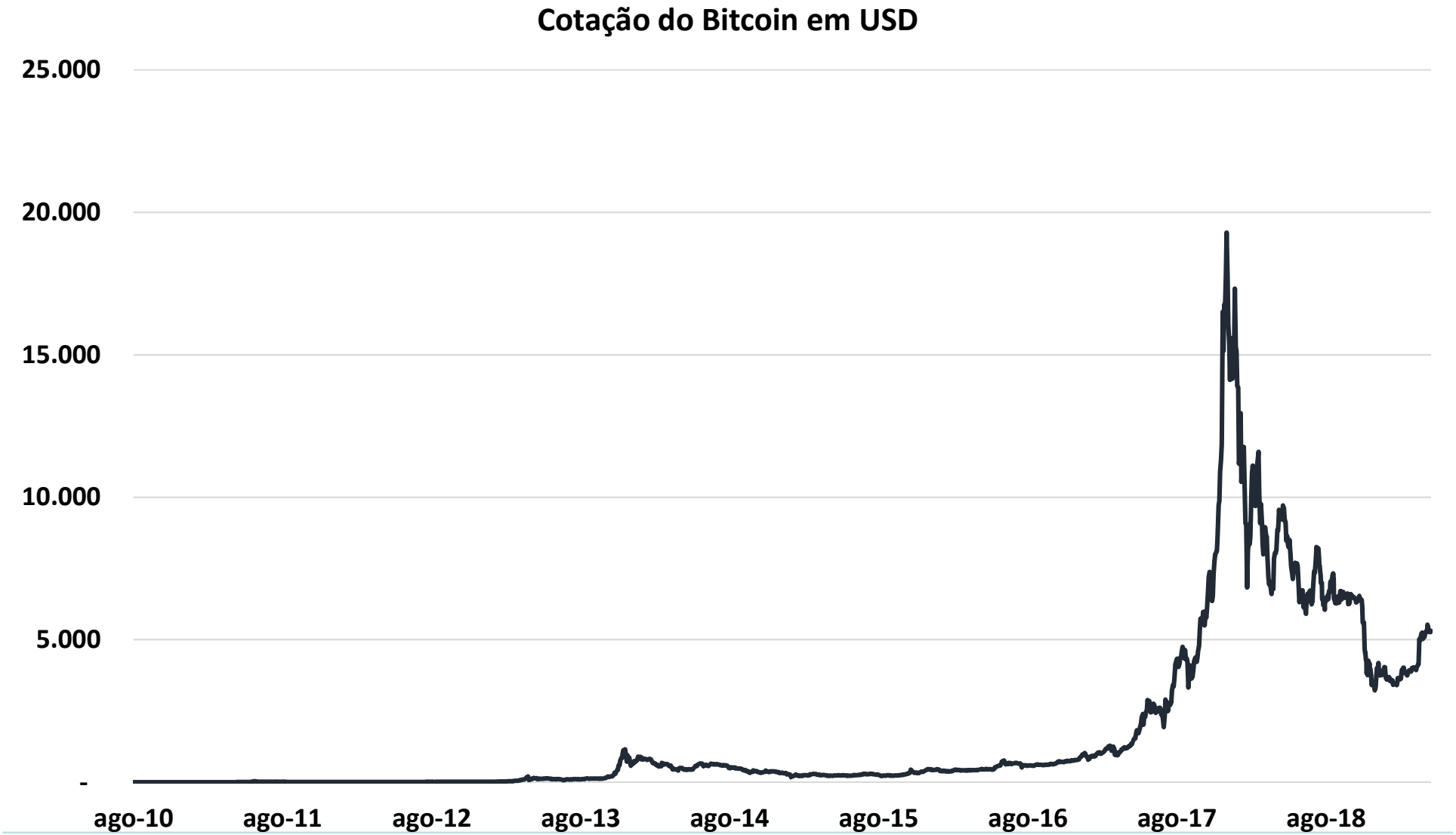
III. Criptomoedas como meio de pagamento

