Revista UNITAS
ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

ENSAIO SOBRE A NATUREZA DO BITCOIN, O CONTEXTO DE SUA CRIAÇÃO E SEU MODO DE FUNCIONAMENTO

Adryan Bracht Juver[1]
Prof. Esp. Cristiane Schmitz Rambo[2]

Resumo: O presente artigo busca estabelecer, em um diminuto número de páginas, alguns princípios básicos que cercam a natureza da rede Bitcoin, discorrendo sobre a filosofia presente na sua concepção e os fins pretendidos pelo seu criador. Como ponto de partida, a crise econômica de 2008 se mostra um evento essencial para a correta compreensão dos objetivos principais do Bitcoin, e merece ser estudada de modo aprofundado. Superado este primeiro ponto, será possível tratar com mais propriedade das questões técnicas atinentes ao objeto, estabelecendo os motivos que tornam o Bitcoin uma revolução para o mercado financeiro. Completando este trabalho, a estrutura da *blockchain* também terá seu lugar de destaque, sendo analisada com certa profundidade, destacando suas principais benesses e falhas, ponderando se ela poderá, eventualmente, ser adotada pelos sistemas financeiros tradicionais.
Palavras-chave: Bitcoin. *Blockchain*. Mineração. Criptomoeda.

Abstract: This article seeks to set, in some few pages, basic principles that are essential to understand Bitcoin, writing about its philosophy, what it represents and what exactly did his creator wanted to achieve. As a starting point, the 2008 economic crisis shows itself as a key factor to acknowledging Bitcoin's base principles, and rightfully deserves to be studied. After this first goal is achieved, it will be possible to deal properly with the technical matters about Bitcoin, showing why it is so big of a revolution to mankind. Moving towards the end, blockchain itself should gain its rightful place as a standout technology, being analyzed in depth, both its flaws and its qualities, considering if its worthy of being adopted by the traditional financial systems.
Key words: Bitcoin. Blockchain. Mining. Crypto-asset.

1 INTRODUÇÃO

A tarefa que se apresenta no horizonte, imponente e altiva, sabe-se, não será fácil. Tanto não o é que, em toda esta última década, autoridades do mundo inteiro se mostraram incapazes de fornecer um caminho sólido e seguro a ser trilhado, na busca de uma solução para a problemática que envolve o Bitcoin. Muitos, porém, já iniciam sua caminhada direcionados ao fracasso iminente. Presos em conceitos pré-estabelecidos, seus passos vacilantes não tendem senão ao precipício.

[1] Acadêmico do Curso de Graduação em Direito da UCEFF. E-mail: adryan.juver@outlook.com
[2] Graduada em Direito (2011). Pós-Graduada em Direito Civil e Processo Civil (2015). Professora do Centro Universitário FAI - UCEFF de Itapiranga. E-mail: cristianerambo@uceff.edu.br

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

Entre os maiores erros dos juristas, é possível destacar aquele que talvez seja o calcanhar de Aquiles de muitos: a arrogância. Mais do que em outras ciências, os operadores forenses possuem um orgulho que, por vezes, lhes custa muito caro. O ramo jurídico se encontra demasiadamente isolado, alheio ao que acontece ao seu redor. Com isto, perde-se a função primordial, a razão de ser de um ordenamento jurídico, que é permitir o bom funcionamento da sociedade, auxiliar em sua caminhada, tal como o faz Atlas, o titã grego, encarregado de suportar o peso do mundo em suas costas. O papel dos juristas deve ser solidário ao de Atlas, pois ambos se assemelham muito.

Entretanto, esta é uma incumbência que nem sempre é prestada com a eficiência devida. Legislações infundadas e hermenêuticas falhas são mais comuns do que deveriam. Este é um luxo que a sociedade não pode custear, é uma trilha que não pode ser seguida neste projeto. Preferir-se-á o caminho tortuoso e penoso, para que a recompensa final seja maior. Então, inicie-se a caminhada.

O primeiro ponto de parada, na construção que foi proposta, se presta a explicar todos os conceitos técnicos do Bitcoin. É preciso analisar a sua essência, seu íntimo, compreender exatamente qual a sua função primordial e como se dá seu funcionamento. Indo ao encontro daquilo que se afirmou nos parágrafos acima, destaque-se desde logo que estas respostas não estarão no mundo jurídico, pois fogem da sua área de competência típica. É necessário se abastecer dos conhecimentos provindos de outras ciências. Por enquanto, análises técnicas e históricas ditarão o rumo que será seguido. Posteriormente, os caminhos jurídicos serão abordados, mas agora não é o momento de fazê-lo.

