



Instituto Universitário de Lisboa

Escola de Ciências Sociais e Humanas
Departamento de Economia Política

Moeda Digital.
Uma exploração bibliométrica do fenómeno Bitcoin

Luís Manuel Andrade Paixão

Dissertação submetida como requisito parcial para obtenção do grau de
Mestre em Economia Monetária e Financeira

Orientador:
Prof. Doutor Sandro Mendonça, Professor Auxiliar
ISCTE-Instituto Universitário de Lisboa

Coorientador:
Doutor Elias Veiga Pereira, Banco de Cabo Verde

Outubro 2018

Agradecimentos

Um trabalho de mestrado é uma longa caminhada, que inclui uma trajetória cheia de desafios, emoções, incertezas, tristezas, alegrias e muitos percalços pelo caminho, mas, contudo, e apesar do trabalho desafiante a que qualquer investigador está destinado, junta contributos de várias pessoas.

Caminhar por este trilho só foi possível com o apoio e energia de várias pessoas a quem dedico este trabalho de investigação.

Agradeço:

À minha família, em especial à minha avó e á minha madrinha, por estarem sempre dispostas a ajudar a concretizar os meus sonhos e objetivos e nunca me deixarem desistir, às minhas primas Rosa e Elisabete e ao meu afilhado Salvador que é uma fonte de energia.

Ao meu melhor amigo, Henrique Melrinho, pela força, incentivo e por sempre acreditar em mim, obrigado por toda a tua amizade e apoio de sempre.

Ao meu orientador, Professor Dr. Sandro Mendonça, pela orientação exemplar pautada por um elevado e rigoroso nível científico, um interesse permanente e fecundo, uma visão crítica e oportuna, um empenho incedível e saudavelmente exigente, os quais contribuíram para enriquecer, com grande dedicação, passo por passo, todas as etapas subjacentes ao trabalho realizado.

Ao Coorientador, Dr. Elias Veiga Pereira, pelo apoio prestado.

Aos meus amigos mais próximos, colegas de faculdade, antigos colegas de trabalho, e restante família, o meu muito obrigado também, um obrigado especial aqueles que sempre me incentivaram, acreditaram e nunca me deixaram desistir apesar de tantos obstáculos encontrados nesta caminhada.

Por último e o mais importante, obrigado à minha mãe, espero que estejas onde estiveres, tenhas orgulho, pois tudo o que faço é para te deixar orgulhosa como se estivesses presencialmente comigo, obrigado pela educação que me deste, sei que estás diariamente comigo nas batalhas, obrigado, isto é, por ti!

A todos vocês que estão comigo no dia-a-dia, o meu muito obrigado!

Resumo

Num mundo cada vez mais globalizado, temos vindo a assistir à emergência da moeda digital e do seu potencial para aumentar a eficiência dos sistemas de pagamento existentes. No entanto, o dinheiro digital pode também ocultar riscos sérios que se podem transformar em perdas financeiras significativas para os seus utilizadores. Perante este cenário os bancos centrais estão preocupados com a manutenção da estabilidade e eficiência do sistema financeiro e em preservar a confiança nas suas moedas, pois as inovações nos pagamentos podem ter implicações importantes para a segurança do sistema bancário.

Com o presente estudo pretende-se efetuar uma revisão sistemática do atual estado da arte da literatura científica sobre a moeda digital, focada sobretudo no caso específico da *bitcoin*, de modo a investigar a forma como este fenómeno tem sido estudado até à presente data. Tendo como base uma síntese crítica sobre os resultados obtidos, nomeadamente o *locus* e foco das questões, teorias, métodos e descobertas abordados na literatura pesquisada, pretende-se contribuir para a construção de uma visão mais integrada de um fenómeno que se encontra em expansão.

Para o efeito, foi utilizada uma abordagem metodológica quantitativa, a qual proporciona ao leitor uma visão mais abrangente da temática abordada. Foi selecionado um *corpus* de 140 artigos publicados em fontes indexadas no site *Scopus*, com o qual foi construída uma base de dados. Essa base de dados serviu depois para efetuar uma análise bibliométrica para estudar a evolução do estado da arte sobre a *bitcoin* por parte da literatura científica.

Palavras-Chave: Moeda digital; Mercado monetário; Segurança monetária; Bitcoin; Comércio eletrónico, Pagamento eletrónico.

Classificação JEL: E41, E42, E51, E52

Abstract

In an increasingly globalized world, we have been witnessing the emergence of digital currency and its potential to increase the efficiency of existing payment systems. However, digital money can also hide serious risks that can turn into significant financial losses for its users. Against this background, central banks are concerned about maintaining the stability and efficiency of the financial system and maintaining confidence in their currencies, as innovations in payments can have important implications for the security of the banking system. In addition, there is great uncertainty about what will be the economic benefit of the digital currency and its effects on the effectiveness of monetary policy.

With the present study we intend to carry out a systematic review of the current state of the art of the scientific literature on digital currency, focused mainly on the specific case of bitcoin, in order to investigate the way this phenomenon has been studied to date. Based on a critical synthesis of the results obtained, namely the locus and focus of the issues, theories, methods and discoveries addressed in the researched literature, it is intended to contribute to the construction of a more integrated vision of a phenomenon that is expanding.

For this purpose, a quantitative methodological approach, which provides the reader with a more comprehensive view of the subject matter, was used. A corpus of 140 research studies published in sources indexed in the *Scopus* was selected, with which a database was built. This database was then used to perform a bibliometric analysis to study the evolution of the state of the art on Bitcoin by the scientific literature.

Keywords: Digital Money; Money Market; Money Security; Bitcoin; E-Commerce: E-Payment.

JEL (Classification system): E41, E42, E51, E52

Índice

Agradecimentos	i
Resumo	ii
Abstract	iii
Índice de Gráficos	v
1. Introdução	1
2. Revisão de literatura sobre moeda digital	4
2.1. Moeda Digital.....	4
2.1.1. Principais características e utilizações da moeda digital	7
2.1.2. Bitcoin	8
2.1.3. Segurança da moeda digital – a tecnologia <i>Blockchain</i>	12
2.2. <i>E-Payment</i> e <i>E-Commerce</i>	13
2.2.1. <i>PayPal</i>	15
3. Metodologia	17
4. Estudo empírico	20
4.1. Análise dos dados.....	20
4.2. Discussão dos resultados.....	29
5. Conclusões	32
Bibliografia	33
Listagem das referências bibliográficas do corpus de estudos analisados.....	40
Anexos	52

Índice de Gráficos

Gráfico 1 – Inflação monetária da Bitcoin entre 2010 e 2060.....	10
Gráfico 2 – Distribuição dos estudos por anos de publicação	20
Gráfico 3 – Áreas Científicas.....	21
Gráfico 4 – Tópico Científico Principal.....	22
Gráfico 5 - Palavras-chave do autor.....	23
Gráfico 6 - Tópicos Científicos Controlados	24
Gráfico 7 - Tópicos Científicos não Controlados	25
Gráfico 8- Áreas Científicas dos 20 artigos mais citados	25
Gráfico 9 - Tópico científico principal (TOP20)	26
Gráfico 10 - Palavras-chave do autor (TOP20)	27
Gráfico 11 - Tópicos científicos controlados (TOP20).....	27
Gráfico 12- Tópicos científicos não controlados (TOP20).....	28
Gráfico 13 - Classificação dos quartis dos artigos analisados.....	28

1. Introdução

O progresso científico e tecnológico que se tem verificado nos últimos anos e o subsequente desenvolvimento da economia virtual, está a reconfigurar as relações comerciais tradicionais. Assim, num mundo cada vez mais globalizado, temos vindo a assistir à emergência da moeda digital que tem potencial para aumentar a eficiência dos sistemas de pagamento convencionais. Diversas abordagens estão a surgir com o objetivo de tornar os pagamentos mais fáceis e mais rápidos, à medida que fenómenos como o *e-money* e o *e-commerce* se estão a desenvolver, os quais apresentam algumas vantagens em comparação com o comércio tradicional e convencional (Tsukerman, 2015). No entanto, esses fenómenos podem também ocultar riscos sérios que se podem transformar em perdas financeiras significativas para seus utilizadores. Por exemplo, ativos digitais, como a *bitcoin*, podem possuir características monetárias, podendo ser usados como meio de pagamento, mas normalmente não estão relacionados com uma moeda soberana. Além disso, ela tem zero valor intrínseco e a sua valorização depende da convicção de que pode ser trocado por outros bens ou serviços, ou por uma certa quantidade de moeda soberana (Ciaian et al., 2016). Perante este cenário os bancos centrais estão preocupados com a manutenção da estabilidade e eficiência do sistema financeiro e em preservar a confiança nas suas moedas, pois as inovações nos sistemas de pagamentos podem ter implicações importantes para a segurança do sistema bancário, bem como implicações sobre os mecanismos de propagação da política monetária (Banque de France, 2013).

Atualmente, assiste-se à crescente valorização da *bitcoin* nos mercados financeiros mundiais, a qual atingiu em dezembro de 2017 o nível histórico mais elevado, tendo a sua cotação ultrapassado a barreira dos 15.000 US\$ / 1 BTC, quando, por exemplo, em meados de 2015, uma *bitcoin* valia pouco mais de 200 dólares¹. Em julho de 2017, o banco suíço Falcon Private Bank tornou-se no primeiro banco convencional a oferecer *bitcoins* para os seus clientes mais ricos (Ferreira, 2017). O dinheiro eletrónico tem vindo a tornar-se numa tendência cada vez mais generalizada entre os consumidores mundiais que se habituaram a usá-lo para pagar as suas compras de forma simples e rápida, sendo o *PayPal* um dos sistemas mais populares. Em Portugal, o sistema de pagamentos móveis MB WAY, que permite fazer pagamentos e

¹ /www.coindesk.com/price/

transferências imediatas através do telemóvel, usando como referência o número de telemóvel do destinatário, tem vindo a ganhar cada vez mais adeptos, sobretudo entre as camadas jovens da população².

A crescente introdução de vários tipos de aplicações para transferência de dinheiro e sistemas para facilitar os processos de transação e pagamentos *online* é algo que tem vindo a despertar o interesse desde há algum tempo a esta parte. O uso da tecnologia móvel, que se generalizou nos últimos anos, particularmente entre as camadas mais modestas da população, que até então não tinha acesso a serviços financeiros, fez com que o dinheiro digital e os pagamentos eletrónicos funcionassem como um meio de inclusão financeira (Braga et al., 2013). A utilização dessas aplicações está aumentando de dia para dia, principalmente entre os adolescentes que não gostam de se deslocar a bancos para realizarem simples transações monetárias e recorrem a essas aplicações que lhes tornaram a vida mais fácil e simples (Cassoni & Ramada, 2013). Assim, ao aprofundarmos a análise desta realidade, apercebemo-nos da existência de muitos estudos a serem desenvolvidos no mundo real, em muitos pontos geográficos e em muitas camadas financeiras (Atzei et al., 2018; Bação et al., 2018; Chetterjee et al., 2018; Conoscenti et al., 2018; Delgado-Segura et al., 2018; Derks et al., 2018; Ferreira et al., 2018; Gatteschi et al., 2018; Hotz-Behofsits et al., 2018; Jirgensons & Kapenieks, 2018). No entanto, estes estudos só permitem olhar para um ponto circunstanciado da problemática. Com esta premissa em vista resolveu-se efetuar este estudo, uma meta-análise que pretende olhar ao mesmo tempo para tudo, ou seja, abranger todos os aspetos desta problemática, mas através da literatura.

Assim, foi formulada a seguinte pergunta de investigação: Como é que o fenómeno da moeda digital tem sido estudado na literatura académica relevante?

Pretende-se, com base nos resultados obtidos, contribuir para desenvolver uma visão integrada desta nova tendência que é pouco conhecida nos seus vários aspetos, que são muitos.

Para atingir o objetivo proposto – analisar a evolução da literatura académica sobre esta problemática e a forma como ela tem sido estudada – foi reunido um *corpus* de artigos académicos (com a data de referência de 30 de setembro de 2018) publicados em fontes indexadas ao site *Scopus*, cuja pesquisa foi efetuada com recurso à palavra-chave “*bitcoin*”. A partir dos resultados obtidos foram selecionados 140 artigos, tendo como critério de seleção o

² <https://acarteira.pt/poupanca/mbway/>

número de vezes que os mesmos foram citados. A pesquisa privilegiou os artigos que obtiveram o maior número de citações, e cuja influência/impacto científico foi mais relevante.

Esta dissertação encontra-se estruturada em cinco capítulos. O capítulo 1 destina-se a apresentar a introdução da dissertação, os motivos que estiveram subjacentes à escolha desta temática, a pergunta de investigação e o objetivo da dissertação, assim como a forma como a mesma se encontram organizada. No capítulo 2 é feita uma revisão qualitativa da literatura mais relevante sobre moeda digital com a finalidade de enquadrar teoricamente o estudo. A metodologia aplicada neste estudo é apresentada no capítulo 3. No capítulo 4 são discutidos os resultados preliminares do estudo e, finalmente, no capítulo 5 são apresentadas as conclusões.

2. Revisão de literatura sobre moeda digital

2.1. Moeda Digital

No site do Banco Central Europeu, é possível ler-se a definição de *e-money* que podemos traduzir como dinheiro eletrónico ou moeda digital, o qual consiste no armazenamento eletrónico de ativos monetários num dispositivo tecnológico que pode ser usado para efetuar pagamentos a entidades sem serem as que emitem o dinheiro eletrónico. O dispositivo funciona como um meio pré-pago que não necessita de envolver contas bancárias nas transações. Estes ativos podem ser baseados em hardware ou em software, dependendo da tecnologia usada para armazenar o valor monetário (Banco Central Europeu, 2018). Quando se trata de produtos baseados em hardware, o poder de compra reside num dispositivo físico pessoal, como um cartão com um chip, com recursos de segurança baseados em hardware. Os valores monetários geralmente são transferidos por meio de dispositivos que não precisam de conectividade de rede em tempo real a um servidor remoto (Cassoni & Ramada, 2013; Chiu & Wong, 2014). Por outro lado, *e-money* baseado em software utiliza um software especial que funciona em dispositivos pessoais comuns, como computadores pessoais, *tablets* ou *smartphones*. Para poder realizar a transferência de valores monetários, esse dispositivo pessoal geralmente precisa estabelecer uma conexão on-line com um servidor remoto que controla o uso do poder de compra. Também existem sistemas que misturam recursos baseados em hardware e software (ECB, 2018). De acordo com a Diretiva 2009/110/CE do Parlamento Europeu e do Conselho, datada de 16 de setembro de 2009, a “definição de moeda eletrónica deverá abranger tanto a moeda eletrónica mantida num dispositivo de pagamento na posse do utilizador da moeda eletrónica como a que é armazenada eletronicamente num servidor e gerida pelo utilizador de moeda eletrónica através de uma conta específica para moeda eletrónica”. Verifica-se, assim, que houve da parte da União Europeia uma preocupação em estabelecer uma definição para a moeda digital que fosse suficientemente ampla de modo a prevenir quaisquer entraves à inovação tecnológica e incluir não só todos os produtos de moeda digital disponíveis no mercado à data da emissão desta diretiva, mas também os que viessem eventualmente a desenvolver-se mais tarde (Jornal Oficial da União Europeia, 2009).

Segundo o Committee on Payments and Market Infrastructures³, a moeda digital constitui uma inovação que poderá ter uma série de impactos em muitas áreas, especialmente nos sistemas e serviços de pagamento. Esses impactos podem incluir a interrupção dos modelos e sistemas de negócios existentes, bem como o surgimento de novas interações e vínculos financeiros, económicos e sociais. Mesmo que os atuais esquemas de moeda digital não persistam, é provável que outros esquemas baseados nos mesmos procedimentos subjacentes e na mesma tecnologia continuem a surgir e a desenvolver-se (CPMI, 2015). De acordo com o relatório deste comité intitulado *Digital currencies*, o aspeto patrimonial das moedas digitais tem algumas semelhanças com análises levadas a cabo nos finais dos anos 90 sobre o desenvolvimento do dinheiro eletrónico que poderia competir com o banco central e com moedas soberanas. No entanto, ao contrário do *e-money* tradicional, as moedas digitais não são uma responsabilidade de um indivíduo ou instituição, nem são apoiadas por uma autoridade. Além disso, elas têm zero valor intrínseco e, como resultado, o seu valor deriva apenas da crença de que poderão, posteriormente, ser trocadas por outros bens ou serviços, ou uma certa quantidade de moeda soberana. Assim, os detentores de moeda digital podem enfrentar custos e perdas substancialmente maiores associados ao risco de preço e liquidez do que os detentores de moeda soberana (CPMI, 2015).