Escalabilidade

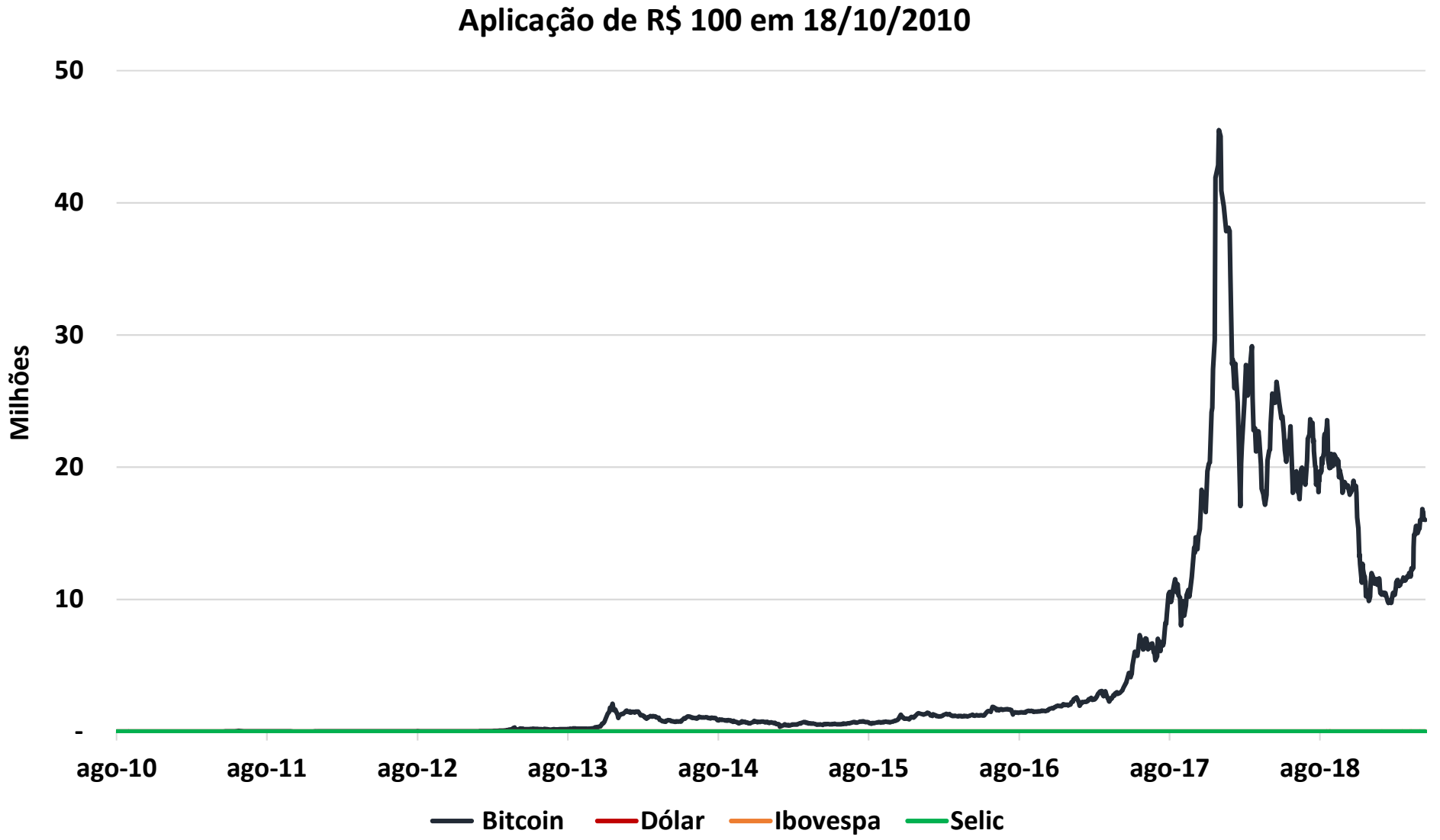


IV. Criptomoedas como investimento

