

SNAPSHOT DA INDÚSTRIA DAS CRIPTOMOEDAS

ANA BROCHADO*

1. INTRODUÇÃO

As criptomoedas registaram um crescimento expressivo quer em termos de volume, quer de notoriedade, desde a introdução das bitcoins em 2009 (Nakamoto, 2008).

Não obstante a crescente popularidade e interesse nas criptomoedas, apenas recentemente a literatura da economia e das finanças tem publicado trabalhos sobre este mercado (Li e Wang, 2017). Rogojanu e Badea (2014), por exemplo, estudaram as vantagens e as desvantagens relativas das bitcoins face a outras moedas. Katsiampa (2017) reconhece que o aparecimento das criptomoedas coloca desafios aos governos, reguladores, consumidores, economistas e empreendedores.

O aumento do valor do mercado das criptomoedas e o crescente interesse da população em geral e dos reguladores tem motivado a realização de diversos estudos na área da economia e finanças (Baur et al., 2017), para identificar se o seu comportamento se aproxima de um ativo financeiro, de uma moeda ou de um ativo de reserva (*e.g.* ouro). As criptomoedas partilham as características-chave do ouro (mineração, descentralização, transação 24 horas por dia 7 dias por semana), das moedas (meio de troca) e de outros ativos financeiros (volatilidade) (Dwyer, 2015).

Se as criptomoedas têm o potencial de se tornarem meios de pagamento globais equivalentes às restantes moedas legais, então podem criar

alterações profundas nos sistemas de pagamentos, no valor das moedas tradicionais, nos bancos centrais e na política monetária (Baur et al., 2017). No entanto, atendendo a que os investimentos e as transações com criptomoedas registam valores reduzidos quando comparados com outros ativos, Baur et al., (2018) consideram que não existem riscos ou ameaças para a estabilidade financeira.

Tal como outros segmentos do mercado Fintech, o mercado das criptomoedas está sujeito a quebras de segurança. Por outro lado, o carácter anónimo do sistema (Li e Wang, 2017) levantou preocupações quanto aos riscos de branqueamento de capitais e financiamento de transações ilegais (Brühl, 2017; Blau, 2018). Também os reguladores do setor financeiro têm expressado a sua preocupação sobre as criptomoedas junto dos consumidores (ver, por exemplo, EBA, 2013; BdP, 2014).

As criptomoedas introduzem nos mercados financeiros novas necessidades, nomeadamente em termos de gestão do risco, análise de portfólio e sentimento de mercado.

O presente artigo tem como objetivos: sintetizar os principais temas abordados na literatura económica e financeira sobre as criptomoedas; descrever a evolução do mercado e efetuar uma discussão dos desenvolvimentos nos principais segmentos da indústria das criptomoedas: *exchanges, wallets, mining e payments*.

* Centre for Socioeconomic and Territorial Studies (DINÂMIA²CET – IUL), Instituto Universitário de Lisboa (ISCTE-IUL).

2. A LITERATURA SOBRE CRIPTOMOEDAS

2.1 As Criptomoedas

O surgimento das criptomoedas tornou-se possível devido a desenvolvimentos em diversas áreas científicas, nomeadamente a criptografia (funções *hash* criptográficas, assinaturas digitais), economia (teoria dos jogos) e ciências da computação (redes *Peer-to-Peer* - P2P) (Li e Wang, 2017).

Uma criptomoeda consiste num *token* digital que existe num determinado sistema de criptomoeda e normalmente assenta nas seguintes componentes: (i) rede P2P; (ii) mecanismo de consenso; e (iii) chave para uma infraestrutura pública. Não existe nenhuma entidade central que governa o sistema. Em alternativa, as regras que governam o sistema (*e.g.*, definição de transação válida, a oferta total de *token* digital) são asseguradas pelos participantes na rede (também designados por '*nodes*'). A história das transações pode ser verificada de forma independente em cada '*node*', existindo acesso ao '*ledger*' partilhado. Este '*ledger*' partilhado, que normalmente tem a forma de cadeias de blocos que compreendem as transações (*blockchain*), é constantemente atualizado através de um processo que se designa por mineração (*mining*), a partir do qual novas unidades no *token* nativo (a criptomoeda) são criadas (Gandal et al., 2018). Qualquer pessoa pode entrar e sair do sistema a qualquer momento já que não há identidades associadas aos utilizadores (Blau, 2018).

Podem ser associadas às criptomoedas três propriedades (CCAF, 2017): (i) ativo digital ao portador (*digital bearer asset*); (ii) sistema integrado de pagamento (*integrated payment network*); (iii) outras utilizações não monetárias (*non-monetary use cases*). O *token* nativo constitui um ativo ao portador, na medida em que o indivíduo que controla a respetiva chave privada (*private key*) controla o montante de criptomoeda a ela associado, que pode ser usado co-

mo uma moeda ou um ativo financeiro. Quando as criptomoedas são usadas como moeda preenchem os requisitos de meio de troca, unidade de conta e reserva de valor (Baur et al., 2018). No caso de utilização como ativo financeiro normalmente as duas primeiras propriedades não estão presentes. A literatura tem discutido a possível classificação das criptomoedas como moeda ou como ativo financeiro com base na evolução das suas cotações e de outras moedas/ativos (Dwyer, 2015).

Adicionalmente, trata-se de um ativo *censorship-resistant* na medida em que nenhuma entidade do sistema pode confiscar os montantes de criptomoedas detidas nem censurar transações. As criptomoedas estão integradas numa rede integrada de pagamentos, que oferece uma forma rápida, económica e de alcance global de pagamentos (não estando circunscritos a uma determinada localização ou jurisdição). Como resultado da desintermediação, as taxas de transação são, em termos gerais, substancialmente inferiores às cobradas pelos operadores de sistemas de pagamento tradicionais (Kim, 2017; Baur et al., 2018), tanto para micro pagamentos como para transferências de valores mais elevados. As taxas não são baseadas no montante transferido, mas na dimensão da transação traduzida em *bytes* (CCAF, 2017).

Os pagamentos tornam-se irreversíveis logo que os montantes são transferidos e se recebem as confirmações do sistema. Para as empresas que operam no setor do retalho, a utilização de criptomoedas apresenta como vantagem adicional a não necessidade de armazenamento de informação sobre os consumidores (*e.g.*, contactos, dados do cartão de crédito), atendendo a que os utilizadores são identificados pela sua morada de criptomoedas que resulta da chave pública.

2.2 Os preços das Criptomoedas

Atendendo a que a bitcoin foi a primeira criptomoeda com sucesso, é também a criptomoeda relativamente à qual são efetuados mais estudos

acadêmicos (Gandal et al., 2018). Algumas exceções são o trabalho de Ciaian et al., (2018), que estudou o preço de 17 criptomoedas, as bitcoins e outras 16 altcoins, e o estudo de Corbet et al. (2017), que analisa os preços da bitcoin e da ethereum. Li e Wang (2017) estudaram empiricamente o valor da bitcoin e Bolt e van Oordt (2016) desenvolveram um modelo teórico para a determinação da cotação das criptomoedas. Hayes (2017) desenvolveu um modelo para a determinação do valor das bitcoins com base nos custos de produção.

Ciaian et al. (2016) concluíram que a atratividade de uma criptomoeda para o investidor exerce um papel importante no seu preço. Katsiampa (2017) estudou a volatilidade das criptomoedas e concluiu que as bitcoins têm sido utilizadas mais como um ativo do que como uma moeda, atendendo à sua natureza especulativa e à sua volatilidade.

Um conjunto de estudos compararam o valor das criptomoedas com o valor de outros ativos. Dyhrberg (2016) concluiu que o comportamento das séries de preços das bitcoins apresenta semelhanças tanto ao comportamento do ouro como ao do dólar americano. Baur et al. (2017) concluiu que a volatilidade das bitcoins é 10 vezes superior à do ouro, do USD e dos mercados financeiros (índice MSCI) e que o seu comportamento em termos de retornos, volatilidade e grau de correlação, é diferente do de outros ativos. Baur et al. (2018) analisou os preços das bitcoins, ações, obrigações e *commodities*, tendo concluído que as criptomoedas são usadas com mais frequência como ativo financeiro do que como moeda.

Bariviera (2017) e Tiwari et al. (2018) estudaram a eficiência do mercado das bitcoins. Xie et al. (2017) analisaram a relação entre as cotações das bitcoins e o sentimento de mercado, medido através de informação de *social media*. Os resultados revelaram que a informação gera-

da pelo utilizador permite prever a evolução das cotações no curto e no longo prazo.

Li e Wang (2017) concluíram que as bitcoins têm gradualmente evoluído para um estado de maturidade, em que os fatores de ordem económica começam a ter maior impacto na determinação do preço das bitcoins no longo prazo do que fatores tecnológicos ou de atividade do mercado das criptomoedas.

A título de síntese, diversas variáveis têm sido usadas na literatura para explicar o comportamento do preço das bitcoins, como sejam:

- i) fatores tecnológicos - dificuldade de mineração e *hash rate* (Kristoufek, 2015; Corbet et al., 2017) e reconhecimento público nas redes sociais (Ciaian et al., 2016);
- ii) fatores económicos - inflação, taxa de juro, PIB, oferta de moeda (Li e Wang, 2017);
- iii) economia bitcoin (oferta de bitcoin, transações, valor e volume de bitcoins) (Li e Wang, 2017);
- iv) atividade de mercado (volume transacionado e volatilidade (Ciaian et al., 2016) e custos de transação em mercado secundário (Kim, 2017);
- v) preço de outros ativos (Dyhrberg, 2016); e
- vi) preço de outras criptomoedas/ *altcoins* (Ciaian et al., 2018).