A noção de pagamentos eletrónicos não é tão recente como se supõe. A primeira pessoa a ter essa ideia terá sido provavelmente o investigador e escritor de ficção Edward Bellamy (1889). Na sua novela futurista *Looking Backward: 2000–1887*, cuja primeira edição data de 1888, Bellamy concebeu uma sociedade utópica onde o dinheiro – numerário – não é usado. Os pagamentos eram efetuados com uma espécie de cartão pré-pago marcado com valores nominais, o qual era utilizado para fazer compras em lojas, pagar estadias em hotéis, refeições em restaurantes, etc., permitindo ao leitor olhar diretamente para o futuro (Bellamy, 1889).

Segundo Tedeev (2005), as primeiras redes de dinheiro eletrónico começaram a ser desenvolvidas em 1993, quando o criptógrafo David Chaum organizou o primeiro sistema de pagamento eletrónico chamado *Digicash*, que permitia efetuar pagamentos de forma anónima, mas com segurança para os vendedores e compradores. Este projeto, no entanto, não teve

³ O Comité de Pagamentos e Infraestruturas de Mercado (CPMI) é um órgão de governação pertencente ao Conselho do Banco Central Europeu que promove a segurança e a eficiência do pagamento, compensação, liquidação e acordos relacionados, apoiando assim a estabilidade financeira e a economia em geral. O CPMI monitoriza e analisa os desenvolvimentos nesses acordos, dentro e entre jurisdições. Ele também serve como um fórum para a cooperação do banco central em assuntos de supervisão, política e operacionais relacionados, incluindo a prestação de serviços do BCE.

grande divulgação e David Chaum foi forçado a vender as suas patentes. Mais tarde os bancos começaram a interessar-se por este produto. O primeiro banco virtual que realizou atividades bancárias exclusivamente através Internet foi criado em 1994, com um projeto de cartão de crédito da rede dos EUA. A base tecnológica dessas operações bancárias foi um simples e-mail. Este sistema utilizava uma rede segura onde eram introduzidos os números de pagamento eletrónico e os números de cartão de crédito dos clientes, emitindo depois um número de identificação para pagar as compras eletrónicas. Os dados nunca saíam dessa rede (Tedeev, 2005). O banco britânico Barclays foi o primeiro grande banco europeu a abrir um negócio online, em fevereiro de 1995. Nesta primeira loja virtual os clientes do banco podiam adquirir vinho, brinquedos e bilhetes de comboio, usando os números dos seus cartões de crédito bancário para pagar esses bens, que eram mais tarde entregues por correio. O projeto permitiu que o Barclays Bank passasse a efetuar operações bancárias através da Internet (Tedeev, 2005). Enquanto a informatização da banca tradicional prosseguia, surgiu uma nova estratégia de automação. O primeiro projeto desenvolvido foi no campo dos serviços de crédito. Quando as corporações começaram a desenvolver programas bancários domésticos, a Microsoft teve a ideia de conceber pagamentos eletrónicos para gerir estratégias de finanças pessoais. A implementação de vários tipos de atividade económica no e-business levou ao uso extensivo de múltiplas versões do dinheiro eletrónico (Tedeev, 2005).

Num artigo publicado em 1995, Crede (1995) alertava para a existência de uma tendência para o desenvolvimento de dinheiro eletrónico por parte de organizações não bancárias. No entanto, segundo as previsões da época, existia a probabilidade de, num futuro próximo, o desenvolvimento do dinheiro digital se realizasse sob o patrocínio dos bancos. Tais estruturas têm muitas vantagens competitivas: a sua base de clientes, vastos recursos financeiros e experiência em atividades financeiras (Cassoni & Ramada, 2013). Este sistema provou ser tão bem-sucedido que os seus princípios fundamentais rapidamente se generalizaram em todo o mundo. Com recurso ao dinheiro digital, tornou-se mais rápido fazer transferências financeiras para qualquer local do globo, efetuar pagamentos de serviços públicos, serviços de telefone e televisão, serviços de internet, e assim por diante (Chiu & Wong, 2014).

2.1.1. Principais características e utilizações da moeda digital

A moeda digital, ou seja, os meios de pagamento digitais, são negociados eletronicamente, cujo volume de negócios garante anonimato. Os documentos eletrônicos contêm o valor nominal, uma indicação das características individuais do emissor (número de série, etc.) e elementos de proteção contra falsificação (a garantia da assinatura digital do emissor) (Miller et al., 2002). As moedas digitais baseadas na utilização da tecnologia *blockchain* representam um desenvolvimento genuinamente novo no que se refere a pagamentos (Barber et al, 2012; Chilton et al, 2016). No entanto, muitos dos fatores que estimularam o desenvolvimento das moedas digitais, também estimularam a inovação em métodos de pagamento mais tradicionais. O custo reduzido e o aumento da velocidade, inclusive nas áreas de comércio eletrônico e transações internacionais, são alguns dos fatores que sustentam o desenvolvimento da moeda digital e a inovação de um sistema de pagamento mais amplo. Em particular, vale a pena destacar o papel da tecnologia ao incentivar o desenvolvimento de moedas digitais e outras inovações (Huumo et al., 2016). Segundo o relatório *Digital currencies* (CPMI, 2015), no que se refere aos pagamentos de retalho, os avanços tecnológicos representaram um fator-chave que despoletou várias mudanças significativas nos serviços de pagamento, com impacto tanto na demanda quanto na oferta desses serviços. No entanto, também existem vários fatores que são mais idiossincráticos, no que concerne às moedas digitais baseadas na tecnologia *blockchain*, e que estão relacionados com as suas propriedades descentralizadas. São eles o fornecimento, a procura e a regulação (CPMI, 2015).

O dinheiro eletrônico oferece a máxima flexibilidade na implementação de pagamentos de pequenos montantes. Pode ser utilizado para pagamento de pequenas despesas como, por exemplo, deslocamentos, bilhetes de cinema e outros espetáculos, ou até mesmo multas, impostos e ordens judiciais. É particularmente útil para efetuar compras na internet, tanto de produtos tradicionais, como tecnológicos, por exemplo, licenças de software (Chiu & Wong, 2014; Fung et al., 2014). Os processos de pagamento com dinheiro eletrônico são rápidos e os valores podem ser transferidos do pagador para o destinatário em segundos, de forma semelhante ao dinheiro tradicional. As transferências bancárias são, normalmente, personificadas, e os detalhes legais de ambas as partes são conhecidos ou, no caso de indivíduos, números de identificação e endereços (Miller et al., 2002).

2.1.2. Bitcoin

A *bitcoin* é uma moeda digital – uma criptomoeda⁴ - que foi projetada tendo em vista o recente cenário do mercado global. A *bitcoin* foi criada em 2009, por Satoshi Nakamoto, um informático cuja verdadeira identidade permanece desconhecida (Nakamoto, 2009). O conceito por trás da *bitcoin* é a criação da versão digital de uma moeda que é mais difícil de falsificar do que as moedas tradicionais. É um ativo que ultrapassa as fronteiras internacionais e que pode ser armazenado no disco rígido de um computador em vez de um banco. Segundo Greenberg (2011), a *bitcoin* é como ouro, sendo que o seu valor deriva em parte da sua escassez e pode ser “minerada” através de um programa de “mineração”, cuja execução requer vários computadores a trabalharem em rede, executando complexas operações matemáticas destinadas a calcular uma função de criptografia denominada *hash* num conjunto de números aleatórios. O número de *bitcoins* produzidos é rigorosamente controlado e o software que permite a sua criação está desenhado para reduzir a produção ao longo do tempo, para que nunca haja mais de 21 milhões de *bitcoins* em circulação (Greenberg, 2011).

Num artigo publicado em dezembro de 2013 na revista *Focus*, o Banco de França alertava para o perigo que representa a emergência das moedas virtuais [digitais], dando o exemplo da *bitcoin* (Banque de France, 2013). Segundo os especialistas do Banco de França (2013) a *bitcoin* é uma moeda virtual que não se encontra regulamentada, a qual se apresenta como uma alternativa às moedas oficiais, mas que, no entanto, não oferece qualquer garantia de reembolso (Banque de France, 2013). Neste artigo são frisados alguns perigos relacionados com a ascensão da Bitcoin, nomeadamente a questão do anonimato inerente a estas transações, o que significa que, na prática, esta moeda pode ser usada para contornar o combate ao branqueamento de capitais e das regras de financiamento antiterroristas (Banque de France, 2013).

Segundo Hespeler (2008), a moeda digital, nomeadamente a *bitcoin*, apresenta algumas vantagens em relação ao dinheiro tradicional, mas também podemos encontrar algumas desvantagens. Em muitos países os bancos centrais estão preocupados com o desenvolvimento da moeda eletrónica (Maltzahn & Westland, 2016). Para eles, a principal ameaça é a emissão descontrolada, bem como o risco de possíveis abusos. Para além disso, a moeda digital levanta

⁴ Uma criptomoeda é um ativo digital projetado para funcionar como um meio de troca que usa a criptografia e a tecnologia *blockchain* para proteger as transações financeiras, controlar a criação de unidades adicionais e verificar a transferência de ativos (Greenberg, 2011).

também uma série de questões adicionais relacionadas com procedimentos de tributação e lavagem de dinheiro (Chilton et al, 2016; Tsukerman, 2015; Reid & Harrigan, 2013).

Entre as vantagens mais referidas destaca-se a proteção de dados. Segundo Franco (2014), existe um risco baixo para os utilizadores da *bitcoin*, ou de outra moeda digital, no caso do parceiro de uma transação ser alvo de um ataque cibernético e perder dados financeiros ou pessoais dos seus clientes. Os utilizadores de *bitcoin* estão em risco apenas se os hackers tiverem acesso às suas chaves privadas. Em 2016, o custo médio dos ataques que resultaram em violação de dados atingiu US \$ 4 milhões. Naquele ano, os EUA e a Alemanha registaram o maior custo médio per capita, com valores rondando US \$ 221 e US \$ 213, respetivamente. Os custos variam consoante o setor que foi alvo do ataque. No caso das organizações de saúde e de educação os custos registados foram mais elevados (US \$ 355 e US \$ 246, respetivamente). Na maior parte dos casos, as violações de dados são executadas por *hackers* e utilizadores internos (Ponemon Institute, 2016). Em 2007, uma empresa de empréstimos de curto prazo – a Wonga - sofreu uma violação significativa de dados, de que resultaram comprometidas as informações privadas de cerca de 245.000 clientes, incluindo números de contas bancárias, nomes completos, endereços de e-mail, endereços residenciais, números de telefone e os últimos quatro dígitos dos números de cartão de débito (Dumitrescu, 2017).

As taxas de transação mais baixas, são outras das vantagens apontadas. Com efeito, as taxas para transações em *bitcoins* são menores do que as do cartão de crédito. Hayes (2016) refere que uma transação com um valor de US \$ 100, efetuada com um cartão de crédito tem um custo de US \$ 3,37, enquanto que uma transação em *bitcoins* de valor similar custaria no máximo cerca de US \$ 0,61, tornando os cartões de crédito cerca de 5 vezes e meia mais caros para essa operação. A esse respeito, Vigna e Casey (2016) consideram que os governos podem estar interessados em apoiar a adoção de criptomoeda para reduzir os custos de aquisição ou trazer maior transparência à governança. Alguns países, como a Dinamarca, China, Reino Unido e Estónia, consideram a implementação da tecnologia *blockchain* para melhorar os seus sistemas bancários e sua administração (Vigna & Casey, 2016). Assim, os negócios que aceitem pagamentos em *bitcoins*, podem economizar em taxas de cartão de crédito, as quais podem variar até 5%, para cada pagamento aprovado. O custo das transações em *bitcoins* é menor, refletindo a quantidade de dados enviados (Blystone, 2015). Por outro lado, os críticos da *bitcoin* argumentam que o custo das transações nessa moeda seria maior se incluíssem proteção contra roubo e custos de conformidade / regulamentação (Franco, 2014).

A velocidade da transferência é outra das vantagens referidas, a qual, segundo Seaman (2014) protege os comerciantes contra fraudes de cobrança retroativa. De facto, um pagamento efetuado com *bitcoin* é confirmado num prazo de 10 a 30 minutos no máximo, enquanto um banco pode precisar de vários dias para liquidar uma ordem de pagamento. Nesse caso, os comerciantes têm tempo para verificar a transação antes de entregar os produtos ou serviços. Outra vantagem, é o fato de as transações com *bitcoins* serem irreversíveis, a menos que o vendedor acorde isso com os seus clientes, pelo que o risco de fraude de *chargeback* é insignificante. O relatório da Lexis Nexis de 2016 revela que o volume de transações fraudulentas bem-sucedidas subiu cerca de 32% em 2015, em relação ao ano anterior e que a proporção de fraude nas receitas dos comerciantes aumentou de 1,42% para 1,47% (LexisNexis, 2016). Segundo Shukairy (2016), em 2016 a indústria do comércio eletrónico sofreu uma perda estimada de receita de US \$ 6,7 bilhões devido a estornos, dos quais 71%, US \$ 4,8 bilhões, respetivamente, devido a fraude de *chargeback*.

Finalmente, a *bitcoin* é imune à inflação. Young (2016) argumenta que a taxa de inflação monetária da *bitcoin* diminuiria a uma taxa fixa ao longo do tempo, à medida que o número de *bitcoins* em circulação continuasse a subir a uma taxa fixa até atingir seu limite máximo de 21 milhões de moedas. De acordo com o Gráfico 1, a sua taxa de inflação monetária diminuiu de cerca de 90% e 2.916 milhões de BTC em 2010 para 4,02% em 2017. Em 2062, quando deveria atingir o limite de 21 milhões de BTC, a inflação monetária deverá atingir 0,0015 % (Gráfico 1).

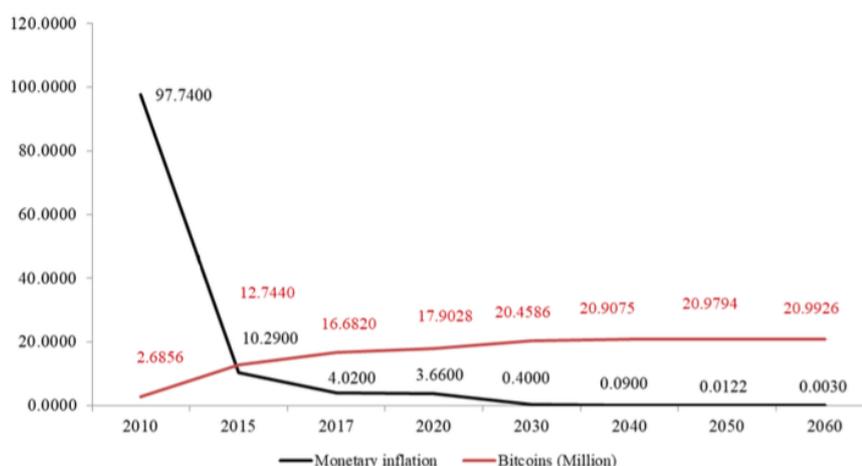


Gráfico 1 – Inflação monetária da Bitcoin entre 2010 e 2060

Fonte: <https://plot.ly/~BashCo/5.embed>

Entre as desvantagens da moeda digital, os investigadores apontam para a ausência de um total anonimato. Reid e Harrigan (2013) argumentam que as transações de *bitcoin*, incluindo serviços centralizados de criptomoeda, como trocas e serviços de carteira, não são totalmente anónimas. A mesma opinião é partilhada por Fanti e Viswanath (2017), que sustentam que os atuais protocolos usados na rede *bitcoin* não protegem suficientemente o anonimato do utilizador. Como não há informações sobre o utilizador na chave pública da criptomoeda, o *bitcoin* desfruta de um grau de privacidade melhor do que em outros serviços tradicionais de transferência digital. Ainda assim, permanecer completamente anónimo é desafiador se levarmos em consideração as técnicas estatísticas e a análise de padrões que podem identificar e revelar até 60% dos utilizadores da *bitcoin* (Tsukerman, 2015). Uma pesquisa realizada por Fabian e colaboradores (2016) revelou que sete em cada dez pessoas consideram que a *bitcoin* tem um nível razoável de anonimato (médio a alto), enquanto os riscos associados são médios ou baixos. No entanto, um em cada 5 utilizadores já consideraram abandonar a *bitcoin* devido a preocupações de anonimato (Fabian et al., 2016). Tal como outras moedas, a *bitcoin* pode ser alvo de fraudes. A chave privada dá ao proprietário acesso à carteira da *bitcoin*. Se essa chave for perdida ou roubada, o proprietário perde o acesso ao dinheiro. Para roubar a chave, um perpetrador precisa de acesso direto à pasta onde ela se encontra.