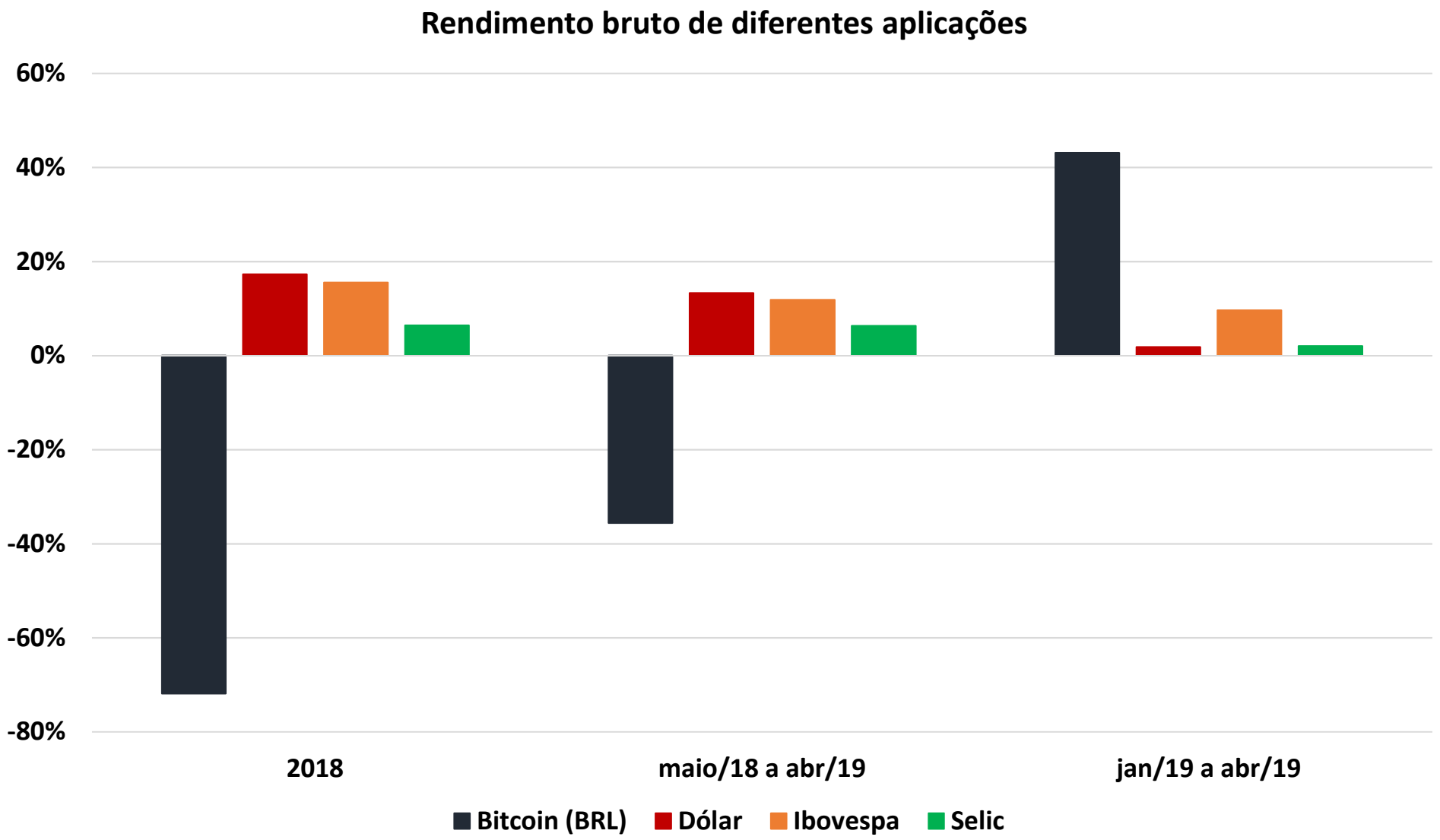
Cotação