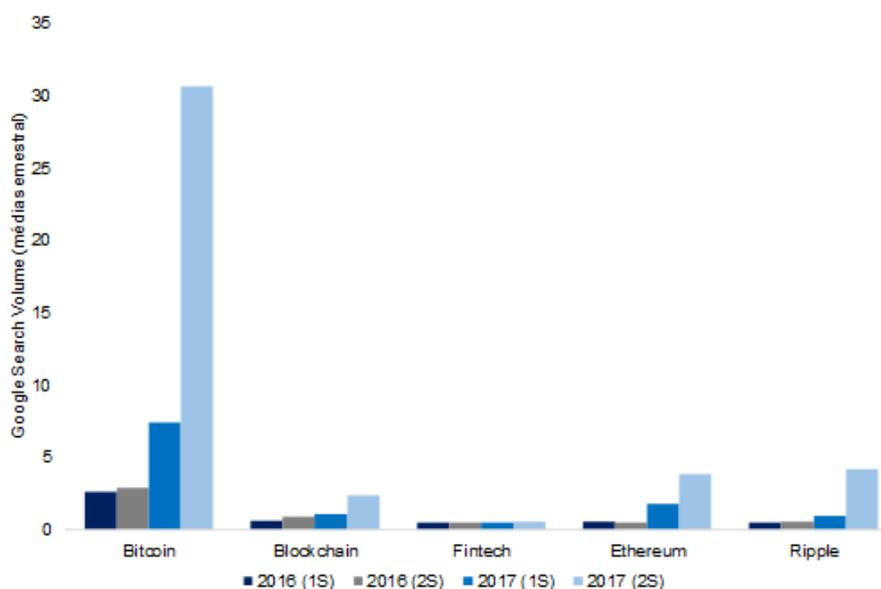
3. AS CRIPTOMOEDAS

3.1 Notoriedade

A criptomoeda com maior notoriedade, medida pelo volume mundial de pesquisas no Google¹, é a bitcoin (BTC). Verifica-se um aumento da atenção nas criptomoedas e da tecnologia *blockchain* no ano de 2017, que se intensificou no último trimestre do ano. O índice máximo de pesquisas do termo bitcoin ocorreu em dezembro de 2017.

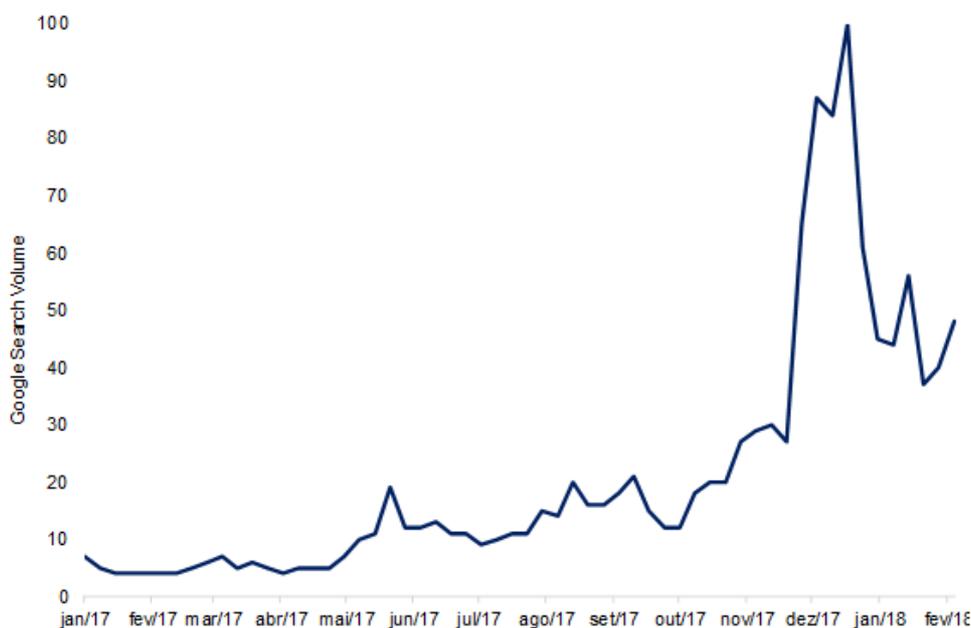
1- O Índice de pesquisas de um determinado termo no Google tem sido utilizado na área das finanças como um indicador da atenção do investidor.

Gráfico 1 - Volume de pesquisas no Google de criptomoedas (média semestral)



Fonte: Google Trends

Gráfico 2- Volume de pesquisas semanal do termo “bitcoins”

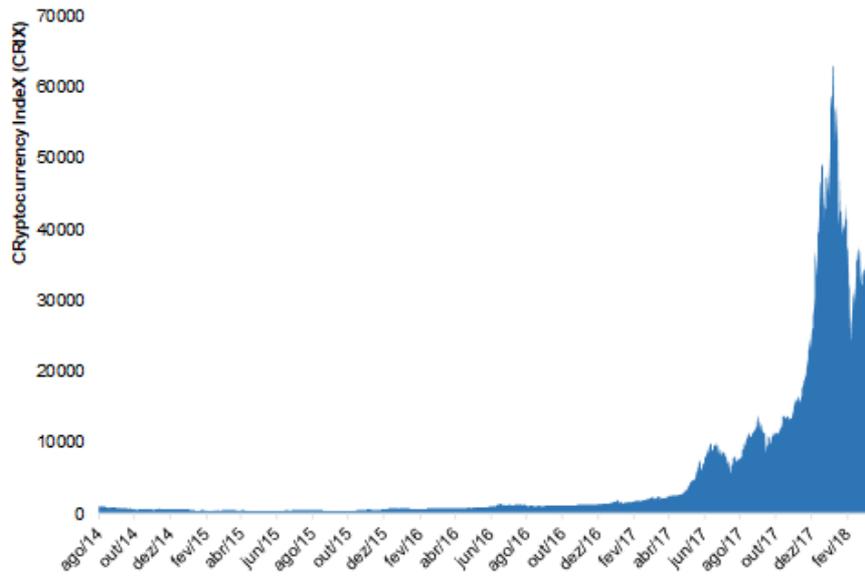


3.2 O mercado em valor

Observou-se um crescimento exponencial na capitalização bolsista, no volume transacionado e na volatilidade das criptomoedas no último ano. Considerando as 75 criptomoedas, o CRyptocurrency IndeX - CRIX (Trimborn e Härdle, 2015) registou um crescimento expo-

nencial no ano de 2017, passando de 1.688,62 (31 de dezembro de 2016) para 48.365,44 (31 de dezembro de 2017), correspondendo a um aumento no índice de 2.764%. Após atingir um máximo de 62.895,26 pontos em 6 de janeiro de 2018, o índice desceu para 24.039,07 em 6 de fevereiro (-61,8%) e subiu para 34.946,61 em 6 de março (+45,4%).

Gráfico 3 - CRIX Index



Fonte: <http://crix.hu-berlin.de/>

O ano de 2017 ficou marcado por um crescimento na generalidade das criptomoedas. Efeti-

vamente, das 30 principais criptomoedas (de acordo com a capitalização bolsista), 27 registraram um crescimento de pelo menos três dígitos.

Tabela 1 - Crescimento y-o-y das 30 principais criptomoedas (2017)

#	Cripto Moeda	Retorno (YoY)	#	Cripto Moeda	Retorno (YoY)
1	Bitcoin (BTC)	1387%	16	Verge (XVG)	3663%
2	Ripple (XRP)	34032%	17	Tron (TRX)	1851%
3	Ethereum (ETC)	9506%	18	RaiBlocks (XRB)	64558%
4	Bitcoin Cash (BCH)	536%	19	Bitconnect (BCC)	292407%
5	Cardano (ADA)	2759%	20	Ethereum Classic (ETC)	1765%
6	Litecoin (LTC)	5176%	21	Lisk (LSK)	14799%
7	IOTA (IOT)	624%	22	ICON (ICX)	1112%
8	NEM (XEM)	31765%	23	OmiseGo (OMG)	5066%
9	Dash (DASH)	9397%	24	Bitshares (BTS)	17116%
10	Stellar Lumens (XLM)	16550%	25	Ardor (ARDR)	686%
11	Monero (XMR)	2496%	26	Populous (PPT)	773%
12	NEO (NEO)	56871%	27	Zcash (ZEC)	945%
13	EOS (EOS)	300%	28	Stratis (STRAT)	19469%
14	Qtum (QTUM)	430%	29	tether (USDT)	1%
15	Bitcoin Gold (BTG)	94%	30	Hshare (HSR)	69%

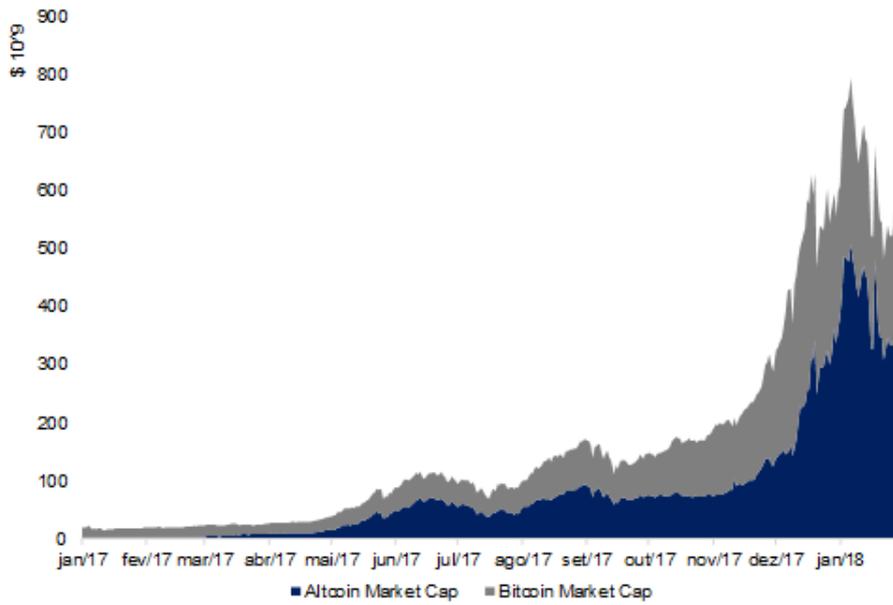
Fonte: CoinGecko (2018)

Em termos de capitalização bolsista, tem-se assistido a um aumento da expressão de outras moedas que não a bitcoin (i.e., as *altcoins*). Efetivamente, desde a introdução da bitcoin, o mercado tem assistido ao lançamento de diversas criptomoedas, observando-se no final de 2017 a existência de mais de 1500 criptomoedas. Um dos motivos para o surgimento de um grande número de *altcoins* está relacionado com as

reduzidas barreiras à entrada, apenas sendo necessário um algoritmo criptográfico, um processo de *mining* e um algoritmo de consenso (Brühl, 2017).