Um estudo realizado por investigadores da Southern Methodist University de Dallas (SMU, 2015) revelou a existência de esquemas fraudulentos, que resultaram em fraudes no valor de mais de 10 milhões de dólares, que foram desviados de depósitos de *bitcoins* de clientes cibernéticos incautos, entre 2011 e 2014. As principais fraudes foram:

- a) Programas de investimento de alto rendimento (esquemas online que prometem altas taxas de juros sobre depósitos);
- b) Fraudes relacionadas com investimento de mineração, em que as vítimas encomendavam e pagavam equipamento de mineração que nunca era entregue;
- c) “Carteiras fraudulentas” onde as vítimas eram convencidas a fazer depósitos de *bitcoins* sob o pretexto de oferecerem maior anonimato nas transações;
- d) Burlas com câmbio. Esquemas que oferecem uma taxa de câmbio melhor do que os concorrentes, mas que após efetuar o pagamento, os clientes nunca chegam a receber as *Bitcoins* ou dinheiro correspondente (SMU, 2015).

Outra das desvantagens da moeda digital está relacionada com a confiança. Investir os seus ganhos ou poupanças numa moeda digital pode ser uma escolha difícil para muitas pessoas, especialmente as gerações mais velhas que estão acostumadas ao dinheiro clássico (moedas, notas, cartões). Como o fenómeno da criptomoeda é relativamente novo, pode-se entender a relutância de pessoas ou empresas em entrar num mundo desconhecido. Para o público em geral, os complexos algoritmos e a ideia de uma carteira virtual podem ser assustadores. Uma pesquisa conduzida pela Harris Interactive nos EUA em 2014 constatou que 48% dos adultos americanos têm conhecimento da *bitcoin*, mas apenas 13% o escolheriam como um investimento em relação ao ouro (WebWire.com, 2017).

2.1.3. Segurança da moeda digital – a tecnologia *Blockchain*

Os registos distribuídos mútuos – *mutual distributed ledger* – que estão na base da tecnologia *blockchain* consistem num banco de dados que se encontra distribuído entre múltiplos dispositivos interligados numa rede descentralizada, onde são armazenados os registos de operações, como transações financeiras, com uma marca temporal – *timestamp*⁵ - e uma assinatura digital. O registo destas transações através do recurso a estruturas de dados universais, persistentes e permanentes replicadas em vários computadores garante a confiança e segurança das mesmas, através da concordância entre os múltiplos membros sobre os registos armazenados (Ferreira, et al. 2018). Os dois principais componentes da tecnologia Blockchain são a criptografia de chave pública e "*peer-to-peer*" ou armazenamento de dados partilhado (Decker & Wattenhofer, 2013). O resultado final é uma fonte de dados que é simultaneamente logicamente "central" enquanto tecnicamente "distribuída" entre os computadores na rede. A rede de computadores que usa o *ledger* pode consultar um único registo oficial e imutável de todas as transações de dados da origem da estrutura de dados. Todos têm a mesma visão dos mesmos dados, embora os possam estar recebendo de diferentes fontes físicas (Mainelli & Milne, 2016). Este tipo de tecnologia garante a segurança da *bitcoin*, pois fornece um registo indelével de todas as transações desta criptomoeda desde o momento em que elas começaram,

⁵ A marca temporal - *timestamp* – consiste numa sequência de caracteres ou informação codificada que identifica quando determinado evento ocorreu, usando a data e a hora, e que é tão precisa que chega a uma pequena fração de segundo.

em 3 de janeiro de 2009, usando um processo de consenso, conhecido como 'prova de trabalho' (mineração de *bitcoin*) para assegurar que os milhares de nós⁶ ativos na rede *bitcoin* têm todos a mesma visão dos dados subjacentes garantindo um nível muito alto de segurança criptográfica (Mainelli & Milne, 2016; Androulaki et al., 2013).

O termo *blockchain* vem da validação criptográfica de transações *bitcoin* em blocos que combinam várias transações juntas (o tamanho desses blocos varia muito, mas pode conter mil transações ou mais). Uma vez que um bloco é validado pela prova de trabalho, as transações nele contidas são gravadas de forma permanente e irreversível no *blockchain* em várias máquinas sem que haja apenas um registo central único ou principal (Mainelli & Milne, 2016).

2.2. E-Payment e E-Commerce

O termo *e-payment*, ou pagamento eletrônico, pode ser definido de forma simples como o pagamento de bens ou serviços que é efetuado através da internet e inclui todas as operações financeiras realizadas através de dispositivos eletrônicos, como computadores, smartphones ou tablets (Weber, 2015). Desde a década de 1960 os sistemas de pagamento que utilizam redes de distribuição eletrônicas constituem uma prática frequente no setor bancário e empresarial, especialmente para a transferência de grandes quantidades de dinheiro (Coppel, 2000; Crede, 1995). Desde o seu surgimento até à atualidade, ocorreram importantes desenvolvimentos tecnológicos, que, por um lado, expandiram as possibilidades dos sistemas de pagamento eletrônico e, por outro lado, criaram novos negócios e práticas sociais, que fazem uso desses sistemas (Kalakota & Whinston, 1996). Essas mudanças afetaram a definição de pagamentos eletrônico, o qual evoluiu de acordo com as necessidades de cada período (Crede, 1995). Na sua forma geral, este termo refere-se a qualquer pagamento a empresas, bancos ou serviços públicos de cidadãos ou empresas, que são realizados através de redes de telecomunicações ou eletrônicas usando tecnologia moderna (Chiu & Wong, 2014). Com base nessa definição, o *e-payment* consiste no pagamento que é efetuado pelo próprio pagador, seja como consumidor ou empresa, sem a intervenção de terceiros e que é feito à distância, sem a presença física do pagador e que, naturalmente, não inclui dinheiro (Robleh et al., 2014).

⁶ Computador ligado à rede.

O *e-payment* constitui parte integrante do e-commerce, tal como o pagamento, em si próprio, forma parte do processo mercantil (Coppel, 2000). O surgimento de novos tipos de transações comerciais, nomeadamente o comércio eletrónico, ou e-commerce, criou novas necessidades financeiras que em muitos casos não podem ser efetivamente cumpridas pelos sistemas de pagamento tradicionais, ditando a necessidade de criar novos métodos de pagamento que permitissem efetuar pagamentos através da internet ou simplesmente enviar dinheiro por e-mail para o outro indivíduo. (Robleh et al., 2014a; Sumanjeet, 2009). Alguns dos sistemas de pagamento eletrónicos que então surgiram são basicamente uma versão eletrónica dos sistemas de pagamento já existentes, como cheques e cartões de crédito, enquanto outros são baseados na tecnologia da moeda digital e possuem potencial para terem um impacto significativo no sistema financeiro e monetário de hoje (Kalakota & Whinston, 1996; Sumanjeet, 2009). No seu livro *The future of money*, Miller e colaboradores (2002) traçam o retrato daquilo que são os meios de pagamento eletrónicos ou digitais, os quais são manuseados eletronicamente e cujo volume de negócios garante o anonimato. Segundo estes autores, os documentos eletrónicos contêm apenas o valor nominal, uma indicação das características individuais do emissor (número de série, etc.) e elementos de proteção contra falsificação (a garantia da assinatura digital do emissor). Tratam-se de ativos altamente móveis, de utilização fácil e conveniente, e estão relativamente bem protegidos de uma variedade de delitos criminais. A sua utilização só se tornou possível com a invenção de um elemento de “segurança especial” – a assinatura digital eletrónica – um componente de um documento eletrónico destinado a protegê-lo contra eventuais falsificações. Essa assinatura resulta da transformação de dados criptográficos através de uma chave privada e de uma assinatura digital que permite a identificação do proprietário do certificado da chave de assinatura (Miller et al., 2002).

O *e-commerce* ou comércio eletrónico consiste na compra e venda de bens e serviços, ou na transmissão de fundos ou dados, através de uma rede eletrónica, principalmente a internet. Essas transações comerciais podem ocorrer entre empresas, empresa para consumidor, consumidor para consumidor ou consumidor para empresa. Os termos *e-commerce* e *e-business* são frequentemente utilizados de forma intercambiável (Shukairy, 2016). As origens do *e-commerce* remontam à década de 1960, quando as empresas começaram a usar o Electronic Data Interchange (EDI) para partilhar documentos comerciais com outras empresas. Em 1979, o American National Standards Institute desenvolveu o ASC X12 como um padrão universal para que as empresas pudessem partilhar documentos através de redes eletrónicas (Researchomatic, 2013a). Durante a década de 1980 o número de utilizadores individuais que

partilhavam documentos eletrónicos cresceu e na década seguinte a ascensão do *eBay* e da *Amazon* revolucionou o setor de comércio eletrónico. As transações típicas de *e-commerce* incluem a compra de livros online (como na *Amazon*, por exemplo) e de música (download de músicas sob a forma de distribuição digital, como a iTunes Store). (Robleh et al., 2014a; Sumanjeet, 2009). Atualmente os consumidores podem comprar uma quantidade infinita de itens online, tanto de lojas físicas que também vendem online, como de outros consumidores que os transacionam entre si (Coppel, 2000).

O *e-commerce* pode ser realizado usando uma variedade de aplicativos, como e-mail, catálogos online, EDI, protocolo de transferência de arquivos e websites (Crede, 1995). A promoção e divulgação dos produtos comercializados através do comércio eletrónico recorre ao envio de e-mails não solicitados (geralmente considerados spam) para os eventuais consumidores, assim como e-newsletters para subscritores (Fung et al., 2014) Com o rápido crescimento deste tipo de comércio, as empresas tendem a ser mais proactivas tentando cativar eventuais clientes através da utilização de ferramentas como cupões digitais, marketing de redes sociais e anúncios direcionados (Researchomatic, 2013). O *e-commerce* apresenta vários benefícios para o consumidor, nomeadamente a disponibilidade 24 horas por dia, a velocidade de acesso, a ampla disponibilidade de bens e serviços, acessibilidade fácil e alcance internacional. As suas desvantagens incluem o facto de que o apoio ao cliente é, muitas vezes, limitado, os consumidores não conseguem ver ou tocar o produto antes da compra, pelo que frequentemente ficam dececionados quando constatam que o mesmo não corresponde às suas expectativas, assim como o tempo de espera necessário para que o produto seja enviado pelo fornecedor e rececionado pelo seu destinatário (Kalakota & Whinston, 1996).

2.2.1. PayPal

O *PayPal* foi criado por Peter Thiel, Luke Nosek, Ken Howery e Max Levchin. Fundada em 1998, com a designação de Confinity, a empresa encontrava-se sediada em San José, no Estado da Califórnia (EUA) e desenvolvia software de segurança para dispositivos portáteis, especialmente PDA's, possibilitando a realização de pagamentos por meio de tecnologia de infravermelhos (Rosoff, 2011). Em 1999, a Confinity lançou o *PayPal*, concebido como um serviço de transferência de dinheiro, com o financiamento de John Malloy da BlueRun

Ventures, e direcionado para pagamentos por correio eletrônico (Lillington, 1999). Em março de 2000, a Confinity fundiu-se com a X.com, uma empresa bancária on-line fundada por Elon Musk. Musk estava otimista sobre o sucesso futuro do negócio de transferência de dinheiro que a Confinity estava desenvolvendo. Em outubro daquele ano, Musk tomou a decisão de que o X.com encerraria as suas outras operações de Internet banking e se concentraria no serviço monetário do PayPal. No mesmo mês, Elon Musk foi substituído por Peter Thiel como CEO da X.com. A empresa X.com foi então renomeada como *PayPal* em 2001, e expandiu-se rapidamente ao longo do ano até que os executivos da empresa decidiram cotá-la na bolsa (Hoffman, 2012).

Atualmente, a empresa é líder no nicho do dinheiro eletrônico em todo o mundo. De acordo com o comunicado de imprensa do *PayPal*, em 10 de março de 2005, o sistema tinha mais de 71 milhões de contas em 45 países do mundo. Em 2002, o *PayPal* foi adquirido pela maior leiloeira da Internet, a *eBay*, por US \$ 1,5 bilhão. As contas dos utentes do sistema podem ser pessoais, principais e comerciais. Essas contas estão seguradas pela SafeWeb Insurance contra levantamentos não autorizados no valor de 100.000 dólares americanos. A conta pode ser aprovacionada por transferência bancária ou por pagamento com cartão de crédito. Trabalhar com o *PayPal* não requer o uso de software especial, porque todas as operações são realizadas diretamente no site. Para garantir que as contas dos utentes de segurança estejam protegidas por senha, a conexão com transações pode ser feita usando apenas o protocolo SSL, de 128 bits ou superior (Paypal.com, 2018).

3. Metodologia

Tendo as premissas e o objeto do presente estudo definido, importa explicar a metodologia escolhida. Para a realização deste estudo a opção metodológica é a revisão sistemática de literatura, através de uma abordagem bibliométrica.

Uma revisão sistemática de literatura é um método que permite identificar, avaliar e analisar estudos primários publicados com vista a conduzir uma investigação científica sobre uma temática específica" (Staples & Niazi, 2007). Pode ser considerada um estudo observacional retrospectivo ou estudo experimental de recuperação e análise crítica da literatura. Testa hipóteses e tem como objetivo levantar, reunir, avaliar criticamente a metodologia da pesquisa e sintetizar os resultados de diversos estudos primários. Trata-se de uma metodologia que responde a questões de pesquisa específicas, claramente formuladas, agrupando estudos existentes, selecionando e avaliando contribuições, analisando e sintetizando dados, e reportando as evidências de forma a permitir obter conclusões claras para se atingir o que é e o que não é conhecido (Brereton et al., 2007).

Com recurso aos dados dos estudos primários (unidades de análise), obtidos de bancos de dados como *Web of Science* ou *Scopus*, por exemplo, a revisão sistemática permite sistematizar o conhecimento existente sobre um tópico específico através de pesquisas e análises estruturadas, sintetizando esses dados através de métodos que tanto podem ser estatísticos como qualitativos (Brereton et al., 2007). Através deste método é possível não só responder a uma questão de investigação, como testar hipóteses e teorias, ou construir novas teorias, limitando ao mesmo tempo erros ou tendências. Neste sentido, a revisão sistemática é menos uma discussão da literatura e mais uma ferramenta científica (Cipriani & Barbui, 2006). Esta metodologia adota processos transparentes, replicáveis e científicos, para identificar, avaliar e sintetizar a literatura. Desta forma é possível minimizar a tendência das buscas exaustivas de estudos já publicados e, fornecer evidências das decisões, procedimentos e conclusões dos revisores, através de sistema de revisão mais rigoroso e definido (Cipriani & Barbui, 2006). A revisão sistemática de literatura constitui o tipo de metodologia mais recomendado para o levantamento da produção científica disponível e para a (re)construção de redes de pensamentos e conceitos, que articulam saberes de diversas fontes com o objetivo de obter as respostas às questões de investigação.

Por outro lado, a bibliometria permite medir os indicadores de produção e disseminação de

conhecimento, e acompanhar o desenvolvimento das diversas áreas científicas (Costa et al. 2012). Segundo Van Leeuwen (2004) um dos principais pressupostos da bibliometria é que a literatura mais relevante se encontra publicada em revistas científicas, que estão usualmente disponíveis. A bibliometria utiliza elementos como o título da revista, autor, referências, palavras-chave, resumo e número de citações, com as quais é possível gerar uma imagem verosímil das contribuições existentes para um tópico específico. Além disso, também é possível detetar tendências, descontinuidades, clusters de temas e grupos de autores, bem como descrever orientações de pesquisa emergentes. Importa referir que, por produção científica se entende livros, teses, capítulos de livros, artigos publicados em revistas científicas e atas de conferências entre outros (Van Leeuwen, 2004).

Para avaliar a produção científica pode-se recorrer à aplicação de diversos indicadores bibliométricos, os quais podem ser divididos em indicadores de qualidade científica, atividade científica, impacto científico e de associações temáticas (Costa et al., 2012). Os indicadores de qualidade científica têm por base a avaliação que é feita pelos pares que analisam o conteúdo das publicações, enquanto que os indicadores de atividade científica se referem à contabilização da atividade científica desenvolvida, ou seja, o volume dos trabalhos publicados, a produtividade dos autores, quer na autoria total dos trabalhos, quer na colaboração com outros autores, entre outros (Costa et al. 2012).