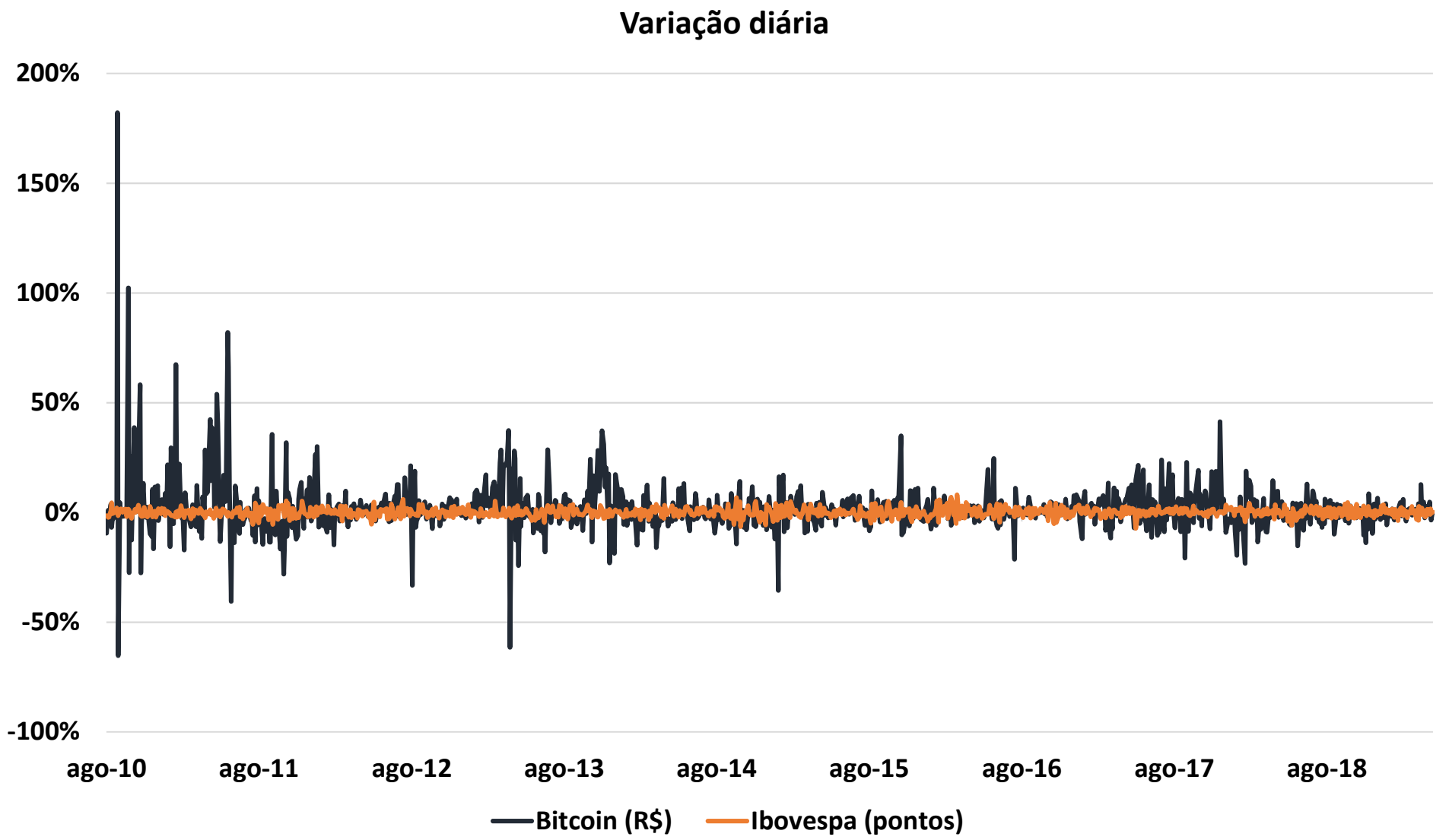
IV. Criptomoedas como investimento
Comparação – série longa