2 A GRANDE CRISE ECONÔMICA DE 2008 E SUA RELAÇÃO COM O BITCOIN

O marco inicial do estado de coisas que está sendo tratado aqui (leia-se: adoção em massa das criptomoedas) possui seu início ao final da década passada, após a criação do Bitcoin e a prova de que, sim, seu protocolo realmente funcionava. Entretanto, uma análise mais completa necessitará buscar os motivos determinantes para o seu surgimento, na busca de entender, de modo adequado, a sua natureza e os objetivos que esta rede almejou (e almeja) alcançar.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

De um modo geral, toda a bibliografia existente sobre o Bitcoin possui um ponto de partida único: a crise econômica iniciada no mercado imobiliário americano, entre os anos de 2007 e 2008. Há uma convergência entre todos os grandes nomes da área, que reforçam a importância deste evento para entender o que está por trás do Bitcoin. A partir de agora, que esta crise seja analisada.

O ano de 2008 pode ser definido como o termo final da derrocada de um sistema financeiro que desafiava todas as regras básicas da economia há várias décadas. Fernando Ulrich, economista e autor de uma das mais brilhantes obras sobre Bitcoin já produzidas, reforça o coro sobre o excesso de intervencionismo estatal no mercado. O monopólio de emissão de moeda e a falta de limites aos Bancos Centrais são aspectos importantes deste cenário. Há muito que a inflação e a emissão ilimitada de moeda retiraram o lastro econômico das moedas estatais, tornando-as meramente fiduciárias. A moeda estatal já não possuía mais nenhum resquício de valor intrínseco, e este fato tornou-a vulnerável aos acontecimentos que o mundo presenciou.[3]

Nas décadas anteriores ao desastre, as políticas econômicas adotadas pelo governo americano, embora questionáveis, não eram incoerentes. O objetivo sempre esteve claro: facilitar a aquisição de imóveis por pessoas de baixa renda, através da expansão creditícia no mercado financeiro. O resultado? Uma sequência gigantesca de empréstimos de má qualidade.[4]

Colocando em termos práticos: quando um banco realiza um empréstimo para um particular, estará concedendo um crédito imediato para este, em troca da promessa de receber, em um tempo futuro, aquele mesmo valor, acrescido de juros. Em teoria, o banco deveria colocar limitações na quantidade de empréstimos realizados, para não ameaçar seu próprio patrimônio em caso de inadimplências. Porém, este risco, na sociedade americana, era afastado dos bancos e suportado por outras duas empresas, essenciais para a compreensão do panorama geral da crise.

As empresas em questão são a *Federal National Mortgage Association* (popular “Fannie Mae”) e a *Federal Home Loan Mortgage Corporation* (popular “Freddie Mac”). Ambas foram concedidas por iniciativa do governo dos Estados Unidos da América. A sua função primordial? Expandir e facilitar a realização de hipotecas no país. Fannie

[3] ULRICH, Fernando. **Bitcoin**: a moeda na era digital. São Paulo – SP: Instituto Ludwig von Mises Brasil. 2014. s/p. Edição do Kindle.
[4] BOOTH, Philip. **Verdict on The Crash**: Causes and Policy Implications. The Institute of Economic Affairs: Great Britain, 2009.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

Mae e Freddie Mac entravam em ação logo após a realização de um empréstimo bancário, momento em que se responsabilizavam por comprar os ativos do banco e cobrá-los do devedor no termo final estipulado, liberando a instituição bancária para realizar novos negócios. Deve-se destacar que as duas empresas gozavam de um fundo de proteção de crédito provido pelo governo americano.[5]

Logo, quando o título hipotecário (afinal, o assunto é a expansão de crédito no setor imobiliário) era vendido pelo banco, os riscos da operação passavam a ser suportados por Fannie e Freddie, que compravam os ativos. Porém, com alguma frequência, estas também não realizavam a retenção do título. Era costume revende-los para investidores interessados, que, bem cientes da proteção de crédito conferida pelo governo, pensavam estar segurados, em caso de inadimplência.[6]

De fato, este fundo de garantia poderia ter sido eficiente, se a qualidade dos empréstimos realizados fosse alta. Mas ela não era, muito em razão da interferência do chamado *Community Reinvestment Act*, uma política pública de inclusão social americana, que visava facilitar a concessão de empréstimos para que pessoas de baixa renda pudessem adquirir um imóvel próprio. A fonte disto é o próprio *Federal Reserve System*, o Banco Central dos Estados Unidos da América, que afirma, com todas as letras:

> *Securitization of affordable housing loans expanded, as did the secondary market for those loans, in part reflecting a 1992 law that required* ***the government-sponsored enterprises, Fannie Mae and Freddie Mac, to devote a percentage of their activities to meeting affordable housing goals***.[7] [8] (grifo nosso)

[5] LIEBOWITZ, Stan J. **Anatomy of a Train Wreck**: Causes of the Mortgage Meltdown. Independent Policy Report. Disponível em: <http://www.independent.org/pdf/policy_reports/2008-10-03-trainwreck.pdf>. Acesso em: 11 nov 2019.