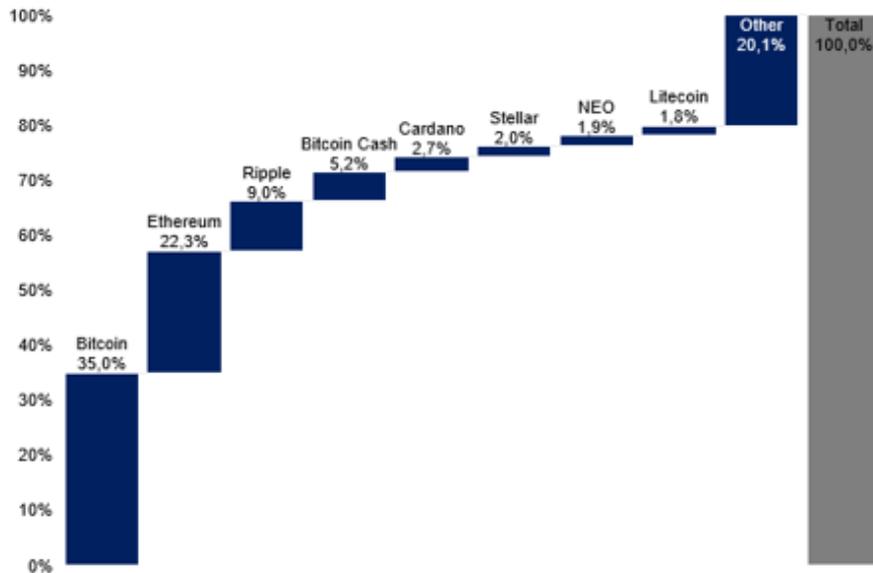
Não obstante, continua a observar-se uma elevada concentração, com três moedas (bitcoin, ethereum e ripple) a representarem 66% do mercado.

Gráfico 4- Capitalização bolsista



Fonte: CoinDance

Gráfico 5- Quota de mercado das criptomoedas (capitalização bolsista), 31 janeiro de 2018



Fonte: CoinDance

O crescimento do mercado das criptomoedas tem sido acompanhado do surgimento de novos fundos de investimento, constituídos por carteiras de criptomoedas, entre 6 e 100 moedas, com ou sem ponderação pela capitalização bolsista, a saber: CRYPTO20², Bitwise HOLD10³, Aggregated Coin⁴ (AGRE), UpStart1K⁵, Bit20⁶, Pantera BitCoin Fund⁷, Crescent Crypto Asset Management⁸, Bletchley 10 Index⁹.

3.3 Perfil dos utilizadores

3.3.1 Perfil demográfico

Os utilizadores de bitcoins são maioritariamente do sexo masculino (94,7%), com idades compreendidas entre 25-34 e 35-44 anos (76,3%), possuem como principais afinidades as categorias ‘*Avid investors*’ (7,3%) e ‘*Technophiles*’ (7,0%) e como interesses de comunidades online de serviços e investimentos financeiros (8,1%)¹⁰.

2- <https://static.crypto20.com>

3- <https://www.bitwiseinvestments.com/fund>

4- <http://www.combined-coins.com/>

5- Ibidem.

6- <http://www.bittwenty.com/>

7- <https://www.panteracapital.com/about/>

8- <https://www.crescentcrypto.com/>

9- <https://www.crescentcrypto.com/>

10- A definição exata do perfil dos utilizadores de criptomoedas é uma tarefa complexa, na medida em que as plataformas e empresas que operam no setor normalmente não divulgam este tipo de informação.

Tabela 2 - Perfil demográfico e psicográfico dos utilizadores de bitcoin*

Variável	Categoria	%
Sexo	Masculino	94,7%
	Feminino	5,3%
Grupo etário	18-24	8,4%
	25-34	45,7%
	35-44	30,6%
	45-54	12,3%
	55-64	1,8%
	65+	1,2%
Afinidades (online)	<i>Avid Investors</i>	7,3%
	<i>Technophiles</i>	7,0%
	<i>Shutterbugs</i>	6,6%
	<i>Movie Lovers</i>	5,9%
	<i>TV Lovers</i>	5,6%
	<i>News Junkies</i>	5,4%
	<i>Political Junkies</i>	3,9%
	<i>Mobile Enthusiasts</i>	2,9%
	<i>Music Lovers</i>	2,8%
	<i>Travel Buffs</i>	2,6%
Interesses (online)	<i>Financial Services/ Investment Services/ Software/ Design/ Drawing & Animation Software</i>	8,1%
	<i>Financial Services/ Banking Services</i>	3,3%
	<i>Employment</i>	2,8%
	<i>Consumer Electronics/ Mobile Phones</i>	2,7%
	<i>Computers</i>	2,7%
	<i>Computers</i>	2,7%
Aparelho de acesso	Desktop	66,8%
	Mobile	28,0%
	Tablet	5,3%

Fonte: CoinDance¹¹, Google Analytics statistics, acedido a 12 de março de 2018

Um estudo realizado na plataforma Reddit (N=331) revelou que 65,3% dos respondentes (utilizadores da plataforma que visitam tópicos sobre criptomoedas) possuem pelo menos o grau de licenciatura e 15% são estudantes¹².

3.3.2 Perfil geográfico

A distribuição geográfica das ATMs de bitcoin e de outras criptomoedas revela uma grande concentração na América do Norte e Canadá,

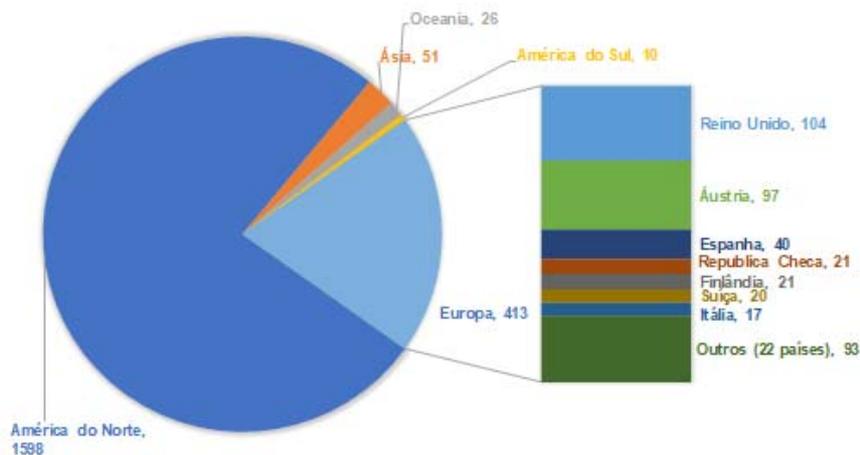
11- <https://coin.dance/stats#demographics>

12- *The Reddit cryptocurrency survey*, disponível a partir de: https://docs.google.com/document/d/1Y2fKK1cJla7r14Pz3y7w7AlkYgg_AM46_RkB-tggEM/edit (acesso 13 de março de 2018)

que em conjunto possuem 97% das máquinas existentes. As ATMs existem em 29 países da Europa, destacando-se o Reino Unido, a Áustria e a Espanha (CoinATMRadar). Das 2.098

ATMs existentes em janeiro de 2018, 100% suportavam bitcoins, 36,7% (770) altcoins, 35% (735) litecoin, 8,1% (170) ether e 5,4% (114) dash.

Gráfico 6- Distribuição das ATM bitcoin

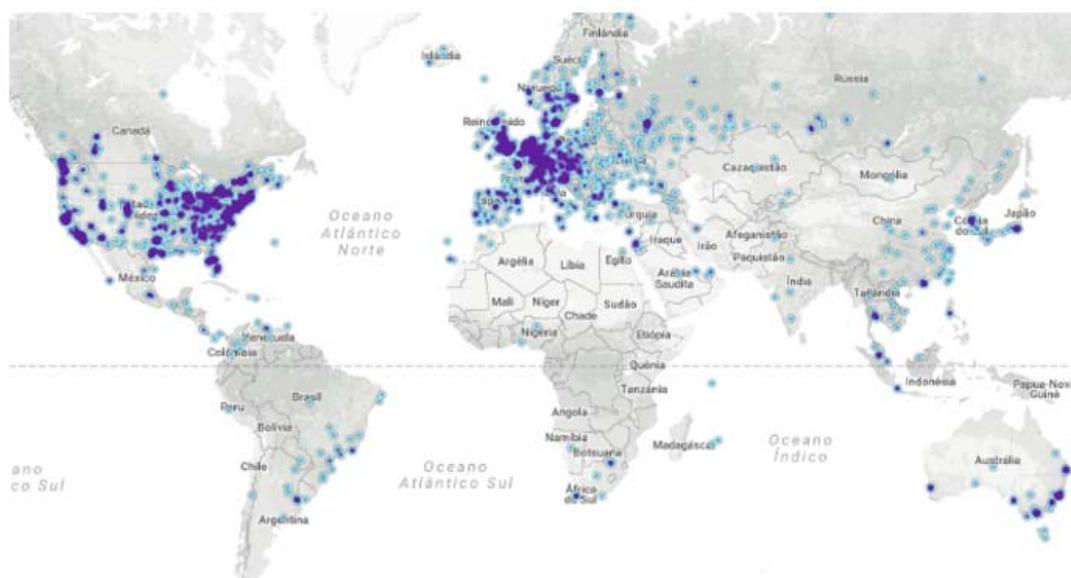


Fonte: CoinATMRadar¹³

A execução de um nó completo fornece também indicação do local em que a atividade ocorre. A distribuição dos *nodes* de bitcoin re-

vêla que existe uma concentração de atividade nos EUA, seguindo-se a Europa, com alguma atividade a ser observada noutras regiões.