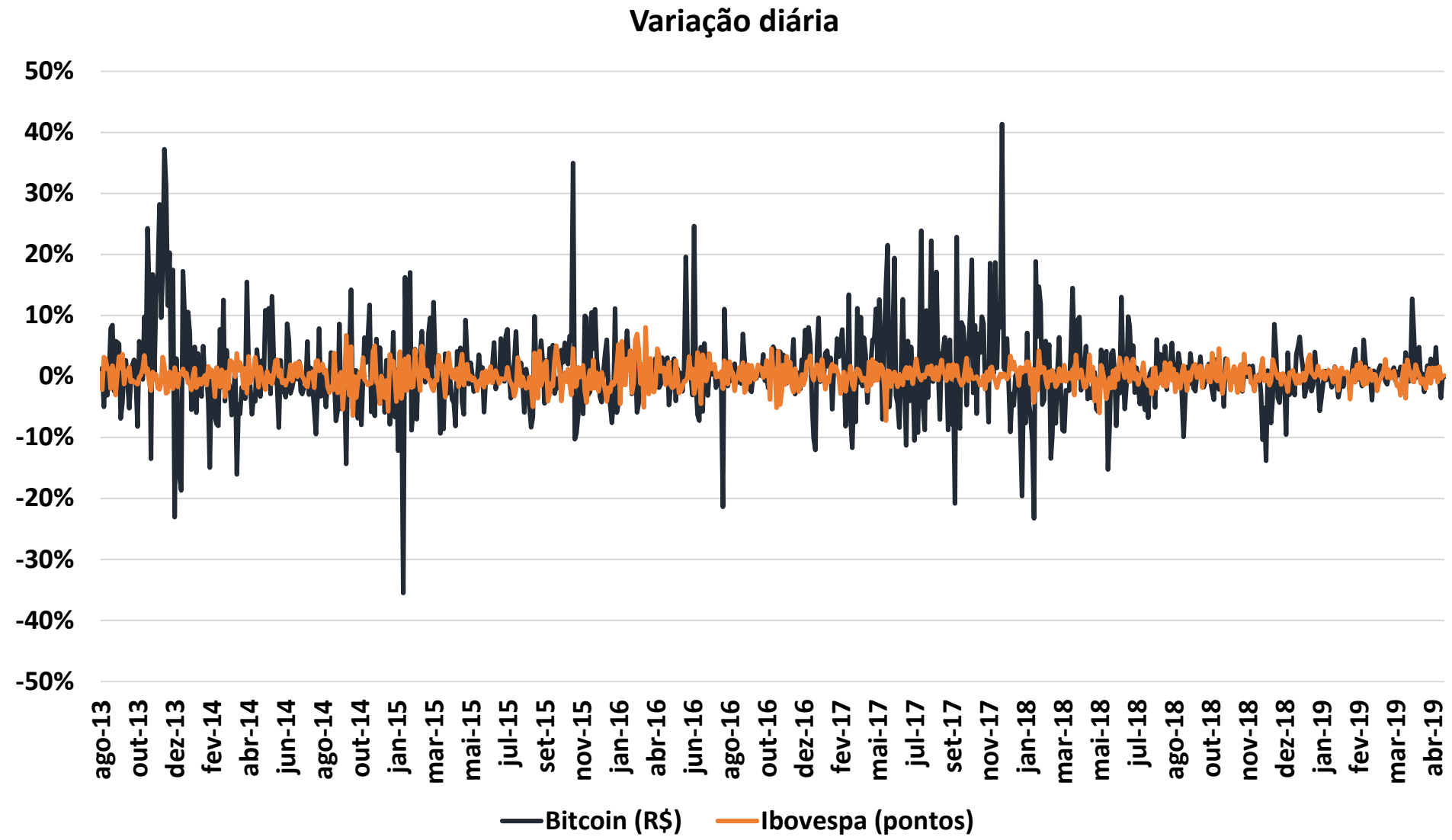
IV. Criptomoedas como investimento
Comparação recente



IV. Criptomoedas como investimento
Variação diária - comparação



IV. Criptomoedas como investimento
Variação diária - comparação



IV. Criptomoedas como investimento

Lei 6.385/76, com redação dada pela Lei 10.303/01, art. 2º: rol taxativo de valores mobiliários)

Via de regra, criptomoedas não são valores mobiliários, mas...

Comunicado CVM de 11/10/2017: "a CVM esclarece que certas operações de ICO podem se caracterizar como operações com valores mobiliários já sujeitas à legislação e à regulamentação específicas, devendo se conformar às regras aplicáveis. Incorrem na mesma situação companhias (abertas ou não) ou outros emissores que captem recursos por meio de uma ICO, em operações cujo sentido econômico corresponda à emissão e à negociação de valores mobiliários."