[6] BOOTH, Philip. **Verdict on The Crash**: Causes and Policy Implications. The Institute of Economic Affairs: Great Britain, 2009.

[7] A securitização de hipotecas a preços acessíveis foi expandida, assim como o mercado secundário de negociação destas ações, que se deve, em parte, à uma legislação de 1992 que exigiu que **Fannie Mae e Freddie Mac, empresas patrocinadas pelo governo, dedicassem uma porcentagem de suas atividades para realizar metas de inclusão para empréstimos hipotecários**. Tradução e grifos nossos.

[8] BERNANKE, Ben S. **The Community Reinvestment Act:** Its Evolution and New Challenges. Federal Reserve System. Disponível em: <https://www.federalreserve.gov/newsevents/speech/Bernanke20070330a.htm>. Acesso em: 09 nov 2019.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

A existência e a motivação do *Community Reinvestment Act* não são controversas. Como se vê, há uma ordem deliberada do governo americano para que Fannie e Freddie incentivassem tais negócios, a despeito de sua má qualidade. Os bancos também eram estimulados a promover a mesma inclusão, porque sabiam que Fannie e Freddie estavam sempre ali, prontas para comprar o título e assumir os riscos assim que o empréstimo fosse realizado (com garantias conferidas pelo governo, observe). Em suma, o padrão exigido para se conseguir um empréstimo foi absurdamente reduzido, e isto contribuiu para os altos índices de inadimplência que começaram a crescer em 2007.[9]

Como não havia uma avaliação rígida sobre a viabilidade dos empréstimos, os títulos resultantes eram de alto risco. Os investidores, acreditando na sua qualidade e pensando estarem protegidos, acabavam por adquiri-los, financiando todo o sistema e aumentando a "bola de neve" que precedeu o desastre.[10]

Esta sequência ininterrupta de empréstimos inviáveis sendo realizados acabou resultando em um aumento exponencial das taxas de inadimplência ao final do ano de 2007, fato que se prolongou até o ano seguinte. Para dar ao leitor uma ideia melhor sobre a quantidade de negócios ruins realizados, os dados abaixo são importantes:

> *Fannie Mae and Freddie Mac were created as government-sponsored enterprises. Beginning in 1992, Congress pushed Fannie Mae and Freddie Mac to increase their purchases of mortgages going to low- and moderate-income borrowers. In 1996, HUD, the department of Housing and Urban Development, gave Fannie Mae and Freddie Mac an explicit target: 42 per cent of their mortgage financing had to go to borrowers with incomes below the median income in their area. The target increased to 50 per cent in 2000 and 52 per cent in 2005.*[11] [12]

A partir dos dados levantados acima, é possível aferir uma compreensão maior acerca dos motivos determinantes desta crise. O aumento da inadimplência acabou

[9] LIEBOWITZ, Stan J. **The Real Scandal**. New York Post. Disponível em: <https://nypost.com/2008/02/05/the-real-scandal/>. Acesso em: 09 nov 2019.
[10] BOOTH, Philip. **Verdict on The Crash**: Causes and Policy Implications. The Institute of Economic Affairs: Great Britain, 2009.
[11] "Fannie Mae e Freddie Mac foram criadas como empresas financiadas pelo governo. A partir de 1992, o Congresso pressionou Fannie Mae e Freddie Mac a aumentar a compra de hipotecas destinadas para pessoas de baixa e média renda. Em 1996, o HUD, "Housing and Urban Development", ordenou que Fannie Mae e Freddie Mac perseguissem uma meta clara: 42% dos seus financiamentos de hipotecas deveria ser destinado para tomadores de empréstimo de baixa e média renda. Essa meta atingiu 50% no ano 2000 e 52% em 2005." Tradução nossa.
[12] BOOTH, Philip. **Verdict on The Crash**: Causes and Policy Implications. The Institute of Economic Affairs: Great Britain, 2009.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

resultando na diminuição do patrimônio de vários grandes bancos de investimento americanos, rotineiros compradores dos títulos oferecidos por Fannie Mae e Freddie Mac. Em setembro de 2007, o banco *Northern Rock* se tornou insolvente.[13] Um ano depois, em setembro de 2008, o gigante americano *Lehman Brothers* tornou público seu estado de falência.[14] Não houve ajuda.