No que refere aos indicadores de impacto científico, estes podem subdividir-se em dois tipos: indicadores de impacto dos trabalhos e indicadores de impacto das fontes. Segundo Costa e colaboradores (2012), o indicador de impacto dos trabalhos pode referir ao número de citações recebidas, enquanto que o indicador de impacto das fontes considera o impacto das revistas, o índice de citação imediata e a influência dessas revistas. Segundo Sancho (2002, citado por Costa et al. 2012) as associações temáticas também podem constituir um importante indicador bibliométrico. A análise de citações e a análise de referências comuns são exemplos de indicadores de associações temáticas. As ferramentas mais úteis para o desenvolvimento de estudos bibliométricos são as bases de dados. Estas podem fornecer orientação para investigar um tema, pesquisar um tópico, dar indicações sobre eventuais alterações de orientação que o mesmo possa ter sofrido ao longo do tempo, assim como a evolução de um autor, etc. Deste modo, se forem usadas como meios, não como fins, podem constituir uma ferramenta preciosa, auxiliando os investigadores na sua pesquisa. As ferramentas bibliométricas mais utilizadas atualmente são a *Web of Science*, a *Scopus* e o recente *Google Scholar Metrics*. Estas abrangem

uma ampla gama de diferentes dados e usam diferentes métricas, pelo que se deve levar isso em consideração quando as utilizamos.

Os procedimentos de análise utilizados nesta dissertação consistiram na seleção de um *corpus* de estudos académicos (com a data de referência de 30 de setembro de 2018) publicados em fontes indexadas ao site *Scopus*, cuja pesquisa foi efetuada através da utilização da palavra-chave “*Bitcoin*”. A partir dos resultados obtidos foram selecionados 140 estudos – artigos, livros, capítulos de livros - tendo como critério de seleção o número de vezes que os mesmos foram citados. A pesquisa privilegiou os trabalhos de investigação que obtiveram o maior número de citações, e cuja influência/impacto científico foi mais relevante. Estes 140 estudos constituem, portanto, o *corpus* que foi utilizado para a análise bibliométrica para estudar a evolução do estado da arte sobre moeda digital, e em particular sobre a *bitcoin*, com vista a identificar de que forma é que este fenómeno tem sido estudado na literatura académica relevante.

4. Estudo empírico

4.1. Análise dos dados

O universo de análise é constituído por 140 artigos que foram pesquisados na base de dados *Scopus* usando para o efeito a palavra-chave “*Bitcoin*”, ordenados de forma decedente a partir do mais citado. No gráfico abaixo (Gráfico 2) é possível ver a distribuição dos estudos por ano de publicação.

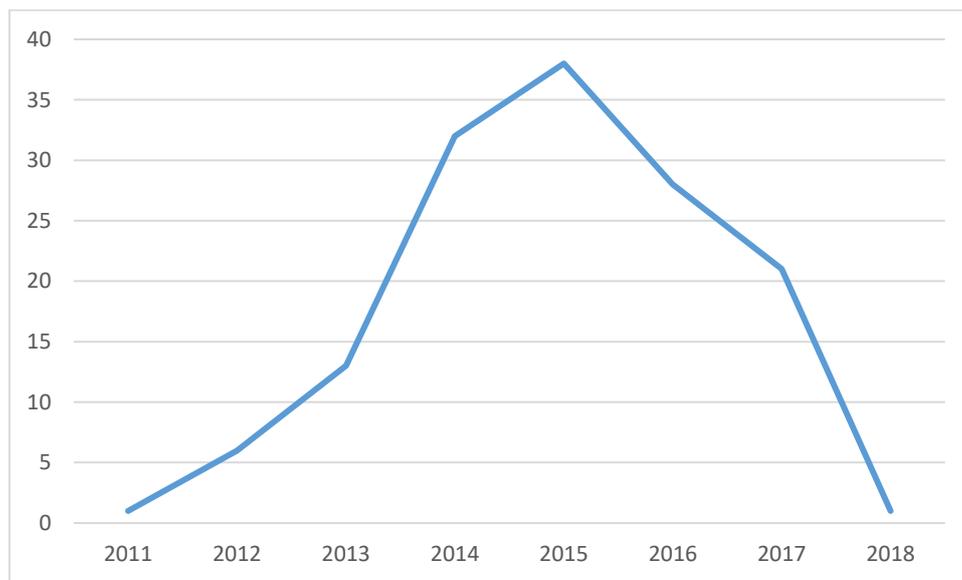


Gráfico 2 – Distribuição dos estudos por anos de publicação

A problemática da *bitcoin* é transversal a diversos âmbitos de estudo, pelo que os investigadores que se debruçam sobre este assunto pertencem a várias áreas científicas. Assim, dos 140 trabalhos que compõem o *corpus* de análise 66% (93) pertencem às Ciências da Computação, e apenas 25% (35) são estudos de Economia. Registe-se ainda 7 estudos (5%) de Criminologia que se debruçaram sobre esta temática, 3 (2%) de Engenharia Eletrónica e 2 investigações (1%) cuja área científica é a Matemática (Gráfico 3).

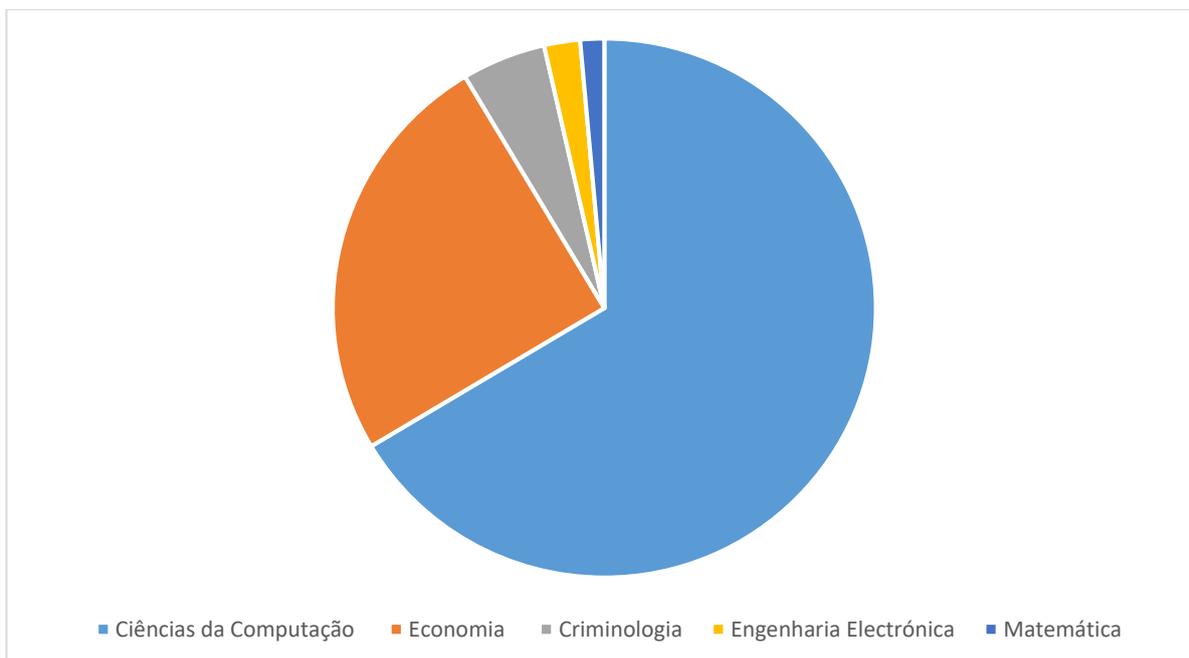


Gráfico 3 – Áreas Científicas

No que respeita aos principais tópicos abordados nestes estudos verificou-se que a segurança de dados foi a temática que mais chamou a atenção dos investigadores, tendo sido esse o principal tema de 27 trabalhos (19%), ultrapassando aquele se seria suposto ser o principal – dinheiro electrónico – que ocupou 19 trabalhos (13%). Criptografia com 17 estudos (12%), economia com 14 (10%) e comércio electrónico com 10 (7%) ocuparam o 3º, 4º e 5º lugares. A problemática da segurança, mas neste caso sob o ponto de vista da rede, dominou também estes estudos com 7 investigações (5%) dedicados especificamente à “segurança de rede”, 6 (4%) que abordaram o “intercâmbio electrónico de dados” e igual número de estudos (6 = 4%) em que a temática da *bitcoin* foi abordada sob o ponto de vista da “lavagem de dinheiro”. “Finanças” e “malwares” foram os temas de 5 estudos (4%), enquanto que assuntos técnicos relacionados com ciências da computação, como “sistemas de computadores distribuídos”, “armazenamento digital” e “medições de conhecimento” foram o tema principal de 4 estudos (3%) (Gráfico 4).

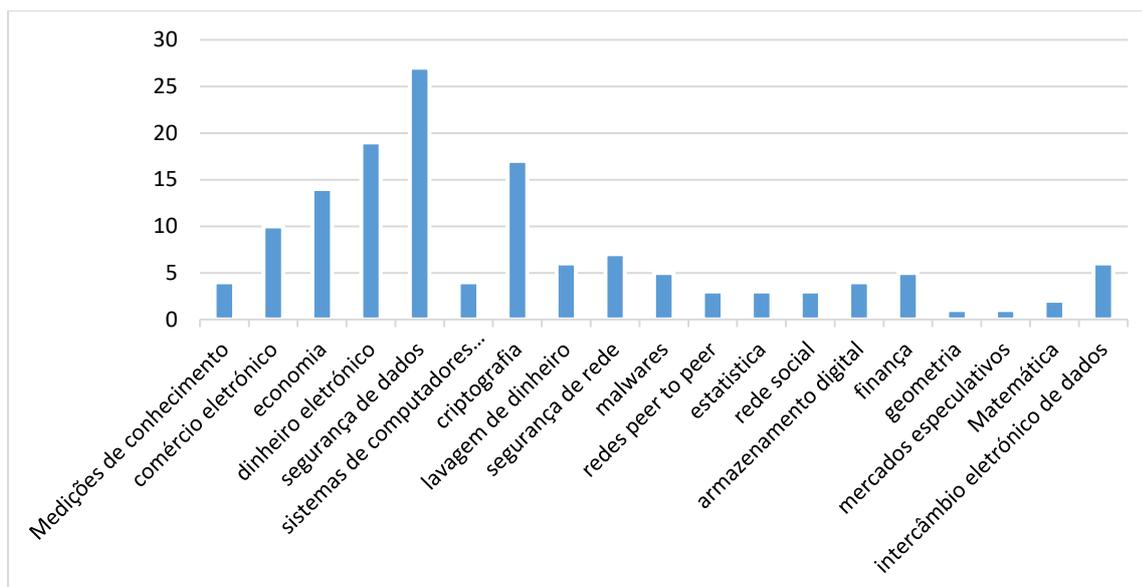


Gráfico 4 – Tópico Científico Principal

A análise abrangeu também as palavras-chave dos autores, de modo a tentar perceber em que vertente de estudo aparecia a associação à *bitcoin*. Excluindo a palavra-chave que foi utilizada para a pesquisa – Bitcoin – que foi a mais utilizada (84 vezes = 34%), o termo “blockchain”, utilizado para denominar a tecnologia que usa os registos distribuídos mútuos – *mutual distributed ledger* – para garantir a segurança desta moeda digital, é aquele que aparece com mais frequência (22 vezes = 9%), seguido de “criptomoedas” (15 vezes = 6%), “privacidade” (13 vezes = 5%) e “anonimato” (12 vezes = 5%). “Dinheiro eletrônico” (9 vezes = 4%), “moedas digitais” e “criptografia”, ambos com 7 registos cada (3%), encontram-se na sétima posição, seguidos de “atividade ilegal” (6 vezes = 3%) e “comércio eletrônico”, “altcoins” e “contrato inteligente”, com 5 registos (2%). “Crime cibernético”, “lavagem de dinheiro”, “malwares”, “gerenciamento de risco” e “câmbio monetário”, foram as palavras-chaves escolhidas pelos autores em 4 estudos (2%). Das restantes palavras-chave utilizadas destaque-se ainda os termos “computação segura” e “economia subterrânea” registados 3 vezes (1%) (Gráfico 5).

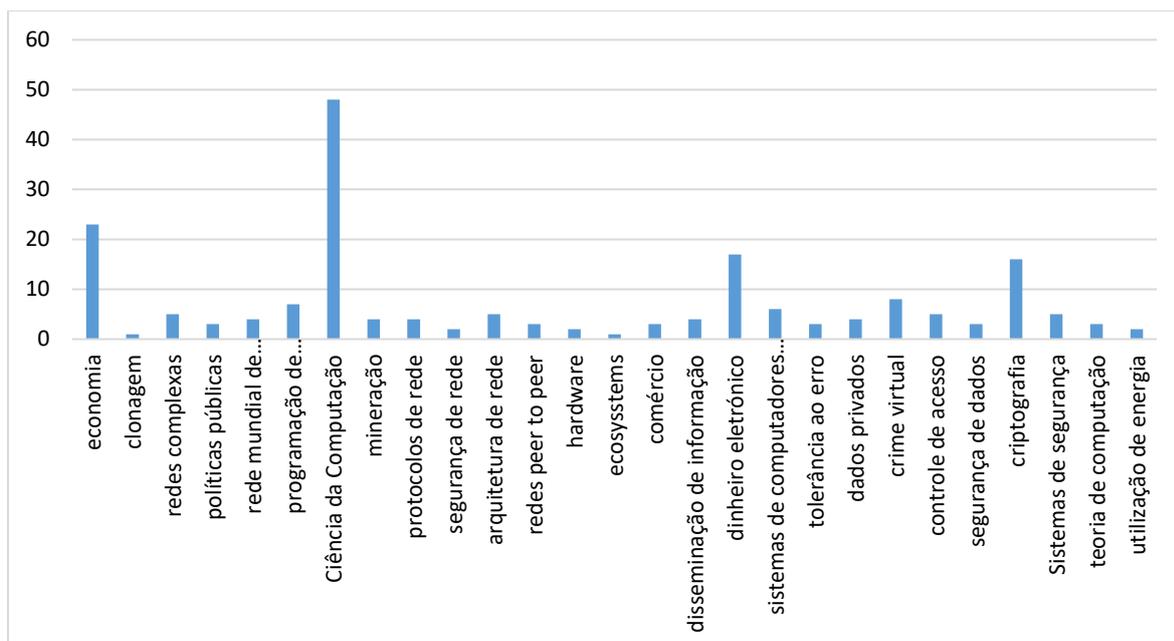


Gráfico 6 - Tópicos Científicos Controlados

Estes estudos têm frequentemente outras palavras-chave indexadas que se referem a tópicos científicos não controlados, ou seja, temáticas para as quais esses estudos remetem. Bitcoin foi a palavra-chave mais frequente (ou não fosse esse o termo a que recorreremos para efetuar esta pesquisa) a qual registou uma frequência de 26% tendo aparecido em 76 trabalhos de investigação. Em segundo lugar apareceu o termo “moedas digitais”, com 23 (8%), seguido de “privacidade” e “atividades criminosas” com 14 estudos cada (5%).

“Anonimato” foi registado 10 vezes (3%) e “blockchain” e “problemas de segurança” 9 vezes (3%), seguindo-se “moeda virtual”, “sistemas de pagamento” e “risco”, com 8 registos (3%). “Altcoins”, “criptografia” e “gerenciamento de chaves” apareceram em 7 estudos (2%). Com 6 registos temos “lavagem de dinheiro” e “valores económicos” (2%). “Protocolos peer-to-peer” e “chave secreta” foram também as mais mencionadas com 5 registos (Gráfico 7).