ICOs > USD 22,5 bilhões (até 2018)

Ofício Circular CVM 1/2008: Vedação a que Fundos de Investimentos regulados pela CVM invistam em criptomoedas

Comunicados de reguladores

V. Riscos das criptomoedas
Comunicado CVM 16/11/2017

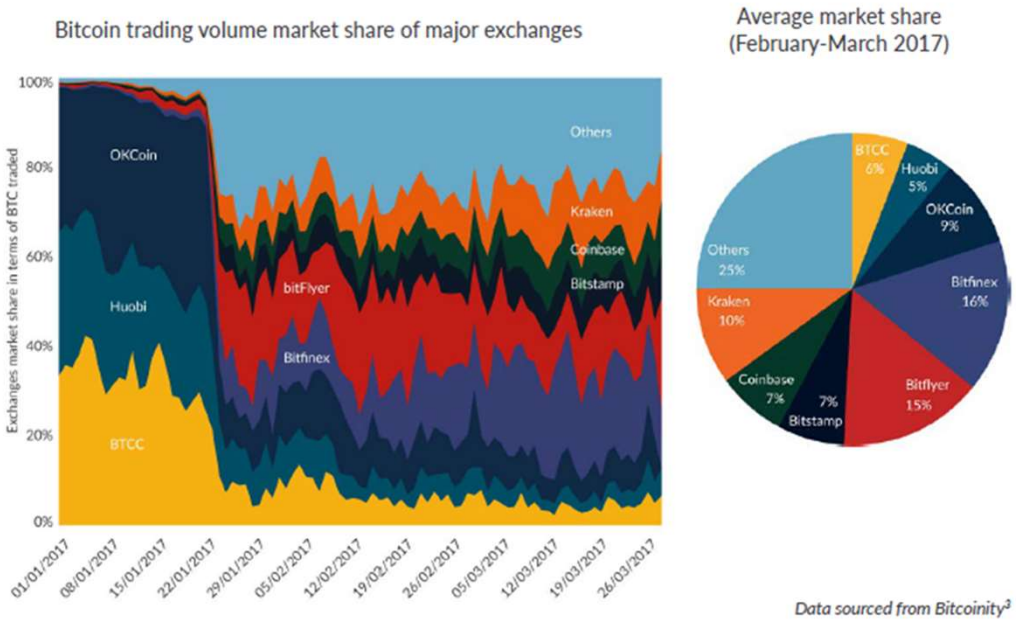
- **Risco de fraudes e pirâmides financeiras;**
- **Inexistência de processos formais de adequação do perfil do investidor ao risco do empreendimento (*suitability*);**
- **Risco de operações de lavagem de dinheiro e evasão fiscal/divisas;**
- **Prestadores de serviços atuando sem observar a legislação aplicável;**
- **Material publicitário de oferta que não observa a regulamentação da CVM;**
- **Riscos operacionais em ambientes de negociação não monitorados pela CVM;**

V. Riscos das criptomoedas
Comunicado CVM 16/11/2017

- **Riscos cibernéticos (dentre os quais, ataques à infraestrutura, sistemas e comprometimento de credenciais de acesso dificultando o acesso aos ativos ou a perda parcial ou total dos mesmos) associados à gestão e custódia dos ativos virtuais;**
- **Risco operacional associado a ativos virtuais e seus sistemas;**
- **Volatilidade associada a ativos virtuais (Vide IV);**
- **Risco de liquidez (ou seja, risco de não encontrar compradores/vendedores para certa quantidade de ativos ao preço cotado) associado a ativos virtuais; e**
- **Desafios jurídicos e operacionais em casos de litígio com emissores, inerentes ao caráter multijurisdicional das operações com ativos virtuais.**

- **Set/17: Proibição de ICO**
- **Set/17: Proibição de bolsas e corretoras de criptomoedas**