Além destes citados, incontáveis outros bancos também sofreram perdas irreversíveis quando o cenário se deteriorou. Correntistas ficaram impossibilitados de sacar seu dinheiro, simplesmente porque não havia mais nenhum. Fannie Mae e Freddie Mac, empresas estatais que são, receberam 187 bilhões de dólares do Tesouro americano para quitarem suas dívidas.[15]

Após toda esta construção, seria razoável esperar que, com o fracasso completo das instituições estatais na economia, suas políticas fossem alteradas. Ora, o Estado fora o responsável por instituir Fannie e Freddie. O Estado, através do *Community Reinvestment Act,* ordenou a realização de hipotecas para pessoas que não possuíam condições de arcar com elas, e, como se não bastasse, incentivou investidores a adquirirem estes títulos, financiando todo um sistema falido. Mas, ao contrário, as autoridades monetárias se mostraram ainda mais centralizadas, opressivas e irresponsáveis, ignorando o fato de que suas políticas trouxeram a recessão de 2008.[16]

É neste ponto que nasce o Bitcoin. Seu *paper* foi publicado para o mundo somente algum tempo depois da falência do banco *Lehman Brothers*. Surgindo naquele momento, o Bitcoin representou uma total independência para com os Estados. Suas transações não são garantidas por nenhum intermediário, mas, sim, pela criptografia presente no sistema. Sua rede não opera de modo centralizado, de sorte que não existe nenhum órgão central no protocolo. As transações e as eventuais mudanças no sistema ocorrem de modo público, em claro sinal de protesto às

[13] BBC News. **Northern Rock gets bank bail out**. Disponível em: <http://news.bbc.co.uk/2/hi/business/6994099.stm>. Acesso em: 11 de nov 2019.
[14] THE GUARDIAN. **Lehman Brothers goes bankrupt, 15 September**. Disponível em: <https://www.theguardian.com/world/2008/dec/28/lehman-brothers-bankrupt-eyewitness-account>. Acesso em: 11 de nov 2019.
[15] AMADEO, Kimberly. **What Was the Fannie Mae and Freddie Mac Bailout?** The Balance. Disponível em: <https://www.thebalance.com/what-was-the-fannie-mae-and-freddie-mac-bailout-3305658>. Acesso em: 11 de nov 2019.
[16] ULRICH, Fernando. **Bitcoin**: a moeda na era digital. São Paulo – SP: Instituto Ludwig von Mises Brasil. 2014. s/p. Edição do Kindle.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

reuniões de portas fechadas nos Bancos Centrais ao redor do mundo, que decidem unilateralmente o destino do dinheiro da população.

A (longa) explanação feita permite que o leitor possua um conhecimento muito importante acerca da razão de ser do Bitcoin. Não se está tratando de uma simples moeda qualquer, mas, sim, de uma tecnologia peculiar, com várias aplicações. Acima de tudo, o Bitcoin representa uma liberdade em relação às amarras estatais.[17] A sua aura de independência deve ser preservada, sob pena de torna-lo inútil, de retirar todas as características que o tornam especial. Uma regulamentação pode ser necessária, mas há que se ter muito cuidado com o provimento final, evitando regulações proibitivas ou irracionais.[18]

3 OS FUNDAMENTOS DO BITCOIN

Este item será um ponto importantíssimo para a sequência da pesquisa iniciada, visto que, aqui, realizar-se-á uma tarefa crucial para a correta compreensão da estrutura do Bitcoin, um conhecimento imprescindível para desenvolver futuras análises jurídicas na busca de uma regulamentação adequada. Então, o próximo passo é explanar, com certa profundidade, as principais questões técnicas que envolvem o Bitcoin. Seu modo de operação será analisado, assim como as benesses de sua utilização, o trabalho realizado pelos mineradores nos registros de transações e criação de novas unidades de BTC,[19] enfim, tudo que será necessário para auferir um conhecimento técnico sobre o tema. Feito este breve comentário, passe-se de imediato à análise dos referidos assuntos.