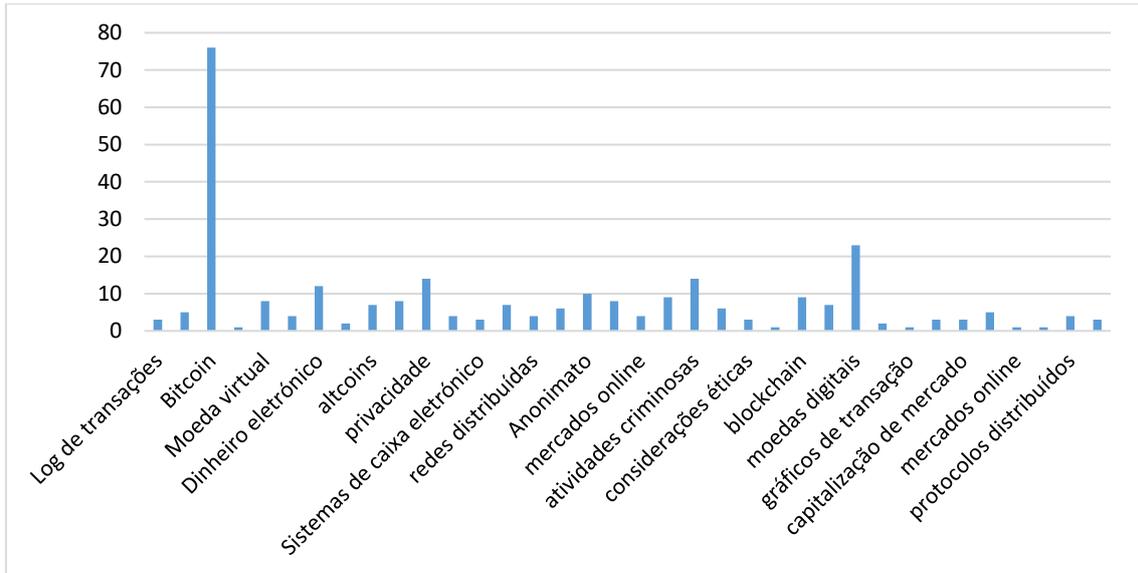


Gráfico 7 - Tópicos Científicos não Controlados

Com vista a restringir o horizonte de análise, de modo a obter uma leitura mais centrada, optou-se por seleccionar uma amostra do universo constituído pelo *corpus* de 140 estudos e analisá-la em separado. Essa amostra integra os 20 trabalhos que recolheram maior número de citações e que apresentamos no Anexo 1. No gráfico abaixo (Gráfico 8) é possível ver a distribuição desses estudos por áreas científicas. Assim, as Ciências da Computação representam 70 % da amostra (14), 25% dos mesmos (5) são de Economia, e apenas um estudo (5%) pertence à área da Criminologia.

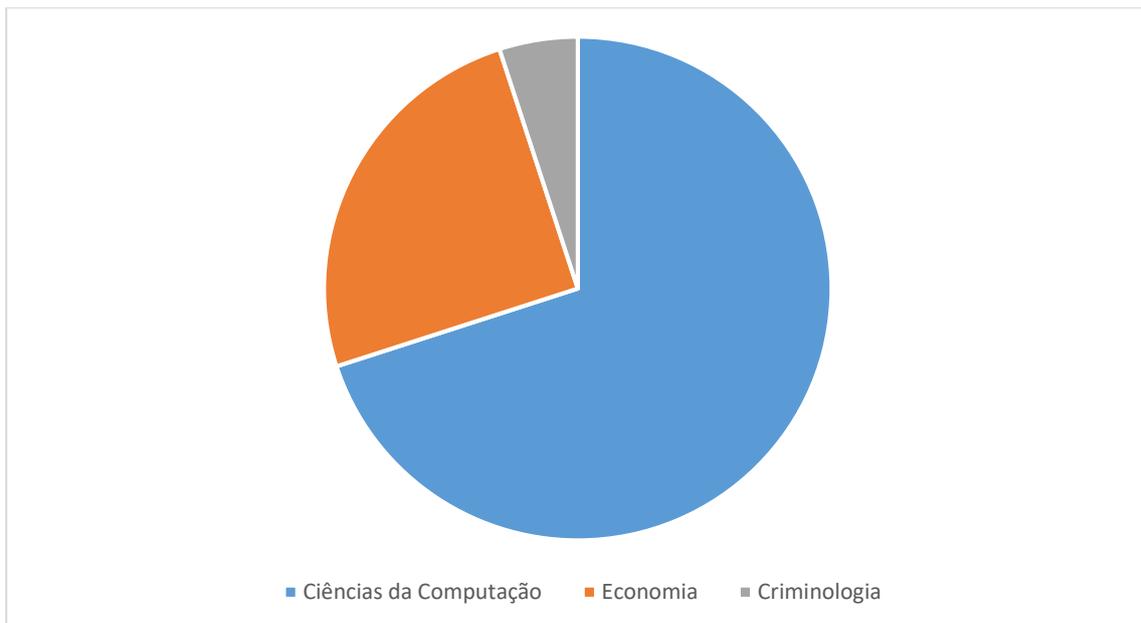


Gráfico 8- Áreas Científicas dos 20 artigos mais citados

No que se refere aos tópicos científicos principais, a “segurança de dados” foi o tema mais abordado, com 7 estudos (39%), seguido do “dinheiro eletrónico” com 3 (17%). O “comércio eletrónico” e as “medições do conhecimento” foram temas abordados em 2 trabalhos (11%). Os restantes quatro estudos tiveram como temas principais: “economia”, “sistemas de computadores distribuídos”, “criptografia” e “lavagem de dinheiro” (Gráfico 9).

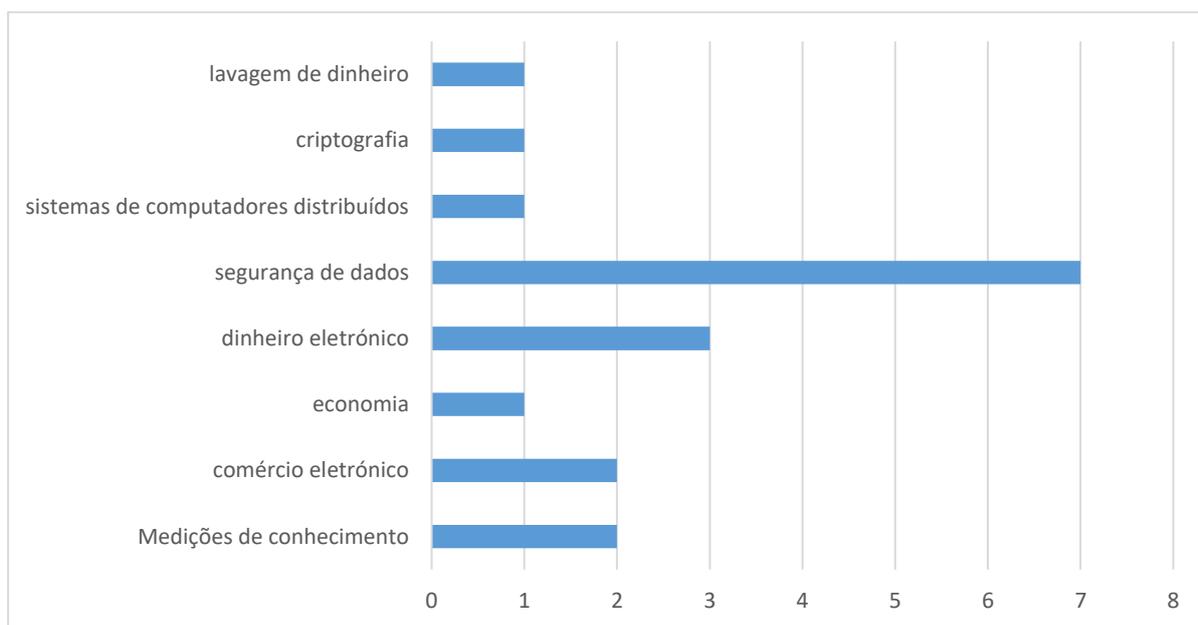


Gráfico 9 - Tópico científico principal (TOP20)

No que se refere às palavras-chave escolhidas pelos autores, “Bitcoin” foi a mais frequente, aparecendo em 8 estudos (21%), seguida de “privacidade” com 4 (10%). 8% dos trabalhos analisados (3) apresentam os temas “dinheiro eletrónico”, “moedas digitais” e “sistemas de pagamento” nas suas palavras-chaves. Menos frequente é a utilização de “anonimato”, “medição”, “blockchain” e “tutorial”, que aparecem apenas em 2 estudos. Por último, as palavras-chave “conhecimento zero”, “análise quantitativa, gráficos de transação”, “comércio eletrónico”, “crime online”, “avaliação experimental”, “lavagem de dinheiro”, “computação multipartidária”, “altcoin” e “criptografia” foram também utilizadas, aparecendo cada uma em apenas um dos trabalhos desta amostra (Gráfico 10).

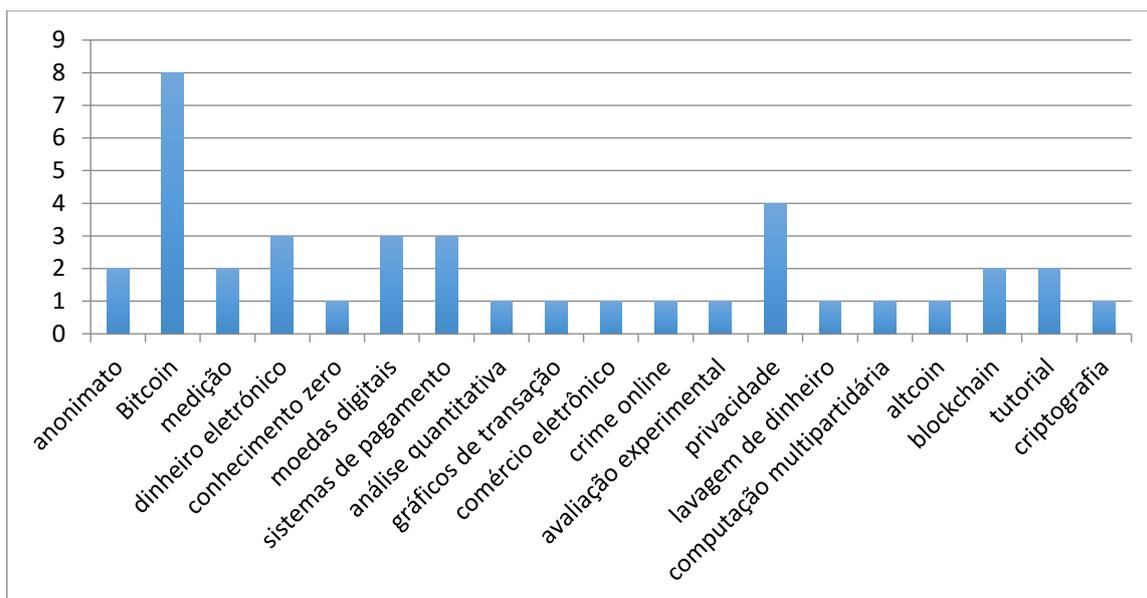


Gráfico 10 - Palavras-chave do autor (TOP20)

Em relação a outros temas abordados nos estudos constantes desta amostra, a sua distribuição privilegiou a “Criptografia” em 33% dos mesmos (7), seguindo-se a “Economia”, presente em 14% dos trabalhos (5). Quanto aos restantes temas, as “Ciências da Computação” e as “Políticas Públicas” foram temáticas abordadas em 2 artigos (10%). As temáticas do “Comércio”, “Protocolos de Rede”, “Segurança de Rede”, “Dinheiro Eletrónico” e “Disseminação de Informação” também estiveram presentes em um dos artigos desta amostra (Gráfico 11).

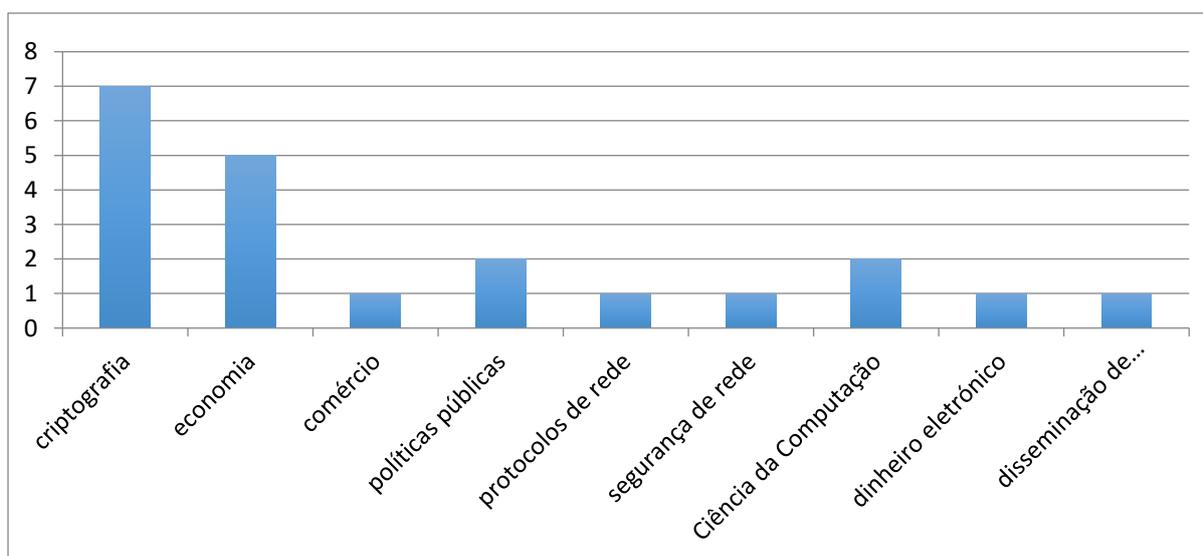


Gráfico 11 - Tópicos científicos controlados (TOP20)

Finalmente, no que se refere às palavras-chave indexadas a tópicos científicos não controlados, depois de “Bitcoin” que aparece em primeiro lugar (8 estudos = 15%), registaram-se: “sistemas de pagamento” (6 = 11%), “criptografia” e “privacidade” (5 = 9%). “Anonimato” e “Protocolos peer-to-peer” que aparecem em 4 trabalhos (7%), seguindo-se de “propagação da informação”, “atividades criminosas”, “segurança” e “blockchain”, registadas em 6% da amostra (3 estudos). “Moeda digital” e “dinheiro eletrónico” foram palavras-chave indexadas em 4% da amostra (2) e por último, registadas em apenas um trabalho (2%), encontramos “altcoins”, “gerenciamento de chaves”, “considerações éticas” e “implicações políticas” (Gráfico 12).

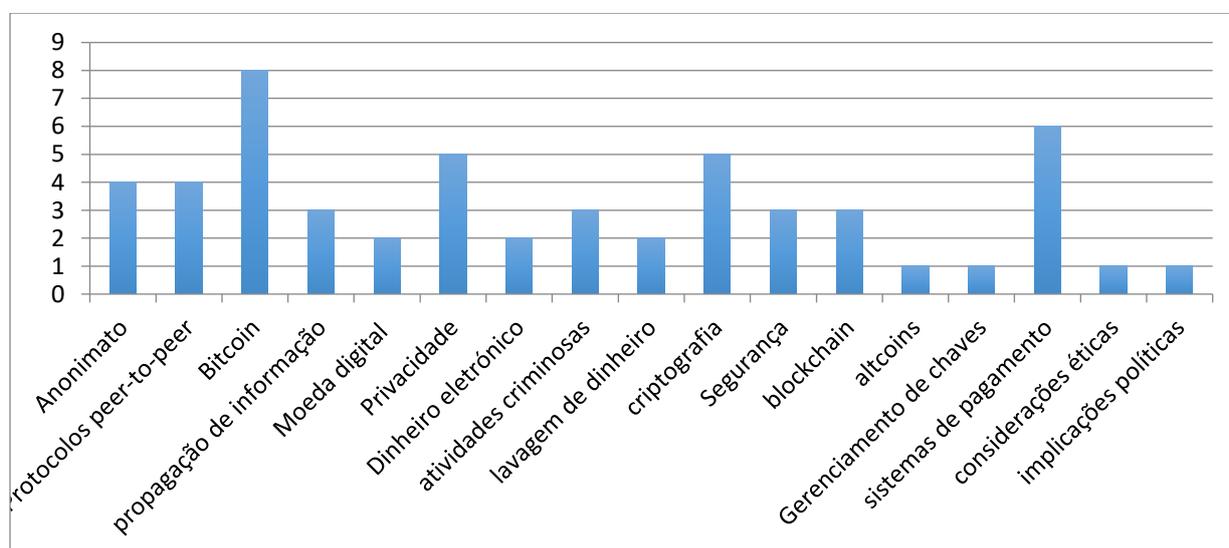


Gráfico 12- Tópicos científicos não controlados (TOP20)

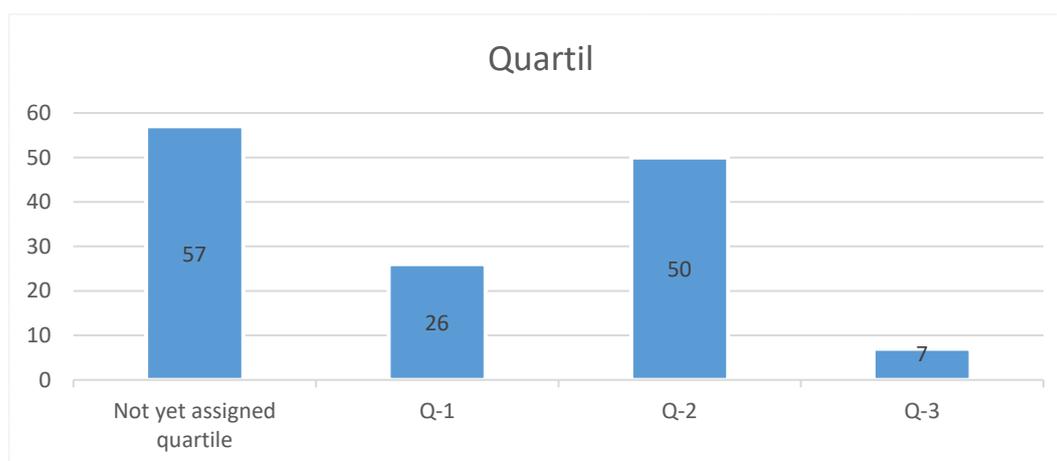


Gráfico 13 – Classificação dos quartis dos artigos analisados

Dos 140 artigos analisados, 57 não têm qualquer quartil associado, 26 artigos pertencem ao Quartil 1, 50 artigos ao Quartil 2 e apenas 7 artigos ao Quartil 3. (Gráfico 13).