Figura 1- Bitcoin nodes



Fonte: <https://bitnodes.eam.com/> (acesso 23 de janeiro de 2018)

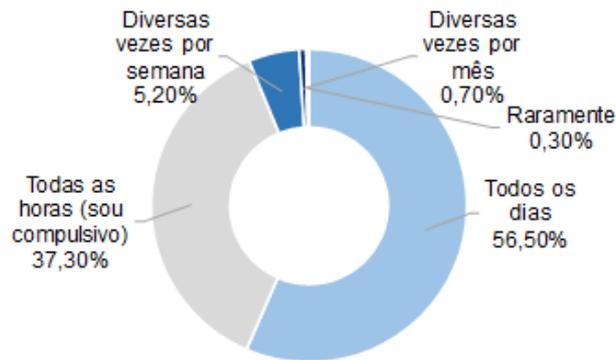
13- Disponível a partir de <https://coinatmr.com/charts/#by-continent> (acesso 31 de janeiro 2018)

3.3.3 Perfil comportamental

Um inquérito realizado no quarto trimestre de 2017 (N=3.000) revelou que 94% dos investidores em bitcoins consultam os preços diaria-

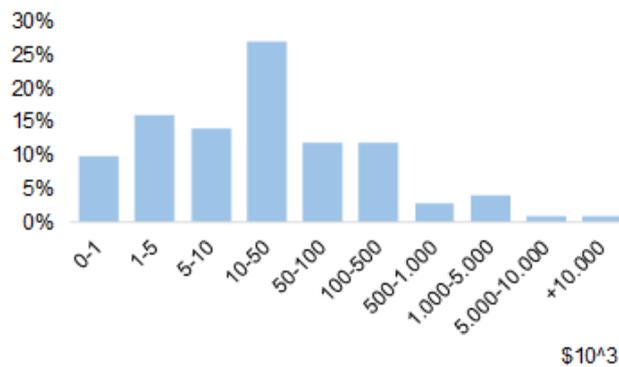
mente e 37% fazem-no mesmo de forma compulsiva (todas as horas). Cerca de 27% dos investidores possuía carteiras entre 10.000 e 50.000 USD, enquanto 86% dos inquiridos possuíam mais de 3 ativos digitais.

Gráfico 7- Frequência de consulta de preços de criptomoedas



Fonte: N=3.000 State of Blockchain, coindesk (2018)¹⁴

Gráfico 8- Valor da carteira

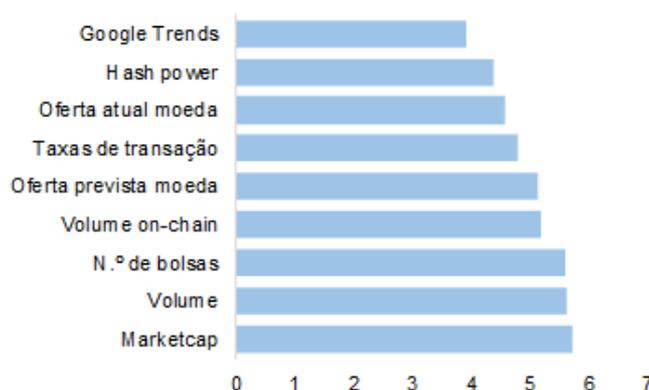


Fonte: N=3.000 State of Blockchain, coindesk (2018)

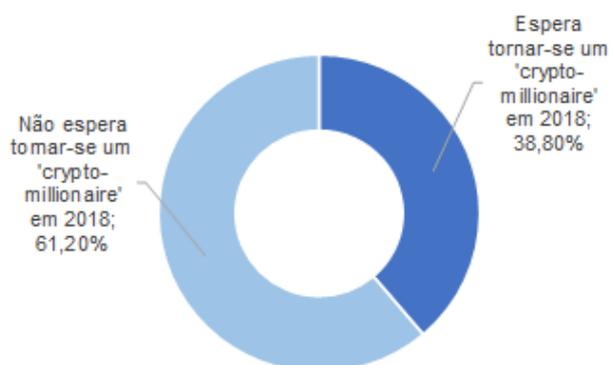
Os critérios mais importantes na escolha de uma criptomoeda são a capitalização bolsista (5,73), o volume transacionado (5,63) e o número de bolsas que a listam (5,60). As expetati-

vas de valorização das criptomoedas são expressivas, com 38,8% dos respondentes afirmando que esperam tornar-se ‘*cryptomillionaires*’ no ano de 2018.

14- Disponível a parte de <https://www.coindesk.com/research/state-blockchain-2018/> (acesso 13 de março de 2018).

Gráfico 9- Critérios de escolha de uma criptomoeda

Fonte: N=3.000 State of Blockchain, coindesk (2018)

Gráfico 10- Sentimento de mercado em relação à valorização das criptomoedas

Fonte: N=3.000 State of Blockchain, coindesk (2018)¹⁵

3.4 O ecossistema financeiro

Um conjunto diverso de agentes económicos oferecem serviços que, simultaneamente, aproveitam as vantagens dos sistemas de criptomoedas e acrescentam valor aos utilizadores (ECB, 2015). O ecossistema financeiro da indústria de criptomoedas inclui agentes económicos que oferecem produtos, serviços e aplicações que envolvem o uso de criptomoedas.

Os principais setores desta indústria são (Gandal et al., 2018; CCAF, 2017):

- i) *Exchanges* (bolsas): compra, venda e troca de criptomoedas (por outras criptomoedas ou moedas 'fiat' nacionais);

- ii) *Wallets* (carteiras): armazenagem de criptomoedas (*handling key management*);
- iii) *Payments* (pagamentos): facilitação dos pagamentos usando criptomoedas; e
- iv) *Mining* (mineração): assegurar o funcionamento do *ledger* global (*blockain*); responsabilidade por confirmar as transações e a segurança do registo de todas as transações.

4. EXCHANGES

Uma bolsa (*exchange*) de criptomoedas é uma plataforma online que oferece serviços de compra e venda de criptomoedas e de outros ativos

15- Disponível a parte de <https://www.coindesk.com/research/state-blockchain-2018/> (acesso 13 de março de 2018).

digitais, em troca de outras criptomoedas ou de moedas nacionais (*fiat currency*). As bolsas são um elemento importante deste ecossistema financeiro. Nomeadamente, permitem a ligação das criptomoedas com a economia real, em que as transações são denominadas nas moedas locais (Li e Wang, 2017).

As bolsas de criptomoedas oferecem três tipos de atividades principais (CCAF, 2017): (i) *order-book exchange*: a plataforma utiliza um sistema de negociação que recebe ordens de compra e de venda dos utilizadores; (ii) *brokerage services*: serviço que permite aos utilizadores adquirir ou vender criptomoedas de forma conveniente a um dado preço; (iii) *plataforma de negociação*: plataforma que permite uma única *interface* na ligação de diversos sistemas de negociação e/ou ofertas permitindo a alavancagem e a oferta de derivados de criptomoedas. As bolsas desempenham um papel importante na indústria, constituindo um mercado para a transação, liquidez e formação do preço das criptomoedas.

As bitcoins são transacionadas por todas as bolsas (CCAF, 2017), sendo seguidas da ether e litecoin. No ano de 2017, 39% das bolsas apenas transacionavam bitcoins, 25% transaciona-

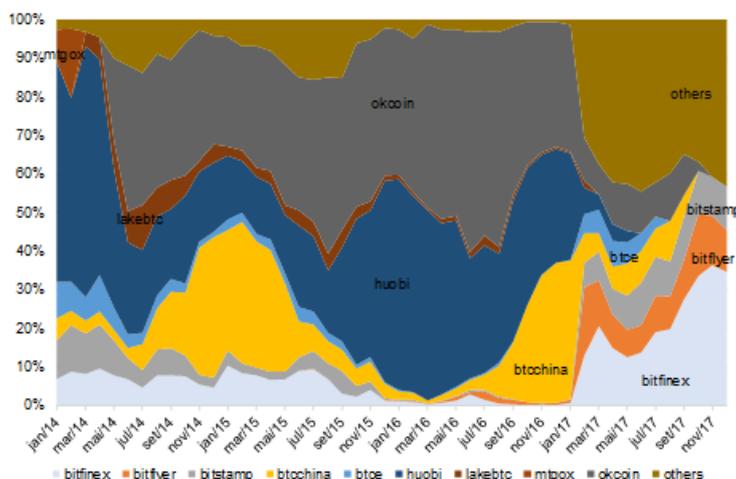
vam 2 moedas e 36% três ou mais moedas, 6% ofereciam produtos derivados e 16% ofereciam serviços de *margin trading* (CCAF, 2017). No caso das bitcoins, apesar de existirem cerca de 110 bolsas que transacionam este tipo de ativo¹⁶, o mercado tem apresentado uma elevada concentração.