3.1 FORMA DE OPERAÇÃO

O protocolo Bitcoin, como já foi mencionado anteriormente, opera de um modo muito diferente das demais formas de transação monetária. Enquanto os sistemas bancários tradicionais realizam suas atividades partindo de um polo central,

[17] CAMPBELL-VERDUYN, Malcolm. **Bitcoin and Beyond**: Cryptocurrencies, Blockchains, and Global Governance. Routledge. 2018. s/p. Edição do Kindle.
[18] ANTONOPOULOS, Andreas. **Mastering Bitcoin**. O'Reilly Media Inc. 2. ed. s/p. Edição do Kindle.
[19] BTC é o cifrão do bitcoin.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

responsável por concentrar todos os dados e ordens da rede, o Bitcoin faz o exato oposto disto.[20] No Bitcoin, não existe servidor central.

Este *modus operandi* representa bem a filosofia que pauta a rede. A descentralização inerente ao sistema, com todos os usuários possuindo todos os dados simultaneamente, permite a exclusão da figura do terceiro intermediário de confiança. As transações em bitcoin[21] não são garantidas por uma autoridade central, mas, sim, pela criptografia da rede, que é responsável por garantir a correta realização de cada ordem e evitar eventuais fraudes em pagamentos.[22]

Todo este ecossistema se baseia na correta utilização de chaves públicas e privadas. É possível criar um exemplo, para facilitar a compreensão: imagine-se que A deseje transferir determinada quantia em dinheiro para B. O primeiro passo de ambos será criar uma carteira de bitcoin, algo que é geralmente feito através de corretoras, apesar de não ser uma prática muito recomendada. Assim que ambos concluírem este primeiro passo, eles terão uma carteira operacional, junto com uma chave pública e uma chave privada. Neste exemplo, B deverá repassar a sua chave pública para A, e, com isso, este poderá fazer a transferência do valor desejado diretamente para a carteira de B, que poderá confirmar a origem da transação usando a chave pública de A. Por sua vez, a rede somente aceitará a transação se esta estiver acompanhada da chave privada de A, uma garantia de que aquela ordem veio do legítimo proprietário da carteira.[23]

Por diversas vezes, o modo de operação do Bitcoin já foi comparado às transações entre duas pessoas que envolvam dinheiro vivo. Porém, diferentemente do que ocorre com estas últimas, as transações em bitcoin possuem registros dos detalhes importantes, incluindo o momento em que foi realizada, a quantia que foi transferida, o saldo remanescente em cada conta e, ainda, a chave pública das duas carteiras envolvidas.[24] Logo, é seguro dizer que as operações realizadas nesta rede não são tão anônimas quanto se faz crer, atualmente (mais detalhes no item 2.2.3).

[20] ULRICH, Fernando. **Bitcoin**: a moeda na era digital. São Paulo – SP: Instituto Ludwig von Mises Brasil. 2014. s/p. Edição do Kindle.
[21] A palavra “bitcoin”, em letras minúsculas, representa exclusivamente a moeda. Por outro lado, “Bitcoin”, com a primeira letra maiúscula, representa toda a rede de transações.
[22] NAKAMOTO, Satoshi. **Bitcoin**: A Peer-To-Peer Electronic Cash System. Bitcoin. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 17 nov 2019.
[23] ANTONOPOULOS, Andreas. **Mastering Bitcoin**. O’Reilly Media Inc. 2. ed. s/p. Edição do Kindle.
[24] GATES, Mark. **Blockchain**: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. Edição do Kindle. s/p.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

3.2 OS MINERADORES DA REDE BITCOIN

As operações descritas anteriormente só se mostram possíveis graças ao trabalho dos mineradores. A mineração é uma peça fundamental para o funcionamento da rede Bitcoin, e Satoshi Nakamoto estabeleceu um sistema de esforço e recompensa para estimular o seu bom funcionamento. Os mineradores são, em resumo, supercomputadores empenhados em realizar as transações que envolvam o Bitcoin, cumprindo as ordens enviadas pelos usuários, certificando-se de que não ocorra nenhum tipo de falha na rede. Para cada bloco registrado na *blockchain*, eles receberão uma determinada quantia em bitcoin, como recompensa pelos seus serviços.[25]

Aqui, é possível fazer um aparte para mencionar que o protocolo criado por Nakamoto garante que somente existirão 21 milhões de unidades de BTC, sendo impossível exceder este número.[26] Na rede Bitcoin, um novo bloco é registrado na *blockchain* a cada 10 minutos e, originalmente, 50 BTC eram minerados a cada bloco, com previsão de que este número fosse reduzido pela metade a cada 4 anos, no processo chamado de *halving*. Portanto, hoje existem 12,5 BTC sendo criados a cada 10 minutos, e este número será novamente reduzido em 2020.[27] A razão desta limitação imposta ao Bitcoin está nas origens de sua criação: deste modo, a Primeira Moeda[28] possui oferta limitada e não se sujeita ao vexame da hiperinflação, algo muito comum nas moedas fiduciárias estatais.