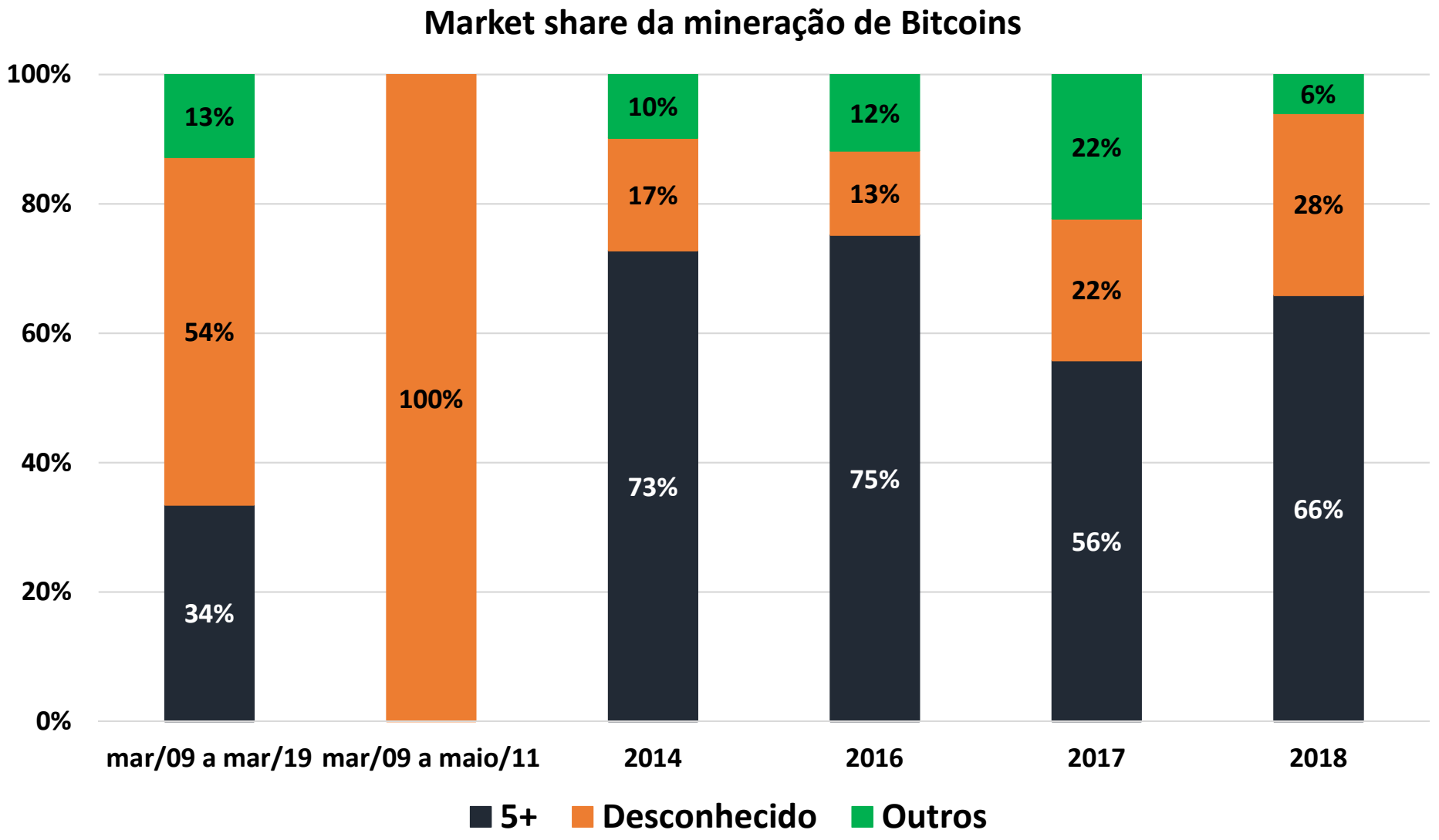
Figure 12: Trading volumes across the top exchanges are more evenly distributed following increased regulation of Chinese exchanges in early 2017