De acordo com CCAF (2017), aproximadamente 72% das bolsas de menor dimensão especializam-se num tipo de serviço (*i.e.*, *brokerage services*), enquanto as bolsas de maior dimensão oferecem diversos serviços.

As principais bolsas em termos de quota de mercado têm registado alguma variação ao longo do tempo. A primeira bolsa que transacionou bitcoins, com início de atividade em 2010, a Mt. Gox, suspendeu todas as transações em fevereiro de 2014 no seguimento de quebras de segurança.

Em dezembro de 2015 a huobi detinha uma quota de mercado de aproximadamente 52%, em janeiro de 2016 a btchina (36,1%), a okcoin (32,2%) e a huobi (29,6%) representavam em conjunto aproximadamente 98% do mercado. Em dezembro de 2017 a bitfinex (34,6%), bitstamp (11,2%) e bitFlyer (10,9%) representavam 56,7% do mercado.

Gráfico 11- Evolução da quota de mercado das bolsas, por volume transacionado



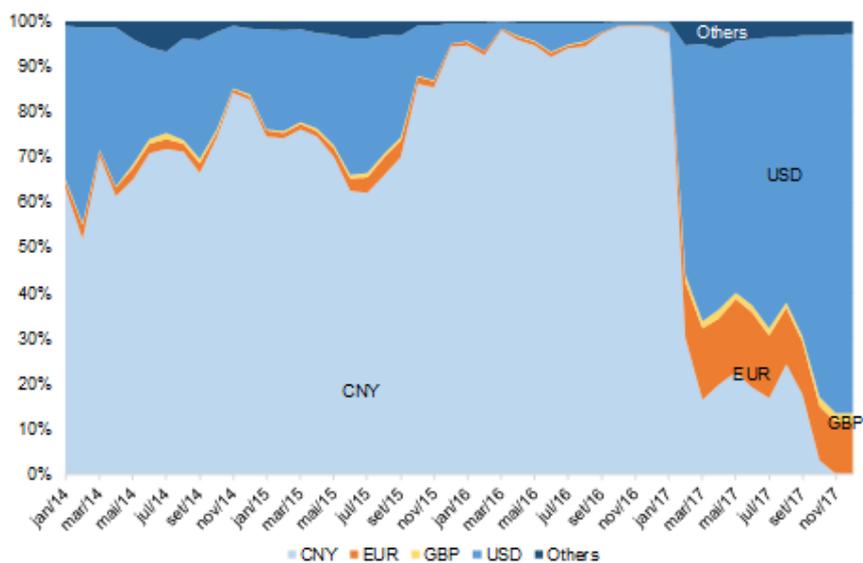
Fonte: <https://data.bitcoinity.org/>

16- <http://bitcoinity.org/> acesso a 17 de janeiro de 2018.

Em termos de volume por moedas nacionais, verifica-se que as transações com bitcoins são efetuadas com mais de 40 moedas. No período de 2014 a 2016 grande parte das transações fo-

ram efetuadas em CNY e no ano de 2017 as principais moedas foram o USD, o EUR e a GBP. A redução da importância do CNY está associada à legislação do *People's Bank of China*.

Gráfico 12- Percentagem transacionada, por moeda

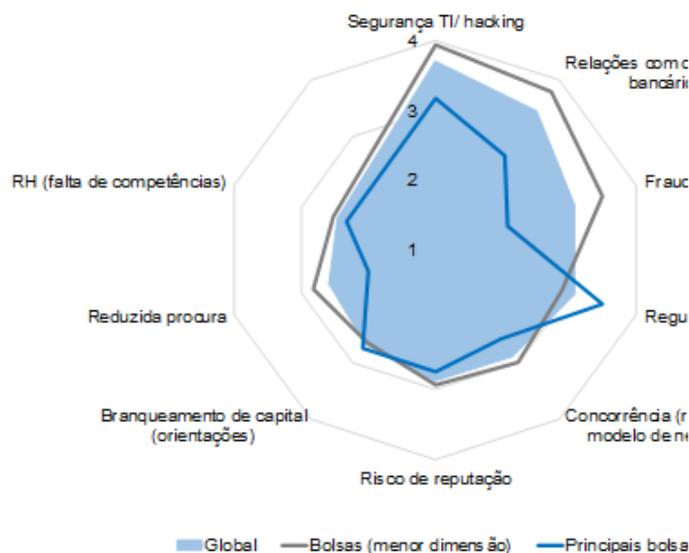


Fonte: <https://data.bitcoinity.org/>

Os principais riscos operacionais percebidos pelas bolsas de criptomoedas estão relacionados

com a segurança tecnológica (*hacking*), a deterioração das relações com os bancos, a regulação e o risco de fraude (CCAF, 2017).

Gráfico 13- Riscos operacionais percebidos pelas bolsas, N=51



Fonte: CCAF (2017)

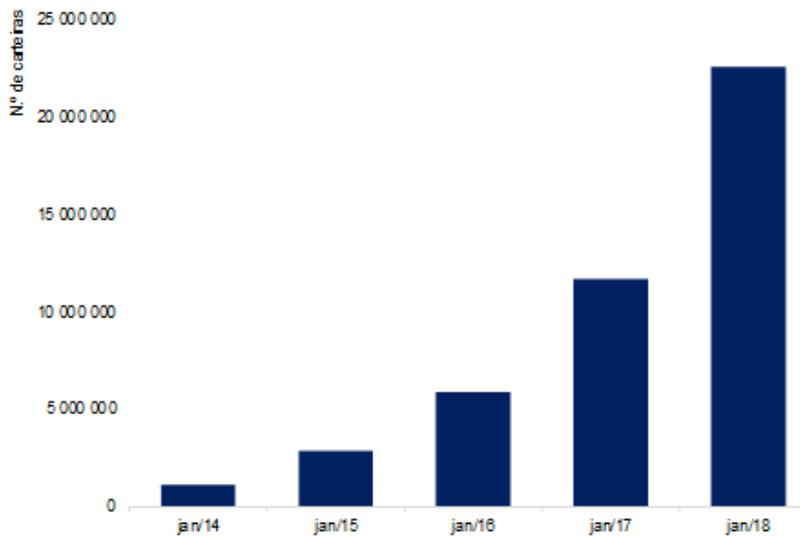
5. WALLETS

A *wallet* é um *software* usado para, de forma segura, armazenar, enviar e receber criptomoedas através da gestão de chaves públicas e privadas criptográficas, por um prestador de serviços. As entidades que prestam este tipo de serviço estão concentradas (CCAF, 2017) nos

Estados Unidos (34%) e na Europa, nomeadamente no Reino Unido (15%), na Alemanha (8%) e na Suíça (8%).

A percentagem de carteiras ativas num mesmo prestador do serviço pode variar entre 7,5% e 30,9%. O número de carteiras tem aumentado de forma expressiva (+93% de janeiro de 2017 para janeiro de 2018).

Gráfico 14- Evolução do número de carteiras

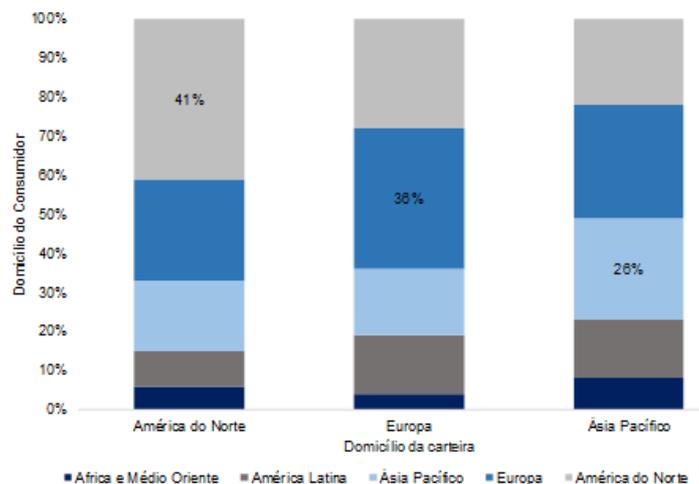


Fonte: <https://blockchain.info/>

Os utilizadores de *wallets* localizados na América do Norte e na Europa possuem preferência

pelos fornecedores localizados nessas reuniões. Na região da Ásia Pacífico apenas 26% da base de clientes é proveniente da mesma região.

Gráfico 15 - Domicílio das *wallets*, por região de residência do consumidor



Fonte: CCAF (2017)

Grande parte das *wallets* são *open sources* (o que significa que o código base está disponível para externos e permite o diagnóstico de eventuais vulnerabilidades) e oferecem diversos formatos, permitindo a interação com os utilizadores em diferentes contextos. O formato mais frequente permite o acesso conveniente através de um *smartphone*, existindo diversas *apps*

disponíveis (*i.e.*, formato *mobile*).

As *wallets* são atualmente programas sofisticados que suportam um grande número de funções. Aproximadamente 56% das *wallets* oferece serviços para além da armazenagem de criptomoedas. A tabela que se segue apresenta uma listagem desses serviços.