Não sem razão, há quem diga que esta escassez forçada equipara o Bitcoin ao ouro. Por sua própria natureza, o ouro possui propriedades intrínsecas que lhe garantem um certo valor mínimo – e é por esta mesma razão que ele já foi utilizado para garantir lastro às moedas tradicionais. Há uma verdade nesta comparação.

O processo de extração do ouro guarda várias semelhanças com a mineração prevista no protocolo de Satoshi Nakamoto. Enquanto os Estados podem oferecer sua moeda em quantias ilimitadas, o minério de ouro não pode ser criado por nenhum

[25] ANTONOPOULOS, Andreas. **Mastering Bitcoin**. O'Reilly Media Inc. 2. ed. s/p. Edição do Kindle.
[26] NAKAMOTO, Satoshi. **Bitcoin**: A Peer-To-Peer Electronic Cash System. Bitcoin. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 17 nov 2019.
[27] GATES, Mark. **Blockchain**: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. s/p. Edição do Kindle.
[28] "Primeira Moeda" é uma alcunha muito utilizada para se referir ao Bitcoin.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

governante. A quantidade existente não é definida pelo arbítrio ditatorial de algum estatista qualquer, mas, sim, pela própria natureza. Para que o ouro possa ser utilizado, primeiro deve ser extraído do lugar em que se encontra, um processo que acaba se tornando exponencialmente mais difícil, na medida em que todo o material existente vai sendo encontrado, obrigando os mineradores a "cavarem mais fundo" na procura de mais matéria-prima.[29]

É exatamente desta mesma maneira que ocorre a mineração de Bitcoin. Com o passar dos anos, está se tornando cada vez mais difícil minerar novas unidades. Por quê? Porque o protocolo exige, para a criação de um novo bloco de transações, que seja resolvido um problema matemático, cuja complexidade é determinada de acordo com a capacidade computacional da rede e aumenta de modo exponencial, na medida em que o número de 21 milhões de BTC vai se aproximando.[30] Encontrar a resposta deste problema é o único meio de registrar um novo bloco de transações.[31] A dificuldade de resolução também é constantemente atualizada pela rede, para garantir que os computadores envolvidos levem aproximadamente 10 minutos para soluciona-lo, que é o tempo estipulado por Nakamoto para a inclusão de um novo bloco na *blockchain*.[32]

Em resumo, todo o protocolo depende da boa atuação dos mineradores, diretamente responsáveis por executar as ordens dos usuários. Apesar disto, e este é um ponto importante, esta qualidade não os dota de nenhum poder em relação aos usuários comuns. Os esforços do criador do sistema proveram resultados efetivos neste quesito. Os mineradores não conseguirão fraudar a rede e realizar transações viciadas de maneira tão fácil, embora, tecnicamente, seja possível, mas muito improvável de ocorrer com o Bitcoin. Explica-se.

Falando em termos financeiros, o Bitcoin domina 66% do mercado das criptomoedas, que é estimado em 191 bilhões de dólares.[33] Em uma pesquisa rápida,

[29] ULRICH, Fernando. **Bitcoin**: a moeda na era digital. São Paulo – SP: Instituto Ludwig von Mises Brasil. 2014. s/p. Edição do Kindle.
[30] GATES, Mark. **Blockchain**: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. s/p. Edição do Kindle.
[31] Detalhes maiores sobre as questões técnicas que envolvem a *blockchain* estão no item 2.3.
[32] GATES, Mark. **Blockchain**: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. s/p. Edição do Kindle.
[33] **COINMARKETCAP**. Disponível em: <https://coinmarketcap.com/charts/>. Acesso em: 18 nov 2019.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

verifica-se que o número de criptomoedas existentes supera a marca de cinco mil.[34] Com isso, é possível atestar, sem qualquer grau de dúvida, a soberania intocável do Bitcoin no setor. Tanto é verdade, que todas as demais criptomoedas, enquanto um coletivo único, recebem o popular apelido de *altcoins*[35]. Tratando de cotações, o Bitcoin está estimado, atualmente, em 1 BTC = R$ 29.000,00[36], enquanto a segunda maior criptomoeda, o Ethereum, possui cotação momentânea de 1 ETH = R$ 601,00[37], com ambas as cotações retiradas no dia 24/11/2019.