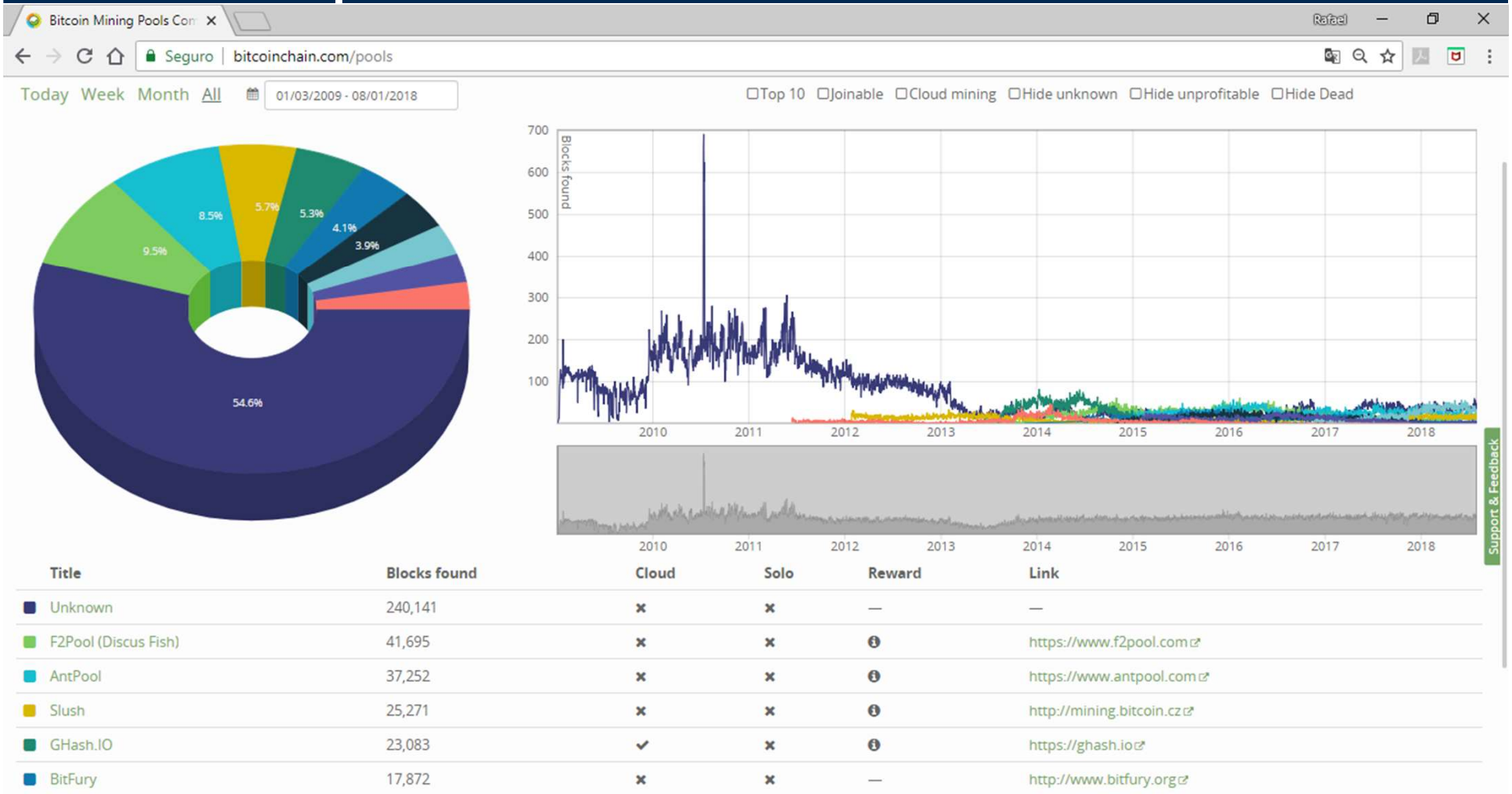
Data sourced from Bitcoinity[3]

- **Ago/19: Comissão Nacional de Desenvolvimento e Reforma – mineração indesejável e deve ser eliminada**

V. China
Mineradores de Bitcoin – market share



V. China
Mineradores de Bitcoin – market share



Title	Blocks found	Cloud	Solo	Reward	Link
Unknown	240,141	✗	✗	—	—
F2Pool (Discus Fish)	41,695	✗	✗	ℹ	https://www.f2pool.com
AntPool	37,252	✗	✗	ℹ	https://www.antpool.com
Slush	25,271	✗	✗	ℹ	http://mining.bitcoin.cz
GHash.IO	23,083	✓	✗	ℹ	https://ghash.io
BitFury	17,872	✗	✗	—	http://www.bitfury.org

Obrigado!

Blog do Bianchini

https://bianchini.blog/2018/03/15/criptomoedas-e-regulacao/

Conjunturando

Bitcoin: da euforia ao choque de realidade

rafael.bianchini.paiva@usp.br