Tabela 3- Serviços oferecidos pelas *wallets*

Variável	Categoria	N	%
Conceção	Closed source	15	32%
	Open source	33	68%
Wallet format	Mobile	31	65%
	Desktop	20	42%
	Web	18	38%
	Tablet	15	31%
	Hardware	11	23%
Serviços oferecidos	Troca de moedas integrada	25	52%
	Ligação ao cartão de crédito	10	20%
	Recuperação de chave de acesso	8	16%
	Transações <i>0-fee off-chain</i>	8	16%
	Envio por email	8	16%
	Ligação ao cartão de débito	6	12%
	Seguro	4	8%
	Transações <i>0-fee on-chain</i>	4	8%
	Envio por sms	4	8%
	Serviço misto integrado	4	8%

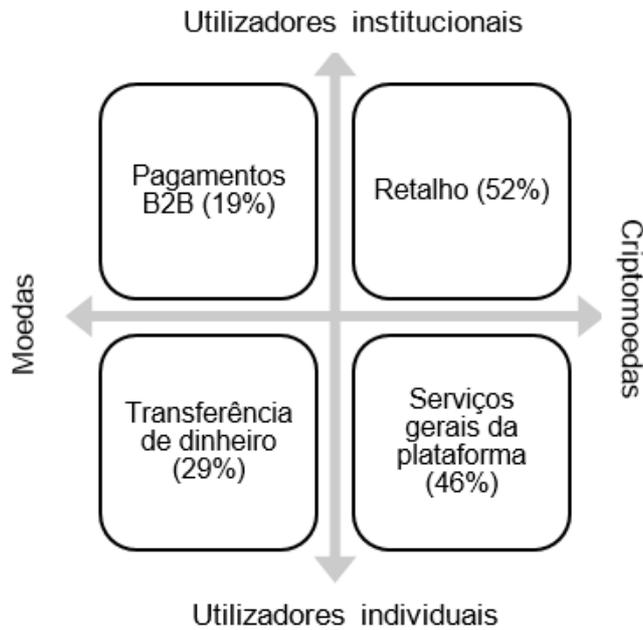
Fonte: CCAF (2017) N=26 wallets (90% setor)

6. PAYMENTS

O sistema de criptomoedas possui uma rede integrada de pagamentos para proceder às transações denominadas no *native token*.

O setor de pagamentos das criptomoedas pode ser organizado em quatro categorias de sistemas de pagamento (CCAF, 2017).

Figura 2- Sistema de pagamentos das criptomoedas e serviços oferecidos pelas plataformas de pagamento

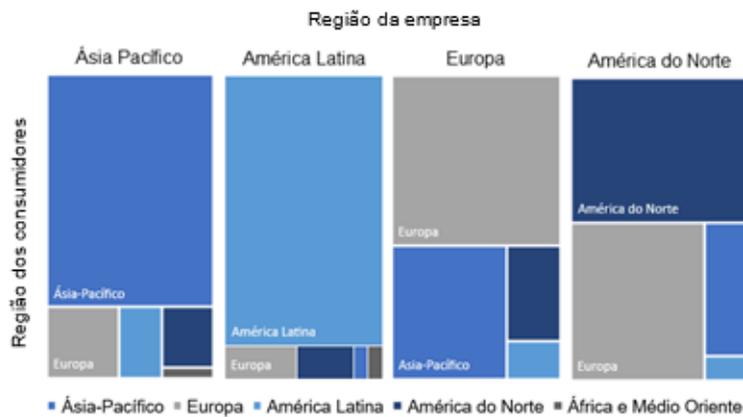


Fonte: adaptado a partir de CCAF (2017)

As empresas de pagamentos localizadas na região Ásia Pacífico e América Latina possuem essencialmente consumidores locais. As empre-

sas de pagamentos localizadas na Europa e na América do Norte possuem uma maior diversidade de clientes em termos geográficos.

Gráfico 16- Localização das empresas de pagamentos vs localização dos consumidores



Fonte: CCAF (2017)

Relativamente ao montante das transações, os pagamentos nacionais assumem em geral montantes mais reduzidos (44% das transações envolvem menos de \$100) e as transações internacionais estão associadas a valores mais elevados (34% assumem valores superiores a \$1.000) (CCAF, 2017).

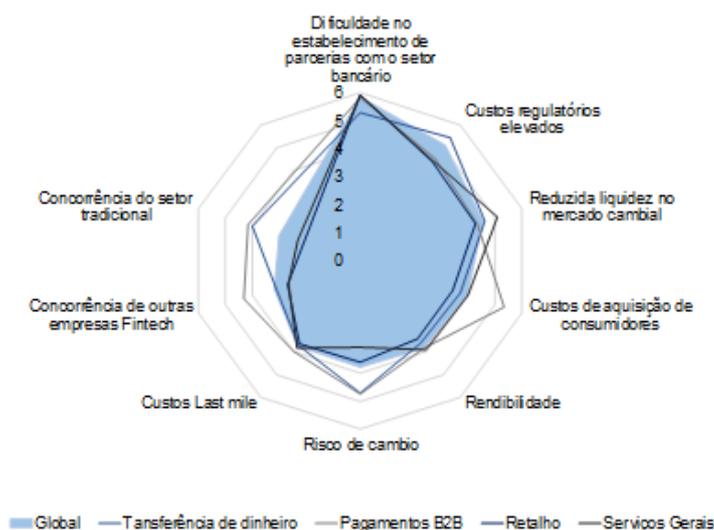
Em termos de canal de pagamento, os pagamentos no segmento *business-to-business* (B2B) assumem valores médios de \$1.878, no

segmento *consumer-to-consumer* (C2C) \$351 e no segmento *consumer-to-business* (C2B) \$210.

As empresas de pagamentos operam como portas de acesso entre as empresas, as finanças tradicionais e o sistema de criptomoedas.

Em termos gerais, a dificuldade no estabelecimento de parcerias com o setor bancário é considerado o principal desafio para as empresas que operam no segmento de pagamentos.

Gráfico 17- Principais desafios das empresas de pagamentos de criptomoedas



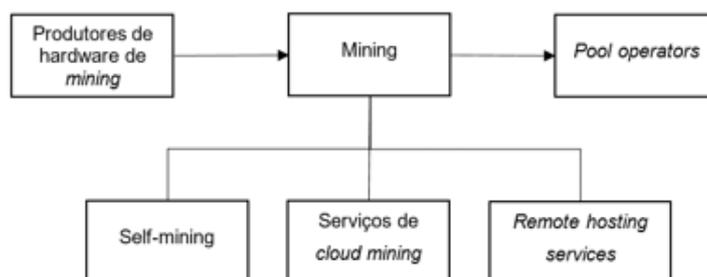
Fonte: CCAF (2017)

7. MINING

Os *miners* desempenham um papel fundamental no sistema de criptomoedas na medida em que são responsáveis por agrupar transações não confirmadas em novos blocos e de as adicionar ao *ledger* global (*blockchain*). Os *miners* oferecem os recursos computacionais (*computing power*) para assegurar a validade da *blockchain*, calculando um vasto número de *hashers* para descobrir um bloco válido. Cada bloco válido é

adicionado pelo *miner* ao *blockchain* em troca de uma recompensa.

O *mining* evoluiu de um simples *hobby* pelos *early adopters* nos computadores pessoais, para uma indústria intensiva que usa equipamento de *hardware* especializado. Podem ser identificados cinco tipos de intervenientes na atividade de *mining*, descritos na Figura 3 (CCAF, 2017): (i) produtores de *hardware* de *mining*; (ii) *pool operators*; (iii) *self-mining*; (iv) serviços de *cloud mining* (v) e *remote hosting services*.

Figura 3 - Cadeia de valor da atividade de *mining*

Fonte: CCAF (2017)

A atividade de *mining* pode ser efetuada por indivíduos ou por organizações, que usam o seu próprio equipamento para processar transações. Em troca, recebem uma recompensa pelo *mining* (*reward mining*) e comissões de transação (*transaction fees*).

As principais empresas de *mining* desenvolvem e mantêm centros de dados e de *mining* por todo o mundo. As *mining pools* combinam os recursos computacionais (*hashing power*) de diversos *miners* (indivíduos ou organizações) para aumentar a probabilidade e a frequência de identificação de um novo bloco. As *mining pools* tornaram-se atividades profissionalizadas, oferecendo diversos serviços para os consumidores. As recompensas são partilhadas pelos participantes, com base na proporção dos recursos computacionais partilhados.

Um conjunto reduzido de empresas dedicaram-se à conceção de equipamento de *mining* especializado.

Os serviços de *cloud mining* oferecem *hashing power* permitindo aos indivíduos participarem no processo de mineração sem terem necessidade de executar o equipamento eles próprios.

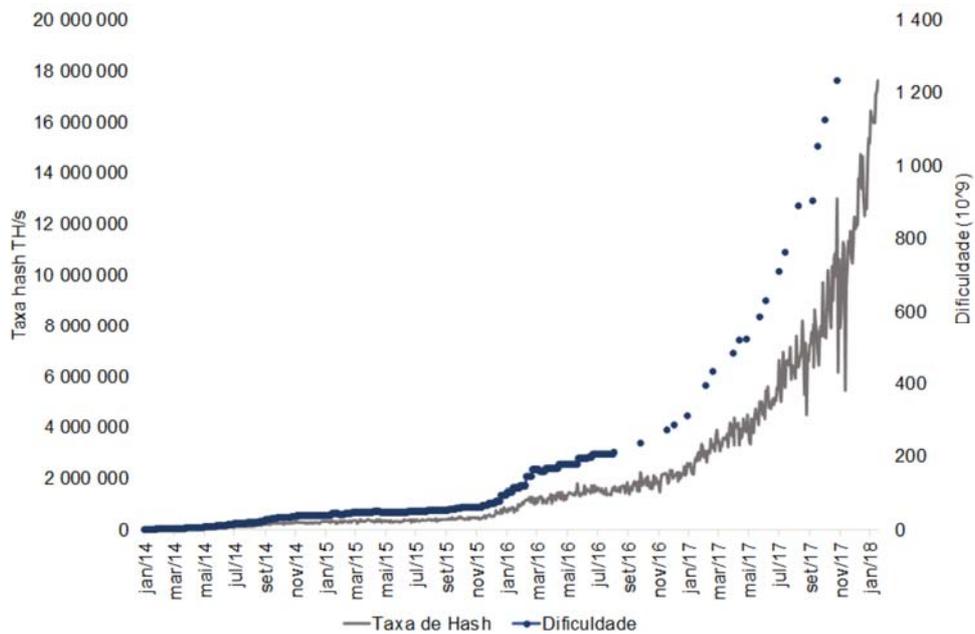
Por fim, os *remote hosting services* oferecem o armazenamento e manutenção do equipamento de *mining* detido por indivíduos.