Por estas razões, afirma-se: a rede Bitcoin é muito mais desenvolvida, muito mais povoada e, portanto, é infinitamente mais segura, se comparada às demais criptomoedas. E isto afeta diretamente o poder dos mineradores do sistema. Se houvessem poucos mineradores, seria crível que um grupo pequeno, unindo forças, conseguisse controlar mais da metade do poder computacional da rede, sendo capaz de realizar transações fraudulentas. Esta técnica, na boa linguagem computacional, leva o nome de “ataque de 51%”.[38]

Teoricamente, a rede Bitcoin também está sujeita a este perigo. Entretanto, considerando o seu elevado número de mineradores e usuários, o poder computacional está muito distribuído, o que tornaria inviável, na prática, reunir 51% sob a mesma finalidade fraudulenta.[39]

3.3 O “ANONIMATO” GARANTIDO AOS USUÁRIOS NA REDE BITCOIN

Outro item de suma relevância que precisa ser debatido é o suposto anonimato que as transações em Bitcoin garantem aos seus usuários. Muito se fala sobre a relação deste criptoativo com a criminalidade, não sendo nada incomum vê-lo associado com crimes financeiros e tráfico de entorpecentes. Todavia, o cenário verdadeiro não é exatamente este.

---

[34] **LIVECOINS**. Descubra quantas criptomoedas existem hoje. Disponível em: <https://livecoins.com.br/mercado-de-criptomoedas-ja-soma-mais-de-5000-altcoins/>. Acesso em: 18 nov 2019.
[35] Abreviação de “*alternative coins*”, que significa, em resumo, “qualquer criptomoeda além do Bitcoin”.
[36] **MERCADO BITCOIN**. Disponível em: <https://www.mercadobitcoin.com.br/negociacoes/bitcoin>. Acesso em: 24 nov 2019.
[37] **MERCADO BITCOIN**. Disponível em: <https://www.mercadobitcoin.com.br/negociacoes/ethereum>. Acesso em: 24 nov 2019.
[38] Mais detalhes sobre a influência dos mineradores estão no item 2.3.
[39] ANTONOPOULOS, Andreas. **Mastering Bitcoin**. O’Reilly Media Inc. 2. ed. s/p. Edição do Kindle.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

Como já foi explicado nos parágrafos anteriores (e será retomado, com mais profundidade, no item 2.3), todas as transações realizadas na rede Bitcoin são públicas, acessíveis para qualquer pessoa. Quando uma carteira de bitcoin é criada, todos os participantes da rede conseguirão ver exatamente a quantia que esta carteira possui, e este, por exemplo, é um dado que nunca seria fornecido por uma instituição bancária tradicional.[40]

É sabido que a *blockchain* armazena todas as informações relativas às transações já realizadas, incluindo o endereço (leia-se: chave pública) das carteiras de Bitcoin envolvidas. A título de ilustração, para que o leitor compreenda melhor este ponto, transcreve-se aqui um endereço público, obtido através da corretora Mercado Bitcoin, de uma carteira de propriedade do próprio autor deste artigo: "1DXed1ZNzzUZQQNfvcyWKQore8GgmSHocF". É deste modo que tais dados são apresentados na *blockchain*. Em um primeiro momento, não há nenhuma identificação das partes envolvidas, mas esta ocultação está longe de ser absoluta.

Foi com este problema em mente que Elli Androulaki, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer e Srdjan Capkun realizaram um estudo que buscou atestar, em grau científico elevado, a real extensão do anonimato existente na rede Bitcoin. Para atingir este fim, os autores simularam o funcionamento do protocolo da Primeira Moeda em uma escala reduzida, dentro de uma universidade. Ao criarem um algoritmo que avaliava o comportamento das pessoas envolvidas na rede, eles buscavam analisar se seria possível, com base nas próprias ações dos usuários, descobrir as suas identidades. Em um *paper* de 18 páginas, inteira e gratuitamente disponível na internet, a conclusão dos autores foi a seguinte:

> *Our findings show that the current measures adopted by Bitcoin are not enough to protect the privacy of users if Bitcoin were to be used as a digital currency in a university setting. […]. Our results show that if Bitcoin is used as a digital currency to support the daily transactions of users in a typical university environment, then behavior-based clustering techniques can unveil, to a large extent, the profiles of 40% of Bitcoin users, even if these users try to enhance their privacy by manually creating new addresses*.[41] [42]