4.2. Discussão dos resultados

A análise efetuada aos temas abordados pelos autores dos trabalhos de investigação selecionados para este estudo revela que as questões de segurança dominam a literatura em torno da *bitcoin*. O receio perante a ocorrência de incidentes referentes à violação de segurança e vigilância, que comprometem a privacidade dos utilizadores da moeda digital, coloca em questão os modelos de segurança existentes, sobretudo tendo em vista as grandes quantidades de dados pessoais que todos os dias são recolhidos e controlados por terceiros. A tecnologia não cria só prosperidade, ela também destrói a privacidade. Assim, aliados às questões de segurança, encontra-se também a discussão acerca da privacidade e anonimato. Não surpreende, pois, que investigadores de várias áreas se debrucem sobre estas problemáticas e que os estudos que recolheram, até hoje, um maior número de citações, tenham em comum o facto de terem sido apresentados num evento académico destinado a debater questões de segurança e privacidade – *IEEE Symposium on Security and Privacy* – o mais importante fórum internacional onde são apresentados os mais recentes desenvolvimentos em segurança de computadores e privacidade eletrónica. Com efeito, cinco dos artigos que lideram a tabela dos mais citados tiveram origem em comunicações apresentadas nestes simpósios, dois deles na edição de 2014 (Ben-Sasson et al, 2014; Miller et al., 2014) e os restantes nas edições de 2011 (Reid et al, 2011), 2013 (Miers et al., 2013) e 2015 (Bonneau et al, 2015).

A *bitcoin* é uma moeda digital baseada num sistema de pagamentos *peer-to-peer* gerido por um software de código aberto, caracterizado por ter custos menores de transação, maior segurança do que a moeda fiduciária e não ter necessidade de um banco central. Apesar das críticas sobre eventuais utilizações ilegais e consequências sociais, a *bitcoin* tem atraído o interesse da comunidade científica, o que se reflete no número de estudos publicados acerca da sustentabilidade desta moeda digital, considerando os impactos ambientais, aspetos sociais e aspetos económicos. Da análise efetuada aos artigos selecionados que abordam esta problemática emerge uma ilação que recolhe o consenso de grande parte dos investigadores de que uma eventual transição para um sistema monetário baseado nesta moeda digital resulta improvável dado a enorme quantidade de energia requerida para minerar novas bitcoins e manter todo o sistema monetário virtual, pelo que esta moeda se irá manter como uma moeda

de nicho, de que o artigo de Bonneau e colaboradores (2015) – que ocupa a 4ª posição na lista dos mais citados - é exemplo.

No que respeita à sustentabilidade social da *bitcoin*, a literatura revela algum ceticismo, já que esta moeda pode ser usada por hackers e para atividades fraudulentas ou associações criminosas ligadas ao tráfico de drogas, armas, etc. Esta associação entre moeda digital e atividades ilícitas parece advir das ligações ao anonimato – uma das características da *bitcoin* - que constitui um atrativo para criminosos, hackers e todos aqueles operam em mercados informais e/ou à margem da lei. Por este motivo a *bitcoin* está presente também em estudos de criminologia e outros que abordam a preocupação das autoridades acerca da utilização de ativos digitais para operações de lavagem de dinheiro, como é o caso de, por exemplo, *An inquiry into money laundering tools in the Bitcoin ecosystem*, um estudo levado a cabo por Moser e colaboradores (2013) e que integra a lista dos artigos mais citados.

A tecnologia *blockchain* está intimamente ligada à moeda digital *bitcoin*, por isso qualquer pesquisa que utilize esta palavra-chave irá apresentar um sem número de resultados onde é feita referência à *blockchain*. E tudo começou com a publicação, em 2009, de um artigo de um autor desconhecido, que o assinou sob o pseudónimo Satoshi Nakamoto, *Bitcoin: A peer-to-peer Electronic Cash System*. Neste artigo, Nakamoto (2009) apresenta um sistema de pagamento P2P, hoje conhecido como criptomoeda, que combina vários componentes criptográficos, para permitir a transferência de ativos digitais sem a necessidade de um intermediário de confiança, e que deu origem à tecnologia *blockchain*.

O princípio inerente a esta tecnologia já foi explicado mais atrás numa seção específica, pelo que não faz sentido estar a repeti-lo. No entanto, importa referir que a utilização desta tecnologia não se esgota com a *bitcoin* ou com as suas congéneres digitais. De facto, a literatura académica relevante que analisámos explora abundantemente a *blockchain*, apresentando uma miríade de utilizações para a mesma. Assim, esta tecnologia parece ser uma opção interessante para aplicação numa estrutura de partilha de dados médicos, para geração de energia e distribuição entre sistemas de geração de energia eólica, solar, ou hidroelétrica, conectados por micro-redes ao nível do cidadão e para a gestão de transações legais entre empresas, baseadas em *blockchains*. Giungato e colaboradores (2017) sustentam que a *bitcoin* e a tecnologias *blockchain*, podem ser impulsionadores de mudança social, e propõem a realização de experiências sociais em larga escala, cujos resultados, segundo os autores poderiam

comprovar a sustentabilidade desta moeda digital e superar os problemas elencados pelos seus inúmeros detratores.

O mecanismo de segurança das *blockchains* também pode ser explorado para executar com segurança alguns tipos de contratos, os chamados “*smart contracts*” (contratos inteligentes), que consistem em acordos entre partes mutuamente desconfiadas que dispensam o recurso a um intermediário de confiança. Nos últimos anos a literatura académica tem proposto vários tipos de *smart contracts* baseados nesta tecnologia, que o estudo de Atzei e colaboradores (2018) é um exemplo, ao revelar alguns dos desafios mais promissores.

Por último, importa fazer uma menção, mesmo que breve, a um dos dois únicos estudos na área da matemática que nos apareceu quando da pesquisa pelo termo Bitcoin. *Statistical Analysis of the Exchange Rate of Bitcoin*, um estudo da autoria de Jeffrey Chu, Saralees Nadaraajah e Stephen Chan (2015), fornece uma interessante análise estatística das taxas de câmbio da Bitcoin versus o dólar americano, com previsões para valores de taxas de câmbio futuras. Chu e colaboradores concluíram que as taxas de câmbio USD-BTC exibiam dinâmicas complicadas, mas salientaram o facto de que nos 24 meses anteriores à realização deste estudo a bitcoin ter valorizado mais de 50 vezes e alertaram potenciais investidores para a alta volatilidade do investimento em bitcoin, ressaltando que, no entanto, o retorno desse investimento poderia ser também muito alto. Se estes investigadores estavam confiantes no resultado do seu estudo e resolveram investir nesta moeda digital, o histórico valor alcançado pela *bitcoin* em dezembro de 2017, terá sido a melhor recompensa que poderiam receber pelo seu labor.

5. Conclusões

Na extensa análise levada a cabo nesta revisão sistemática de literatura acerca da Bitcoin, com base num *corpus* de 140 artigos pesquisados na base de dados *Scopus*, com o objetivo de investigar de que modo e sob que perspectivas esta problemática tem sido estudada pela comunidade académica, foi possível obter uma visão mais alargada dos desafios que se colocam perante este fenómeno.

A literatura pesquisada, vasta e fragmentada, revela-nos novas ideias e novas abordagens não só no que respeita à conceção prática das criptomoedas, como nos desvenda toda uma miríade de questões relacionadas com segurança – segurança de dados e segurança de redes – privacidade e anonimato que representam um desafio para a sociedade e para as redes que dependem dos sistemas informáticos.

A inovação e o avanço tecnológico representados pelo surgimento desta nova geração de ativos financeiros, não se limitou à moeda digital em si, mas lançou as bases para o desenvolvimento de projetos de protocolos, sistemas distribuídos, design de hardware e várias outras áreas que abrangem a segurança informática, as ciências da computação e a economia.

Esta é uma temática onde ainda existe muito por explorar. No entanto, a literatura já tem muito para oferecer no que respeita a estudos sobre as potencialidades económicas e sociais da moeda digital em geral, e da *bitcoin* em particular, apesar de não haver ainda um modelo científico com poder preditivo suficiente para responder a perguntas sobre como será a evolução deste fenómeno, em diferentes circunstâncias. A nível económico, no entanto, a Bitcoin representa um fenómeno raro, em que a realidade ultrapassou todas as perspectivas que as teorias deixariam antever.

Bibliografia

Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T. & Capkun, S. (2013). Evaluating user privacy in bitcoin. In *Financial Cryptography and Data Security* (pp. 34-51). Berlin Heidelberg: Springer.

Australian Government (2016). *GST treatment of digital currency*. Discussion Paper.

Badev, A. & Chen, M. (2014). Bitcoin: technical background and data analysis, *Finance and Economics Discussion Series*, 2014–104, Board of Governors of the Federal Reserve System.

Banque de France (2013). The dangers linked to the emergence of virtual currencies: the example of bitcoins, *Focus*, 10. Disponível em: https://www.banque-france.fr/sites/default/files/medias/documents/focus-10_2013-12-05_en.pdf.

Barber, S., Boyen, X., Shi, E. & Uzun, E. (2012). Bitter to better—how to make bitcoin a better currency. In *Financial cryptography and data security* (pp. 399-414). Berlin Heidelberg: Springer.

Beck, U. (2015). *What is globalization*. New Jersey: John Wiley & Sons.

Bellamy, E. (1889). *Looking backward*, Boston: Houghton, Mifflin & Co.

Blystone, D. (2015). *Bitcoin Transactions Vs. Credit Card Transactions*. Retrieved from: <https://www.investopedia.com/articles/forex/042215/bitcoin-transactions-vs-credit-card-transactions.asp>

Braga, F.D.A., Isabella, G. & Mazzon, J.A. (2013). Do Digital Wallets as a Payment Method Influence Consumer in Their Buying Behavior? *XXXVII Encontro da ANPAD, Rio de Janeiro/RJ - 7-11 Setembro de 2012*.

Brereton, P., Kitchenham, B.A., Budgen, D., Turner, M. & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *J. Syst. Softw.* 80, 571–583

Brookes, B. C. (1990). Biblio, sciento, informetrics? What are we talking about? In: Egghe, L.; Rousseau, R. (Eds.). *Informetrics 89/90*. Amsterdam: Elsevier, pp. 31-43.

Cassoni, A. & Ramada, C. (2013). Digital money and its impact on local economic variables: the case of Uruguay. Comunicação apresentada em *Digital Payment Systems and Local Development*, San Pablo, 2012, 27-28 Nov. Uruguai: Universidad Ort.

Chilton, B. et al. (2016). *Blockchain and the law: Practical implications of a revolutionary technology for financial markets and beyond*. Chamber of Digital Commerce. DLA Piper.

Chiu, J. & Wong, T-N. (2014). E-money: efficiency, stability and optimal policy, Bank of Canada, *Working Paper*.

Cipriani, A. & Barbui, C. (2006). What is a systematic review? *Epidemiol. Psichiatr. Soc.* 15, 174–175.

Committee on Payments and Market Infrastructures (2015). *Digital currencies*. Bank for International Settlements. Available on: www.bis.org.

Coppel, J. (2000). E-Commerce: Impacts and Policy Challenges, *OECD Economics Department Working Papers*, No. 252, OECD Publishing, Paris.

Costa, T., Lopes, S., Fernandez-Llimós, S., Amante, M.J. & Lopes P.F. (2012). A Bibliometria e a Avaliação da Produção Científica: indicadores e ferramentas. *ACTAS - Congresso Nacional de Bibliotecários, Arquivistas e Documentalistas, 11*, pp.1–7.

Crede, Andreas (1995). Electronic Commerce and the Banking Industry: The Requirement and Opportunities for New Payment Systems Using the Internet. *Journal of Computer-Mediated Communication*, 1(3).

Decker, C. & Wattenhofer, R. (2013). Information propagation in the bitcoin network. In *Peer-to-Peer Computing (P2P)*, 2013 IEEE Thirteenth International Conference on (pp. 1-10). IEEE.

Dumitrescu, G.C. (2017). *Bitcoin – A Brief Analysis of the Advantages and Disadvantages*. Retrieved from: http://www.globeco.ro/wp-content/uploads/vol/split/vol_5_no_2/geo_2017_vol5_no2_art_008.pdf

European Central Bank (2016). A brave new world? What impact will distributed ledger technology have on the financial industry? *Focus*, 1, pp.1-9.

European Central Bank (2018). *Electronic money*. Available on: https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.htm

European Central Bank (2015). *Virtual currency schemes – a further analysis*. Available on: www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

ESMA- European Securities and Market Authority (2016) The Distributed Ledger Technology Applied to Securities Markets. *Discussion Paper 2016/773*.

Fabian, B., Ermakova, T. & Sander, U. (2016). *Anonymity in Bitcoin? –The Users’ Perspective*.

Fanti, G., & Viswanath, P. (2017). Anonymity Properties of the Bitcoin P2P Network. *arXiv preprint arXiv:1703.08761*.

Ferreira, M.L. (2017). Banco suíço é o primeiro a oferecer bitcoins aos clientes. *Observador*.

Disponível em: <https://observador.pt/2017/07/13/banco-suico-e-o-primeiro-a-oferecer-bitcoins-aos-clientes/>

Ferreira, M., Rodrigues, S., Reis, C. I. & Maximiano, M. (2018). Blockchain: A Tale of Two Applications, *Appl. Sci.* 8, 1506, 1-24.

Franco, P. (2014). *Understanding Bitcoin: Cryptography, engineering and economics*. John Wiley & Sons.

Fujita, M. & Thisse, J.F. (2013). *Economics of agglomeration: cities, industrial location, and globalization*. Cambridge: Cambridge University Press.

Fung, B., Molico, M. & Stuber, G. (2014). Electronic money and payments: recent developments and issues, Bank of Canada, *Discussion Paper*.

Fung, B. & Halaburda, H. (2014). Understanding platform-based digital currencies, *Bank of Canada Review*, Spring, pp. 12–20.

Gandal, N. & Halaburda, H. (2014). Competition in the cryptocurrency market, Bank of Canada, *Working Paper*, 2014 -33.

Gandal, N. & Halaburda, H. (2013). Some economics of private digital currency, Bank of Canada, *Working Paper*, 2013- 38.

Garman, C., Green, M., Miers, I. & Rubin, A. (2013). Zerocoin: anonymous distributed e-Cash from Bitcoin. In *IEEE Symposium on Security and Privacy* (Oakland).

Greenberg, A. (2011) Crypto currency. *Forbes*. Disponível em: <https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html#3d7469c4353e>

Grinberg, R. (2012). Bitcoin: an innovative alternative digital currency. *Hastings Sci. & Tech. LJ*, 4, p.159.

Hayes, A. (2017). *Bitcoin Predictions for 2017*. Investopedia.com. Retrieved from: <https://www.investopedia.com/news/bitcoin-predictions-2017/>

Hirst, P., Thompson, G. & Bromley, S. (2015). *Globalization in question*. New Jersey: John Wiley & Sons.

Huumo, J.Y., Ko, D., Choi, S., Park, S. & Smolander, K. (2016). Where is Current Research on Blockchain Technology? – A Systematic Review. *PloS ONE*, 11(10): e0163477.

Kalakota, R. & Whinston, B. A. (1996). *Frontiers of Electronic Commerce*. Singapore: Pearson Education.

Jarecki, S., Kiayias, A., Krawczyk, H. & Xu, J. (2016). Highly-Efficient and Composable Password-Protected Secret Sharing (Or: How to Protect Your Bitcoin Wallet Online). In *2016 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 276-291). IEEE.

Jornal Oficial da União Europeia (2009) *Directiva 2009/110/CE do Parlamento Europeu e do Conselho de 16 de Setembro de 2009 relativa ao acesso à actividade das instituições de moeda electrónica*. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32009L0110&from=EN>

Kristoufek, L. (2013). BitCoin meets Google Trends and Wikipedia: Quantifying the relationship between phenomena of the Internet era. *Scientific reports*, 3.