A taxa de *hash* (*hash rate*) é uma unidade de medida da potência de processamento usada para resolver as operações matemáticas computacionalmente intensivas para a rede bitcoin (atuação coletiva dos mineradores de bitcoin). Esta taxa é assim definida como o número estimado de *terahashes* por segundo (trilhões de *hashes* por segundo) que a rede bitcoin é capaz de desempenhar.

A dificuldade de mineração mede o grau de dificuldade para decifrar um código para descobrir um *hash* abaixo ou acima de um valor esperado, i.e., para encontrar um dado bloco.

Para além da dificuldade de mineração, o custo computacional de mineração depende da tecnologia usada. Desde a introdução da bitcoin, terão sido usados pelo menos quatro gerações de equipamento de mineração: Central Processing Units (CPUs), Graphics Processing Units (GPUs), Field Programmable Gate Arrays (FPGAs) e ASIC – Application-Specific Integrated Circuits (Li e Wang, 2017).

Gráfico 18- Evolução da taxa de *hash* e da dificuldade da mineração, de janeiro de 2014 a janeiro de 2018

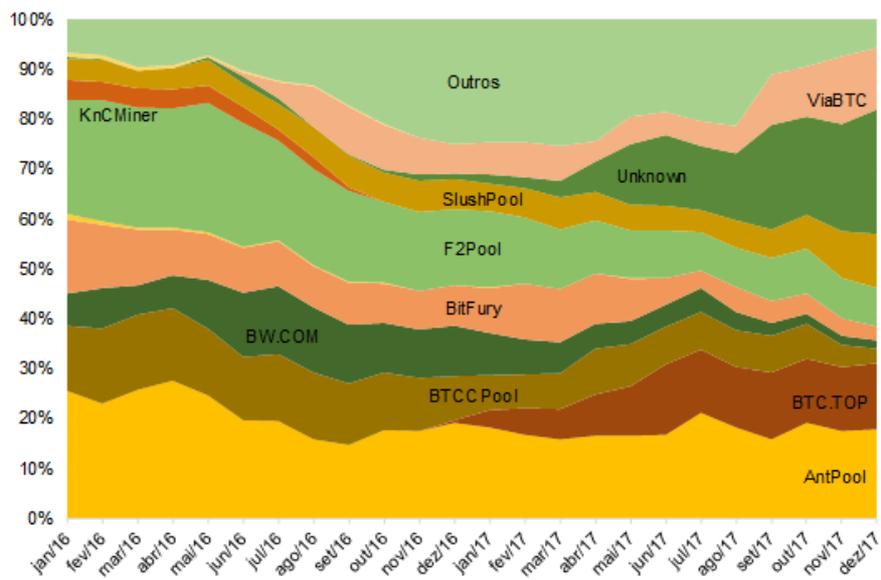


Fonte: Blockchain.info

Em termos de *mining blocks*, em janeiro de 2018 destacavam-se os seguintes *miners*: Ant Pool (China), BTC.com (China, USA, Europe),

Via BTC, BTC.TOP e Slush.com (Global). No ano de 2017 mais de metade das *pools* de mineração estavam localizadas na China (58%), seguidas dos USA (16%) - (CCAF, 2017).

Gráfico 19 - Quota de mercado das *pools* de mineração, de janeiro de 2016 a dezembro de 2017



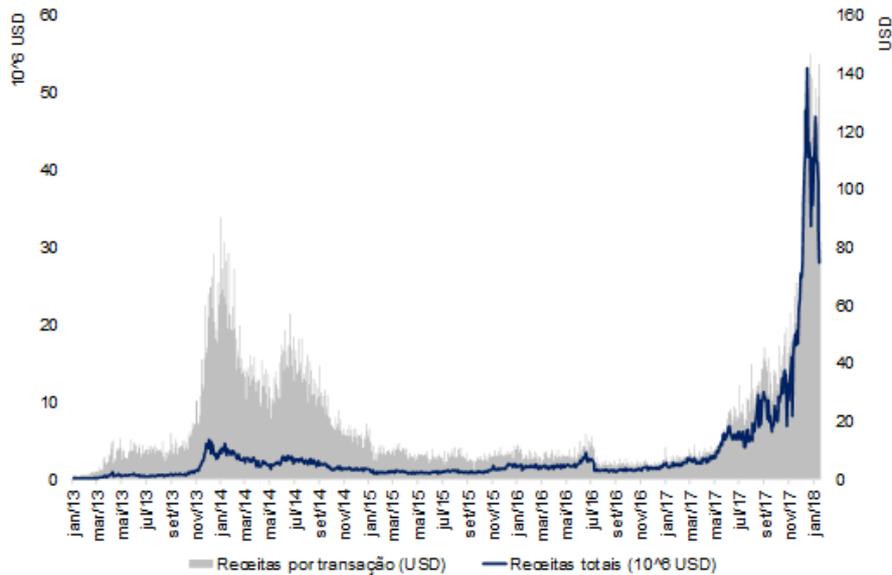
Fonte: data.bitcoinity.org

Apenas com a mineração de bitcoins, os *miners* terão recebido no período de janeiro de 2013 a dezembro de 2018 aproximadamente 3×10^9 USD. No entanto, estima-se que as receitas totais da indústria de *mining* sejam superiores (incluindo as receitas dos produtores de *hardware* e da oferta de serviços de *mining* e

cloud remotos).

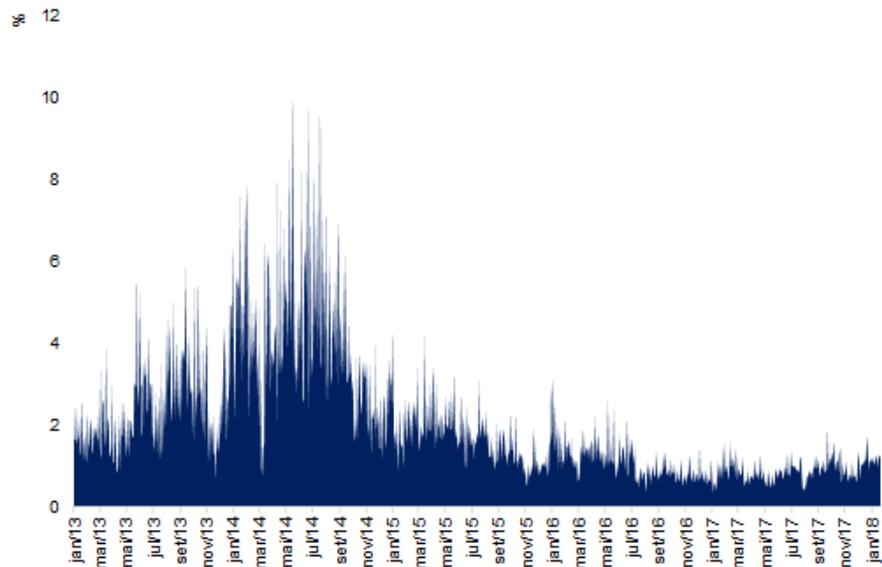
O ano de 2017 ficou marcado por um aumento das receitas por transação e globais. Não obstante, a receita da mineração como porcentagem do volume transacionado tem diminuído.

Gráfico 20- Evolução da receita total da mineração e da receita por transação



Fonte: Blockchain.info

Gráfico 21- Receita da mineração (% do volume transacionado)



Fonte: Blockchain.info

A tabela que se segue apresenta o protocolo do algoritmo *hash* das principais criptomoedas, bem como a velocidade e a capacidade.

Tabela 4- Algoritmo *hash* das principais criptomoedas

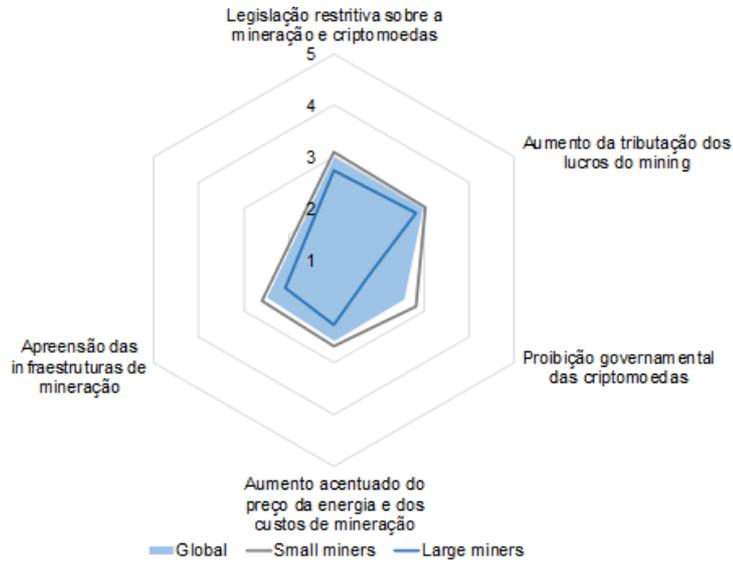
#	Cripto Moeda	Descrição	Algoritmo Hash	Oferta disponível
1	Bitcoin (BTC)	Digital gold	SHA-256	16,8M
2	Ripple (XRP)	Enterprise payment settlement network	SHA-512	38,7B
3	Ethereum (ETC)	Programmable contracts and Money	Ethash	96,5M
4	Bitcoin Cash (BCH)	Bitcoin clone	SHA-256	16,9M
5	Cardano (ADA)	Layered currency and contracts	Ouroboros	25,9B
6	Litecoin (LTC)	Faster Bitcoin	Scrypt	54,4M
7	IOTA (IOTA)	Internet-of-things payments	SHA-3	2,78B
8	NEM (XEM)	Batteries-included digital assets	Proof-of-importance	9,0B
9	Dash (DASH)	Privacy-focused Bitcoin clone	X11	7,77M
10	Stellar Lumens (XLM)	Digital IOUs	Proof-of-Stake	17,9B
11	Monero (XMR)	Private digital cash	Cryptonight	15,5M
12	NEO (NEO)	Chinese-market Ethereum Decentralized applications on	Delegate PoS	65M
13	EOS (EOS)	WebAssembly Ethereum contracts on	-	559M
14	Qtum (QTUM)	Bitcoin	Proof-of-Stake	73,8M
15	Bitcoin Gold (BTG)	GPU-only Bitcoin Clone	Equidash	16,7M
16	Verge (XVG)	Privacy Dogecoin	Scrypt	14,5B
17	Tron (TRX)	In-app Purchases Scalable	-	65,7B
18	RaiBlocks (XRB)	Digital Currency Madoff-like	Blake2b	133M
19	BitConnect (BCC)	Investment Fund	Scrypt	6,02M
20	Ethereum Classic (ETC)	Ethereum clone	Ethash	98,6M