LexisNexis (2016). *True Cost of Fraud*. SM 2016 - LexisNexis. (n.d.). Retrieved from: <http://www.lexisnexis.com/risk/insights/true-cost-fraud.aspx>

Mainelli, M. & Milne, A. (2016) The impact and potential of Blockchain on the Securities Transaction Lifecycle. *Swift Institute Working Paper N° 2015-007*. Swift Institute.

Maltzahn, L. & Westland, S. (2016). *Banking in a world of programmable assets*. Accenture Strategy.

Mattila, J. (2016). The Blockchain Phenomenon: The Disruptive Potential of Distributed Consensus Architectures. *ETLA Working Papers N° 38*.

McCallum, B.T. (2014). Bitcoin Issues. *Shadow Open Market Committee Meeting*. New York, November 3, 2014.

Miller R., Michalski, W. & Stevens, B. (2002) *The future of money*, OECD PUBLICATIONS, France.

Miller, A., Juels, A., Shi, E., Parno, B. & Katz, J. (2014). Permacoin: Repurposing bitcoin work for data preservation, *2014 IEEE Symposium on Security and Privacy*, San Jose, CA, 2014, pp. 475-490.

Morgan Stanley Research (2016). Global Insight: Blockchain in Banking: Disruptive Threat or Tool? *Global Financials/ FinTech*, pp- 1-31.

Nakamoto, S. (20). *Bitcoin: A peer-to peer electronic payment system*.

Nasser, M. M. & Mahmood, K. (2009). Use of bibliometrics in LIS research. *LIBRES: Library of Information Science Research Electronic Journal*, 19 (2), pp. 1-11.

Oshodin, O, Molla, A. & Ong, C.E. (2016). An Information Systems Perspective on Digital Currencies: A Systematic Literature Review. *Australasian Conference on Information Systems*, Wollongong.

Pinna, A. & Ruttenberg, W. (2016). Distributed ledger technologies in securities post-trading: Revolution or evolution? *Occasional Paper Series N° 172*. European Central Bank.

Ponemon Institute. (2016). *2016 Cost of Data Breach Study: Global Analysis*. Ponemon Institute © Research Report. Retrieved from <https://app.clickdimensions.com/blob/> 2016 Cost of Data Breach Study: Global Analysis. (n.d.). Retrieved from <https://app.clickdimensions.com/blob/>

Pritchard, A. (1969). Statistical bibliography or bibliometrics? *Journal of Documentation*, 24, pp. 348-49.

Reid, F. & Harrigan, M. (2013). An analysis of anonymity in the Bitcoin system. In *Security and privacy in social networks* (pp. 197-223). Springer New York.

Researchomatic (2013). *Electronic And Mobile Commerce*. Available on: <http://www.researchomatic.com/electronic-and-mobile-commerce-181035.html>

Researchomatic (2013a). *Online Trading*. Available on: <http://www.researchomatic.com/online-trading-159326.html>

Reid, F. & Harrigan, M. (2013). *An analysis of anonymity in the bitcoin system* (pp. 197-223). New York: Springer.

Robleh, A., Barrdear, J., Clews. R. & Southgate, J. (2014). Innovations in payment technologies and the emergence of digital currencies. Bank of England, *Quarterly Bulletin*, 54 (3), pp. 262–75.

Robleh, A., Barrdear, J., Clews. R. & Southgate, J. (2014a). The economics of digital currencies. Bank of England, *Quarterly Bulletin*, 54 (3), pp. 276–86.

Ron, D. & Shamir, A. (2013). Quantitative analysis of the full bitcoin transaction graph. In *Financial Cryptography and Data Security* (pp. 6-24). Berlin Heidelberg: Springer.

Rostaing, H. (1996). *La bibliométrie et ses techniques*. Toulouse: Sciences de la Société.

Santori, M.A., DeRidder, C.A. & Grosser, J.M. (2016). *Blockchain Basics: A Primer. Advisory: Corporate & Securities – Technology*. Pillsbury Winthrop Shaw Pittman LLP.

Seaman, D. (2014). *The Bitcoin Primer: Risks, Opportunities, And Possibilities*. Amazon Digital Services LLC.

Shukairy, A. (2016). *E-commerce Fraud And Chargebacks – Statistics And Trends*. Retrieved from: <https://www.invespro.com/blog/e-commerce-fraud-and-chargebacks-infographic/>

Shum, V. (2014) *Regulating Digital Currencies: A Study on Bitcoin*. *Research Project for Emerging Issues/Advanced Topics Course*. University of Toronto.

SMU (2015). *Bitcoin scams steal at least \$11 million in virtual deposits from unsuspecting customers*. SMU Research News.

- Staples, M. & Niazi, M. (2007). Experiences using systematic review guidelines. *J. Syst. Softw.* 80, 1425–1437.
- Sumanjeet, S. (2009) Emergence of payment systems in the age of electronic commerce: the state of art. *Asia Pacific Journal of Finance and Banking Research*, 3 (3), 18-40.
- Sveriges Riksbank (2014). What is Bitcoin?, *Sveriges Riksbank Economic Review*, 2, pp. 71–87.
- Sveriges Riksbank (2014). Have virtual currencies affected the retail payments market?, *Economic Commentaries*, 2.
- Swan, M. (2015). *Blockchain. Blueprint for a New Economy*. Sebastopol: O'Reilly Media, Inc.
- Tague-Sutcliffe, J (1994). *Introducción a la informetría*. ACIMED, Havana, 3 (2), pp. 26- 35.
- Tedeev A.A. (2005). *Electronic Banking Services*. Moscow: Eksmo.
- Tsukerman, M. (2015). The Block is Hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future. *Berkeley Tech. LJ*, 30, 1127.
- Van Leeuwen, T. (2004). Descriptive Versus Evaluative Bibliometrics. In: Moed, H.F Glänzel, W., Schmoch, U. (Eds.), *Handbook of Quantitative Science and Technology Research*. Springer Netherlands, Dordrecht, pp. 373–388.
- Velde, F.R. (2013). Bitcoin: A primer. *Chicago Fed Letter*, 317. Essays on issues. The Federal Reserve Bank of Chicago.
- Vigna, P. & Casey, M. (2016). *The Age of CryptoCurrency*.
- Weber, W. (2015). Government and private e-money-like systems: Federal Reserve notes and national bank notes, Bank of Canada, *Working Paper*, 2015–18.
- Weber, W. (2015). The efficiency of private e-money-like systems: the US experience with national bank notes. Bank of Canada, *Working Paper*, 2015–3.
- Weber, W. (2014). The efficiency of private e-money-like systems: the US experience with state bank notes. Bank of Canada, *Working Paper*, 2014–15.
- WebWire. (2014). *Most Americans Still Don't Trust Bitcoin Despite Widespread Awareness*, New Survey Shows. WebWire.com
- White, H. D. & McCain, K. W. (1989). Bibliometrics. *Annual Review of Information Science and Technology*, 24, pp.119-86.

Yermack, D. (2013). *Is Bitcoin a real currency? An economic appraisal* (No. w19747). National Bureau of Economic Research.

Listagem das referências bibliográficas do corpus de estudos analisados

Andrychowicz, M. et al. (2014). Fair two-party computations via bitcoin deposits. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8438, pp. 105-121.

Baek, C. et al. (2015). Bitcoins as an investment or speculative vehicle? A first look. *Applied Economics Letters*, 22 (1), pp. 30-34.

Balcilar, M. et al. (2017). Can volume predict Bitcoin returns and volatility? A quantiles-based approach. *Economic Modelling*, 64, pp. 74-81.

Bamert, T. et al. (2013). Have a snack, pay with Bitcoins. *13th IEEE International Conference on Peer-to-Peer Computing, IEEE P2P 2013 - Proceedings*, art. no. 6688717.

Barber, S. et al. (2012). Bitter to better How to make bitcoin a better currency. *Lecture Notes in Computer Science*.

Bariviera, A.F. et al. (2017). The inefficiency of Bitcoin revisited: A dynamic approach. *Economics Letters*, 161, pp. 1-4.

Bariviera, A.F. et al. (2017). Some stylized facts of the Bitcoin market. *Physica A: Statistical Mechanics and its Applications*, 484, pp. 82-90.

Barratt, M.J. et al. (2013). Internet content regulation, public drug websites and the growth in hidden Internet services. *Drugs: Education, Prevention and Policy*, 20 (3), pp. 195-202.

Barratt, M.J. et al. (2016). ‘What if you live on top of a bakery and you like cakes?’—Drug use and harm trajectories before, during and after the emergence of Silk Road. *International Journal of Drug Policy*, 35, pp. 50-57.

Barratt, M.J. et al. (2016). Safer scoring? Cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy*.

Beck, R. et al. (2016). Blockchain - The gateway to trust-free cryptographic transactions. *24th European Conference on Information Systems, ECIS 2016*.

Becker, J. et al. (2013). Can we afford integrity by proof-of-work? scenarios inspired by the bitcoin currency. *The Economics of Information Security and Privacy*, pp. 135-156.

BenSasson, E.a et al. (2014). Zerocash: Decentralized anonymous payments from bitcoin. *Proceedings IEEE Symposium on Security and Privacy*, art. no. 6956581, pp. 459474.

Bentov, I. et al. (2014). How to use Bitcoin to design fair protocols. *Lecture Notes in Computer Science (inc luding subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8617 LNCS (PART 2), pp. 421-439.

Biryukov, A. et al. (2014). Deanonymisation of clients in bitcoin P2P network. *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 15-29.

Biryukov, A. et al. (2015). Bitcoin over tor isn't a good idea. *Proceedings - IEEE Symposium on Security and Privacy, 2015-July*, art. no. 7163022, pp. 122-134.

Bissias, G. et al. (2014). Sybil-resistant mixing for Bitcoin. *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 149-158.

Bjerg, O. (2016). How is Bitcoin Money?. *Theory, Culture & Society*, 33 (1), pp. 53-72.

Bohr, J. et al. (2014). Who Uses Bitcoin? An exploration of the Bitcoin community. *2014 12th Annual Conference on Privacy, Security and Trust, PST 2014*, art. no. 6890928, pp. 94-101.

Bonneau, J. et al. (2014). Mixcoin: Anonymity for bitcoin with accountable mixes. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8437, pp. 486-504.

Bonneau, J. et al. (2015). SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. *Proceedings IEEE Symposium on Security and Privacy, 2015-July*, art. no. 7163021, pp. 104121.

Bos, J.W. et al. (2014). Elliptic curve cryptography in practice. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8437, pp. 157-175.

Bouoiyour, J. et al. (2015). What does Bitcoin look like?. *Annals of Economics and Finance*, 16 (2), pp. 449-492.

Bouri, E. et al. (2017). Does Bitcoin hedge global uncertainty? Evidence from wavelet-based quantile-in-quantile regressions. *Finance Research Letters*, 23, pp. 87-95.

Bouri, E. et al. (2017). On the hedge and safe haven properties of Bitcoin: Is it really more than a diversifier?. *Finance Research Letters*, 20, pp. 192-198.

Bradbury, D. (2013). The problem with Bitcoin. *Computer Fraud and Security, 2013 (11)*, pp. 5-8.

Brandvold, M. et al. (2015). Price discovery on Bitcoin exchanges. *Journal of International Financial Markets, Institutions and Money*, 36, pp. 18-35.

- Brière, M. et al. (2015). Virtual currency, tangible return: Portfolio diversification with bitcoin. *Journal of Asset Management*, 16 (6), pp. 365-373.
- Bryans, D. (2014). Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal*, 89 (1), pp. 441-472.
- Carlsten, M. et al. (2016). On the instability of Bitcoin without the block reward. *Proceedings of the ACM Conference on Computer and Communications Security*, 24-28-October-2016, pp. 154-167.
- Castronova, E. (2014). Wildcat currency: How the virtual money revolution is transforming the economy. *Wildcat Currency: How the Virtual Money Revolution is Transforming the Economy*, pp. 1-265.
- Cheah, E. et al. (2015). Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. *Economics Letters*, 130, pp. 32-36.
- Cheung, A.W.-K. et al. (2015). Crypto-currency bubbles: an application of the Phillips–Shi–Yu (2013) methodology on Mt. Gox bitcoin prices. *Applied Economics*, 47 (23), pp. 2348-2358.
- Chu, J. et al. (2015). Statistical analysis of the exchange rate of bitcoin. *PLoS ONE*, 10 (7), art. no. E0133678.
- Chuen, D.L.K. (2015). Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, pp. 1-588.
- Ciaian, P. et al. (2016). The economics of BitCoin price formation. *Applied Economics*, 48 (19), pp. 1799- 1815.
- Clark, J. et al. (2012). CommitCoin: Carbon dating commitments with bitcoin. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7397 LNCS, pp. 390-398.
- Danezis, G. et al. (2013). Pinocchio coin: Building Zerocoin from a succinct pairing-based proof system. *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 27-29.
- Decker, C. et al. (2014). Bitcoin transaction malleability and mtgox. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8713 LNCS (PART 2), pp. 313-326.

Decker, C. et al. (2015). A fast and scalable payment network with bitcoin duplex micropayment channels. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9212, pp. 3-18.

Decker, C. et al. (2013). Information propagation in the Bitcoin network. 13th IEEE International Conference on Peer-to-Peer Computing, IEEE P2P 2013 Proceedings, art.no. 6688704.

Dinh, T.T.A. et al. (2017). BLOCKBENCH: A framework for analyzing private blockchains. *Proceedings of the ACM SIGMOD International Conference on Management of Data, Part F127746*, pp. 1085-1100.

Dodd, N. (2012). Simmel's Perfect Money: Fiction, Socialism and Utopia in The Philosophy of Money. *Theory, Culture & Society*, 29 (8), pp. 146-176.

Dorri, A. et al. (2017). Towards an optimized blockchain for IoT. *Proceedings - 2017 IEEE/ACM 2nd International Conference on Internet-of-Things Design and Implementation, IoTDI 2017 (part of CPS Week)*, pp. 173-178.

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

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

Dyhrberg, A.H. (2016). Hedging capabilities of bitcoin. Is it the virtual gold?. *Finance Research Letters*, 16, pp. 139-144.

Dziembowski, S. et al. (2015). Proofs of space. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9216, pp. 585-605.

Extance, A. (2015). The future of cryptocurrencies: Bitcoin and beyond. *Nature*, 526 (7571), pp. 21-23.

Eyal, I. (2015). The miner's dilemma. *Proceedings - IEEE Symposium on Security and Privacy, 2015-July*, art. no. 7163020, pp. 89-103.

Finn, E. (2017). What algorithms want: Imagination in the age of computing. *What Algorithms Want: Imagination in the Age of Computing*, pp. 1-257.

Frantz, C.K. et al. (2016). From institutions to code: Towards automated generation of smart contracts. *Proceedings - IEEE 1st International Workshops on Foundations and Applications of Self-Systems, FAS-W 2016*, art.no. 7789470, pp. 210-215.

Fry, J. et al. (2016). Negative bubbles and shocks in cryptocurrency markets. *International Review of Financial Analysis*, 47, pp. 343 -352.

Garcia, D. et al. (2014). The digital traces of bubbles: Feedback cycles between socio-economic signals in the Bitcoin economy. *Journal of the Royal Society Interface*, 11 (99), art. no. 0623.

Gervais, A. et al. (2014). Is Bitcoin a Decentralized Currency?. *IEEE Security and Privacy*, 12 (3), art. no. 6824541, pp. 54-60.

Gervais, A. et al. (2014). On the privacy provisions of bloom filters in lightweight bitcoin clients. *ACM International Conference Proceeding Series, 2014-December (December)*, pp. 326-335.

Gervais, A. et al. (2015). Tampering with the delivery of blocks and transactions in Bitcoin. *Proceedings of the ACM Conference on Computer and Communications Security, 2015-October*, pp. 692-705.

Gilad, Y. et al. (2017). Algorand: Scaling Byzantine Agreements for Cryptocurrencies. *SOSP 2017 - Proceedings of the 26th ACM Symposium on Operating Systems Principles*, pp. 51-68.

Glaser, F. et al. (2014). Bitcoin - Asset or currency? Revealing users' hidden intentions. *ECIS 2014 Proceedings - 22nd European Conference on Information Systems*.

Glaser, F. et al. (2015). Beyond cryptocurrencies - A taxonomy of decentralized consensus systems. *23rd European Conference on Information Systems, ECIS 2015, 2015-May*.

Groth, J. et al. (2015). One-out-of-many proofs: Or how to leak a secret and spend a coin. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9057, pp. 253-280.

Huh, S. et al. (2017). Managing IoT devices using blockchain platform. *International Conference on Advanced Communication Technology, ICACT*, art. no. 7890132, pp. 464-467.

Ifrim, G. et al. (2014). Event detection in Twitter using aggressive filtering and hierarchical tweet clustering. *CEUR Workshop Proceedings, 1150*, pp. 33-40.

Jarecki, S. et al. (2016). Highly-efficient and composable password-protected secret sharing (Or: How to Protect Your Bitcoin Wallet Online). *Proceedings - 2016 IEEE European Symposium on Security and Privacy, EURO S and P 2016*, art.no. 7467360, pp. 276-291.

Johnson, B. et al. (2014). Game-theoretic analysis of DDoS attacks against bitcoin mining pools. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8438, pp. 72-86.

- Juels, A. et al. (2016). The ring of gyges: Investigating the future of criminal smart contracts. *Proceedings of the ACM Conference on Computer and Communications Security, 24-28-October-2016*, pp. 283-295.
- Karame, G.O. et al. (2012). Doublespending fast payments in Bitcoin. *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 906917.
- Karame, G.O. et al. (2015). Misbehavior in Bitcoin: A study of double-spending and accountability. *ACM Transactions on Information and System Security*, 18 (1).
- Karlstrøm, H. (2014). Do libertarians dream of electric coins? The material embeddedness of bitcoin. *Distinktion*, 15 (1), pp. 23-36.
- Katsiampa, P. (2017). Volatility estimation for Bitcoin: A comparison of GARCH models. *Economics Letters*, 158, pp. 3-6.
- Khan, M.A. et al. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82, pp. 395-411.
- Kiayias, A. et al. (2016). Blockchain mining games. EC 2016 - *Proceedings of the 2016 ACM Conference on Economics and Computation*, pp. 365-382.
- Kiayias, A. et al. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10401 LNCS, pp. 357-388.
- Kiviat, T.I. (2015). Beyond Bitcoin: Issues in regulating blockchain transactions. *Duke Law Journal*, 65 (3), pp. 569-608.
- Kondor, D. et al. (2014). Do the rich get richer? An empirical analysis of the Bitcoin transaction network. *PLoS ONE*, 9 (2), art. no. E86197.
- Koshy, P. et al. (2014). An analysis of anonymity in bitcoin using P2P network traffic. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8437, pp. 469-485.
- Kostakis, V. et al. (2014). The (A)political economy of bitcoin. *TripleC*, 12 (2), pp. 431-440.
- Kraft, D. (2016). Difficulty control for blockchain-based consensus systems. *Peer-to-Peer Networking and Applications*, 9 (2), pp. 397 -413.
- Kristoufek, L. (2015). What are the main drivers of the bitcoin price? Evidence from wavelet coherence analysis. *PLoS ONE*, 10 (4), art. no. E0123923.

- Kumaresan, R. et al. (2014). How to use bitcoin to incentivize correct computations. *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 30-41.
- Kumaresan, R. et al. (2015). How to use bitcoin to play decentralized poker. *Proceedings of the ACM Conference on Computer and Communications Security, 2015-October*, pp. 195-206.
- Kuo, T.-T. et al. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 24 (6), pp. 1211-1220. *Lecture Notes in Bioinformatics*, 7397 LNCS, pp. 399-414.
- Lewenberg, Y. et al. (2015). Bitcoin mining pools: A cooperative game theoretic analysis. *Proceedings of the International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS, 2*, pp. 919-927.
- Lewenberg, Y. et al. (2015). Inclusive block chain protocols. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8975, pp. 528-547.
- Li, X. et al. (2017). The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. *Decision Support Systems*, 95, pp. 49-60.
- Liao, K. et al. (2016). Behind closed doors: Measurement and analysis of CryptoLocker ransoms in Bitcoin. *eCrime Researchers Summit, eCrime, 2016-June*, art. no. 7487938, pp. 1-13.
- Lischke, M. et al. (2016). Analyzing the bitcoin network: The First Four Years. *Future Internet*, 8 (1), art. no. 7.
- Lustig, C. et al. (2015). Algorithmic authority: The case of Bitcoin. *Proceedings of the Annual Hawaii International Conference on System Sciences, 2015-March*, art. no. 7069744, pp. 743-752.
- Luther, W.J. (2016). CRYPTOCURRENCIES, NETWORK EFFECTS, AND SWITCHING COSTS. *Contemporary Economic Policy*, 34 (3), pp. 553-571.
- Luu, L. et al. (2015). Demystifying incentives in the consensus computer. *Proceedings of the ACM Conference on Computer and Communications Security, 2015-October*, pp. 706-719.
- Luu, L. et al. (2016). A secure sharding protocol for open blockchains. *Proceedings of the ACM Conference on Computer and Communications Security, 24-28-October-2016*, pp. 17-30.
- Magaki, I. et al. (2016). ASIC Clouds: Specializing the Datacenter. *Proceedings - 2016 43rd International Symposium on Computer Architecture, ISCA 2016*, art. no. 7551392, pp. 178-190.

Meiklejohn, S. et al. (2016). A fistful of Bitcoins: Characterizing payments among men with no names. *Communications of the ACM*, 59 (4), pp. 86-93.

Meiklejohn, S.a et al. (2013) .A fistful of bitcoins: Characterizing payments among men with no names. *Proceedings of the ACM SIGCOMM Internet Measurement Conference , IMC*, pp. 127139.

Miers, I. et al. (2013). Zerocoin: Anonymous distributed ecash from bitcoin. *Proceedings IEEE Symposium on Security and Privacy*, art. no. 6547123, pp. 397411.

Mihaylov, M. et al. (2014). NRG-X-change a novel mechanism for trading of renewable energy in smart grids. *SMARTGREENS 2014 - Proceedings of the 3rd International Conference on Smart Grids and Green IT Systems*, pp. 101-106.

Mihaylov, M. et al.(2014). NRGcoin: Virtual currency for trading of renewable energy in smart grids. *International Conference on the European Energy Market, EEM*, art. no . 6861213.

Miller, A. et al. (2014). Permacoin: Repurposing bitcoin work for data preservation. *Proceedings - IEEE Symposium on Security and Privacy*, art. no. 6956582, pp. 475-490.

Moore, T. et al. (2013). Beware the middleman: Empirical analysis of Bitcoin-exchange risk.

Moser, M. et al. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. *eCrime Researchers Summit, eCrime*, art. no. 6805780.

Möser, M. et al. (2015). Trends, tips, tolls: A longitudinal study of bitcoin transaction fees. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8976, pp. 19-33.

Nadarajah, S. et al. (2017). On the inefficiency of Bitcoin. *Economics Letters*, 150, pp. 6-9.

Nayak, K. et al. (2016). Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. *Proceedings - 2016 IEEE European Symposium on Security and Privacy, EURO S and P 2016*, art. no. 7467362, pp. 305-320.

Ober, M. et al. (2013) . Structure and anonymity of the bitcoin transaction graph. *Future Internet*, 5 (2), pp. 237-250.

O'Dwyert, K.J. et al. (2014). Bitcoin mining and its energy footprint. *IET Conference Publications, 2014 (CP639)*, pp. 280-285.

Ølnes, S. (2016). Beyond Bitcoin enabling smart government using blockchain technology. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9820 LNCS, pp. 253-264.

Ouaddah, A. et al. (2016). FairAccess: a new Blockchain-based access control framework for the Internet of Things. *Security and Communication Networks*, 9 (18), pp. 5943-5964.

Ouaddah, A. et al. (2017). Towards a novel privacy-preserving access control model based on blockchain technology in IoT. *Advances in Intelligent Systems and Computing*, 520, pp. 523-533.

Phelps, A. et al. (2014). I shop online - Recreationally! Internet anonymity and Silk Road enabling drug use in Australia. *Digital Investigation*, 11 (4), pp. 261-272.

Plohmann, D. et al. (2012). Case study of the Miner Botnet. *2012 4th International Conference on Cyber Conflict, CYCON 2012 - Proceedings*, art. no. 6243985.

Polasik, M. et al. (2015). Price fluctuations and the use of bitcoin: An empirical inquiry. *International Journal of Electronic Commerce*, 20 (1), pp. 9- 49.

Reid, F. et al. (2011). An analysis of anonymity in the Bitcoin system. *Proceedings - 2011 IEEE International Conference on Privacy, Security, Risk and Trust and IEEE International Conference on Social Computing, PASSAT/SocialCom 2011*, art. no. 6113303, pp. 1318-1326.

Ron, D. et al. (2013) . Quantitative analysis of the full Bitcoin transaction graph. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7859 LNCS, pp. 624.

Ruffing, T. et al (2015). Liar, Liar, coins on fire!: Penalizing equivocation by loss of bitcoins. *Proceedings of the ACM Conference on Computer and Communications Security, 2015-October*, pp. 219-230.

Ruffing, T. et al. (2014). CoinShuffle: Practical decentralized coin mixing for bitcoin. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8713 LNCS (PART 2), pp. 345-364.

Sapirshtein, A. et al. (2017). Optimal selfish mining strategies in bitcoin. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9603 LNCS, pp. 515-532.

Sharpley, M. et al. (2016). The blockchain and kudos: A distributed system for educational record, reputation and reward. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9891 LNCS, pp. 490-496.

Sompolinsky, Y. et al. (2015). Secure high-rate transaction processing in bitcoin. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8975, pp. 507-527.

Spagnuolo, M. et al. (2014). Bitiodine: Extracting intelligence from the bitcoin network. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8437, pp. 457-468.

Stokes, R. (2012). Virtual money laundering: the case of Bitcoin and the Linden dollar. *Information and Communications Technology Law*, 21 (3), pp. 221 -236.

Taylor, M.B. (2013). Bitcoin and the age of Bespoke Silicon. *2013 International Conference on Compilers, Architecture and Synthesis for Embedded Systems, CASES 2013*, art.no. 6662520.

Tschorsch, F. et al. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys and Tutorials*, 18 (3), art. no. 7423672, pp . 20842123.

Tu, K.V. et al. (2015). Rethinking virtual currency regulation in the bitcoin age. *Washington Law Review*, 90 (1), pp. 271-347.

Urquhart, A. (2016). The inefficiency of Bitcoin. *Economics Letters*, 1 48, pp. 80-82.

Urquhart, A. (2017). Price clustering in Bitcoin. *Economics Letters*, 1 59, pp. 145-148.

Valenta, L. et al. (2015). Blindcoin: Blinded, accountable mixes for bitcoin. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8976, pp. 112-126.

Van Alstyne, M. (2014). Economic and business dimensions: Why bitcoin has value. *Communications of the ACM*, 57 (5), pp. 30-32.

van de Pol, J. et al. (2015). Just a little bit more. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9048, pp. 3-21.

Vasek, M. et al. (2014). Empirical analysis of denial-of-service attacks in the bitcoin ecosystem. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8438, pp. 57-71.

Vovchenko, N.G. et al. (2017). Electronic currency: The potential risks to national security and methods to minimize them. *European Research Studies Journal*, 20 (1), pp. 36-48.

Watanabe, H. et al. (2016). Blockchain contract: A complete consensus using blockchain. *2015 IEEE 4th Global Conference on Consumer Electronics , GCCE 2015*, art. no. 7398721, pp. 577-578.

Weber, B. (2015). Bitcoin and the legitimacy crisis of money. *Cambridge Journal of Economics*, 40 (1), pp. 17-41.

Wörner, D. et al. (2014). When your sensor earns money: Exchanging data for cash with Bitcoin. *UbiComp 2014 - Adjunct Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pp. 295-298.

Yelowitz, A. et al. (2015). Characteristics of Bitcoin users: an analysis of Google search data. *Applied Economics Letters*, 22 (13), pp. 1030-1036.

Zhang, F. et al. (2016). Town crier: An authenticated data feed for smart contracts. *Proceedings of the ACM Conference on Computer and Communications Security, 24-28-October-2016*, pp. 270-282.

Zhang, Y. et al. (2015). An IoT electric business model based on the protocol of bitcoin. *2015 18th International Conference on Intelligence in Next Generation Networks, ICIN 2015*, art.no. 7073830, pp. 184-191.

Zhang, Y. et al. (2017). The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications*, 10 (4), pp. 983-994.

Zheng, Z. et al. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, art.no. 8029379, pp. 557-564.

Ziegeldorf, J.H. et al. (2015). CoinParty: Secure multi-party mixing of bitcoins. *CODASPY 2015 - Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, pp. 75-86.

Zohar, A. (2015). Bitcoin: Under the hood. *Communications of the ACM*, 58 (9), pp. 104-113.

Anexos

Anexo 1 – Listagem dos 20 artigos mais citados

	Ano da Publicação	Artigo	Fonte/Revista	Área Científica	Impacto da citação	Proeminência percentual	Nº de citações recebidas	Max. de citações por ano
1	2013	Meiklejohn, S. et al.” A fistful of bitcoins: Characterizing payments among men with no names”	Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC	Ciências da Computação	21.79	99.530	164	47
2	2014	Ben-Sasson, E. et al.”Zerocash: Decentralized anonymous payments from bitcoin”	Proceedings - IEEE Symposium on Security and Privacy	Ciências da Computação	46.58	99.530	160	56
3	2013	Miers, I. et al. “ Zerocoin: Anonymous distributed e-cash from bitcoin”	Proceedings - IEEE Symposium on Security and Privacy	Ciências da Computação	35.97	99.530	154	45
4	2015	Bonneau, J. et al “ SoK: Research perspectives and challenges for bitcoin and cryptocurrencies”	Proceedings - IEEE Symposium on Security and Privacy	Economia	54.76	99.530	141	57
5	2013	Ron, D. et al. “Quantitative analysis of the full Bitcoin transaction graph”	Lecture Notes in Computer Science	Ciências da Computação	23.35	99.530	139	37
6	2013	Decker, C. et al. “Information propagation in the Bitcoin network”	13th IEEE International Conference on Peer-to-Peer Computing	Ciências da Computação	23.34	99.530	116	39
7	2012	Barber, S. et al. “Bitter to better - How to make bitcoin a better currency”	Lecture Notes in Computer Science	Ciências da Computação	15.67	99.530	113	27
8	2012	Karame, G.O. et al “Double-spending fast payments in Bitcoin”	Proceedings of the ACM Conference on Computer and Communications Security	Ciências da Computação	9.15	99.530	83	24
9	2016	Tschorsch, F. et al. “ Bitcoin and beyond: A technical survey on decentralized digital currencies”	IEEE Communications Surveys and Tutorials	Ciências da Computação	16.16	99.530	75	45
10	2013	Moore, T. et al “ Beware the middleman: Empirical analysis of Bitcoin-exchange risk”	Lecture Notes in Computer Science	Ciências da Computação	11.50	99.530	59	14

11	2015	Kristoufek, L. “ What are the main drivers of the bitcoin price? Evidence from wavelet coherence analysis”	PLoS ONE	Economia	7.81	99.530	58	33
12	2016	Urquhart, A. “ The inefficiency of Bitcoin”	<i>Economics Letters</i>	Economia	16.69	99.530	55	47
13	2014	Bentov, I. et al . “How to use Bitcoin to design fair protocols”	<i>Lecture Notes in Computer Science</i>	Ciências da Computação	13.96	99.530	54	23
14	2015	Cheah, E.-T. et al.” Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin”	<i>Economics Letters</i>	Economia	10.07	99.530	54	40
15	2013	Ober, M. et al “Structure and anonymity of the bitcoin transaction graph”	<i>Future Internet</i>	Ciências da Computação	4.66	99.530	54	12
16	2014	Miller, A. et al. “Permacoin: Repurposing bitcoin work for data preservation”	<i>Proceedings - IEEE Symposium on Security and Privacy</i>	Ciências da Computação	13.57	99.530	51	21
17	2013	Moser, M. et al. “An inquiry into money laundering tools in the Bitcoin ecosystem”	<i>Crime Researchers Summit, eCrime</i>	Criminologia	9.92	99.530	50	14
18	2014	Garcia, D. et al. “The digital traces of bubbles: Feedback cycles between socio-economic signals in the Bitcoin economy”	<i>Journal of the Royal Society Interface</i>	Economia	2.76	99.530	49	19
19	2011	Reid, F. et al. “An analysis of anonymity in the Bitcoin system”	<i>Proceedings - 2011 IEEE International Conference on Privacy, Security, Risk and Trust and IEEE International Conference on Social Computing</i>	Ciências da Computação	5.32	99.530	48	13
20	2015	Sompolinsky, Y. et al. “Secure high-rate transaction processing in bitcoin”	<i>Lecture Notes in Computer Science</i>	Ciências da Computação	19.35	99.530	47	21