Nota: As 20 criptomoedas foram selecionadas com base na respetiva capitalização bolsista
 Fonte: <https://www.crunchbase.com/>

Os principais riscos legislativos percecionados pelos *miners* são o surgimento de legislação restritiva sobre a mineração de criptomoedas e a

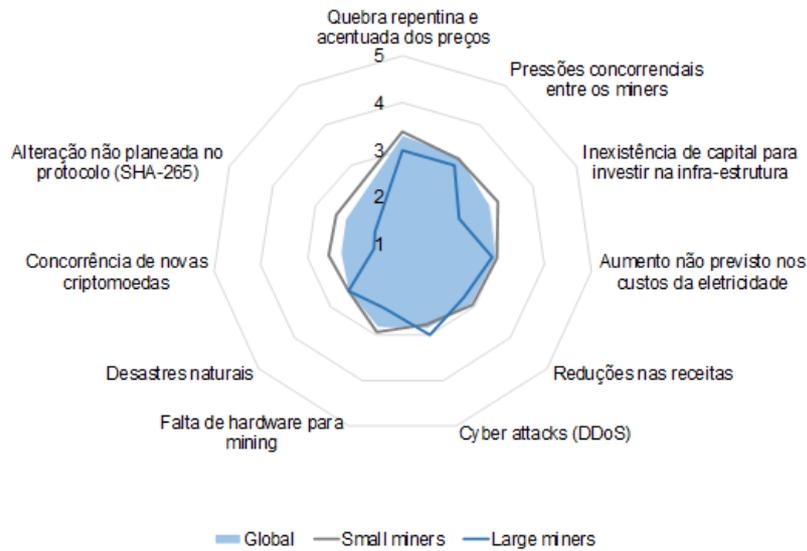
tributação da atividade de *mining*. Em termos de riscos operacionais, destaca-se a quebra repentina e acentuada de preços e as pressões concorrenciais entre os *miners*.

Gráfico 22- Riscos legislativos percecionados pelos *miners*



Fonte: CCAF (2017). N=48, 18 (38%) consideradas *large miners* (organizações) e 30 (62%) classificadas como *small miners* (*miners* individuais).

Gráfico 23- Riscos operacionais percecionados pelos *miners*



Fonte: CCAF (2017)

8. CONCLUSÕES

O mercado das criptomoedas registou no ano de 2017 um crescimento exponencial em termos de notoriedade, volume transacionado, capitalização bolsista e número de criptomoedas oferecidas.

Paralelamente, assistiu-se a um interesse da comunidade académica sobre o comportamento do preço das criptomoedas (e das bitcoins em particular). O preço das criptomoedas tem sido associado a fatores tecnológicos, variáveis macro-económicas, indicadores de atividade do mercado das bitcoins, preço de outros ativos e preço de outras criptomoedas.

Os utilizadores de criptomoedas são maioritariamente do sexo masculino e situam-se na faixa etária 25-34 anos, consultam o preço das criptomoedas frequentemente (todos os dias) e têm expectativas de retornos elevados no curto prazo. Os principais segmentos da indústria das criptomoedas são as *exchanges*, as *wallets*, os *payments* e o *mining*. De forma integrada, acrescentam valor ao mercado.

Os reguladores do setor financeiro têm emitido alertas aos utilizadores de criptomoedas atendendo, nomeadamente à sua volatilidade. Levantaram igualmente preocupações quanto aos riscos de branqueamento de capitais e de financiamento de transações ilegais. Atendendo ao volume transacionado, comparativamente ao de outros ativos, ser ainda reduzido, não existirão atualmente riscos para a estabilidade financeira (Baur et al., 2018).



REFERÊNCIAS

Bariviera, A. F. (2017). The inefficiency of bitcoin revisited: a dynamic approach. *Economics Letters*, 161, 1-4.

Baur, D. G., Dimpf, T., & Kuck, K. (2018). Bitcoin, gold and the US dollar – A replication and extension. *Finance Research Letters*, 25, 103-110.

Baur, D. G., Hong, K., & Lee, A. D. (2017). Bitcoin: medium of exchange or speculative assets? <https://ssrn.com/abstract=2561183> (acesso a 31 de janeiro de 2018).

BdP (2014). Alerta aos consumidores para os riscos de utilização de “moedas virtuais”, <https://www.bpportugal.pt/comunicado/alerta-aos-consumidores-para-os-riscos-de-utilizacao-de-moedas-virtuais> (acesso a 31 de janeiro de 2018).

Blau, B M. (2018). Price dynamics and speculative trading in Bitcoin. *Research in International Business and Finance*, 43, 15-21.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: economics, technology, and governance. *Journal of Economic Perspectives*, 29 (2), 213–38.

Bolt, W., & van Oordt, M. R., (2016). On the value of virtual currencies. <http://www.bankofcanada.ca/wp-content/uploads/2016/08/swp2016-42.pdf>

Bouri, E., Jalkh, N., Molnár, P. & Roubaud, D. (2017) Bitcoin for energy commodities before and after the December 2013 crash: diversifier, hedge or safe haven? *Applied Economics*, 49 (50), 5063-5073.

Brühl, V. (2017). Virtual Currencies, Distributed Ledgers and the Future of Financial Services. *Intereconomics*, 6, 370-378.

CCAF (2017). Global Cryptocurrency Benchmarking Study. Cambridge Centre for Alternative Finance. <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/global-cryptocurrency/#.WzC3szqWyUk> (acesso a 31 de janeiro de 2018).

Ciaian, P., Rajcaniova, M., & Kancs, D. (2016). The economics of Bitcoin price formation. *Applied Economics*, 48 (19), 1799-1815.

Ciaian, P., Rajcaniova, M., & Kancs, d'Artis (2018). Virtual relationships: Short- and long-run evidence from BitCoin and altcoin markets. *Journal of International Financial Markets, Institutions and Money*, 52, 173-195.

Corbet, S., Lucey, B., & Yarovya, L. (2017). Datestamping the Bitcoin and Ethereum bubbles. *Finance Research Letters*, doi:10.1016/j.frl.2017.12.006

Dwyer, G. P. (2015). The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability*, 17, 81–91.

Dyhrberg, A.H. (2016). Bitcoin, gold and the dollar – a Garch volatility analysis. *Finance Research Letters*, 16, 85-92.

EBA (2013). EBA warns consumers on virtual currencies. EBA Press Release. <https://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies> (acesso a 31 de janeiro de 2018).

EC (2018). The Digital Agenda of Virtual Currencies. http://publications.jrc.ec.europa.eu/repository/bitstream/JRC97043/the%20digital%20agenda%20of%20virtual%20currencies_final.pdf (acesso a 31 de janeiro de 2018).

ECB (2015). Virtual currency schemes – a further analysis. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> (acesso a 31 de janeiro de 2018).

REFERÊNCIAS

- EY (2017). EY Research: initial coin offerings. <http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/%24File/ey-research-initial-coin-offerings-icos.pdf> (acesso a 31 de janeiro de 2018).
- Gandal, N., Hamrick, J.T., Moore, T., & Oberman, T. (2018). Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics*, 95, 86-96.
- Hayes, A. S. (2017). Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. *Telematics and Informatics*, 34 (7), 1308-1321.
- Katsiampa, P. (2017). Volatility estimation for bitcoin: A comparison of GARCH models. *Economic Letters*, 158, 3-6.
- Kim, T. (2017). On the transaction cost of Bitcoin. *Finance Research Letters*, 23, 300-305.
- Kristoufek, L. (2015). What are the main drivers of the bitcoin price? Evidence from wavelet coherence analysis. *PLoS One*, 10(4), e0123923.
- Li, X., & Wang, C. A. (2017). The technology and economic determinants of cryptocurrency exchange rates: The case of bitcoin. *Decision Support Systems*, 95, 49-60.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf> (acesso a 31 de janeiro de 2018).
- Rogojanu, A., & Badea, L. (2014). The issue of competing currencies. Case study–bitcoin, *Theoretical Applications Economics*, 21(1), 103–114.
- Tiwari, A. K., Jana, R. K., Das, D., & Roubaud, D. (2018). Informational efficiency of Bitcoin – An extension. *Economic Letters*, 163, 106-109.