[40] ANTONOPOULOS, Andreas. **Mastering Bitcoin**. O'Reilly Media Inc. 2. ed. s/p. Edição do Kindle.
[41] ANDROULAKI, Elli; et al. **Evaluating User Privacy on Bitcoin**. Disponível em: <https://eprint.iacr.org/2012/596.pdf>. Acesso em: 18 nov 2019.
[42] Nossas descobertas mostram que as medidas atualmente adotadas pelo Bitcoin não são suficientes para proteger a privacidade dos usuários, se fosse utilizado como uma moeda digital em uma universidade. Nossos resultados mostram que, se o Bitcoin for utilizado como moeda digital nas transações de usuários em um ambiente universitário comum, então algumas técnicas de agrupamento baseadas em padrões comportamentais poderiam revelar os perfis de até 40% dos usuários, mesmo

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

A conclusão atingida naquele estudo mostra que, ao contrário do que é costumeiramente falado, o Bitcoin não garante o anonimato de seus usuários. Tecnicamente falando, seria mais correto dizer que ele garante, em verdade, uma discrição para as partes envolvidas, ao transformar seus nomes em endereços eletrônicos. Descobrir os nomes, a partir dos endereços eletrônicos, seria um trabalho de engenharia reversa relativamente complicado, mas perfeitamente possível, na maioria dos casos.[43]

Esta privacidade é aumentada se o próprio usuário tomar as precauções necessárias para se manter anônimo, mas, muitas vezes, não é o que de fato acontece. O ato de transacionar quantias em bitcoin diretamente na rede *blockchain* pode parecer demasiadamente arriscado para a maioria das pessoas, que acabam preferindo realizar suas operações através de um intermediário, em regra, uma corretora. Mark Gates menciona este quadro do seguinte modo[44]:

> *The process of connecting to blockchain networks, sending transactions, setting up the private keys is complicated and risky for many people. Many people prefer to give access to their private keys to third-party intermediaries with web-wallets or similar software, which eliminates another main benefit of blockchain networks*.[45]

Não deixa de ser um paradoxo bastante irônico. Mas, ainda assim, é essencial para explicar adequadamente toda a questão do anonimato. Ao se cadastrar em alguma corretora, que atuará como intermediária, o usuário será obrigado a fornecer uma quantidade inconfortavelmente alta de informações e documentos pessoais. Deste modo, não há como manter o seu anonimato na rede, pois ele já terá fornecido seus próprios dados para um terceiro, que poderá revela-los, por exemplo, em caso de uma ordem judicial que assim ordene.

que estes usuários tentem aumentar sua privacidade ao criar novos endereços [de carteiras] manualmente. Tradução nossa.

[43] ANTONOPOULOS, Andreas. **Mastering Bitcoin**. O'Reilly Media Inc. 2. ed. s/p. Edição do Kindle.

[44] GATES, Mark. **Blockchain**: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. s/p. Edição do Kindle.

[45] "O processo de se conectar na rede blockchain, enviar transações, lidar com chaves privadas, tudo isto pode ser muito complicado e arriscado para várias pessoas. Então, as pessoas preferem dar acesso às suas chaves privadas para terceiros intermediários em carteiras virtuais, o que elimina outro grande benefício da rede blockchain." Tradução nossa.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

4 O FUNCIONAMENTO DA REDE *BLOCKCHAIN*

Finalmente, é chegado o momento de descrever, com mais detalhes, a estrutura de um dos aspectos mais importantes de toda a rede Bitcoin, aquela que é considerada a sua tecnologia mais revolucionária e que, para alguns, é mais relevante que a própria criptomoeda.

Nos últimos anos, é possível perceber uma aceitação cada vez maior da tecnologia *blockchain* no mercado financeiro estatal. De certo modo, pode-se dizer que ela se mostrou imune aos receios e preconceitos enfrentados pelos ativos criptografados. A título de exemplo: no ano passado, durante o 11º Fórum de Tecnologia da Informação, foi anunciado o projeto "Sistema Financeiro Digital" (SFD), fruto de uma parceria entre várias instituições financeiras, como Banco do Brasil, Banrisul, Caixa Econômica Federal, Santander e Sicoob.[46]

O objetivo do SFD, que ainda não está disponível para o público, é oferecer uma alternativa mais moderna ao DOC e ao TED, utilizando a tecnologia *blockchain* para realizar transações. A sua grande vantagem, em relação aos concorrentes citados, é a eliminação do intermediário (a câmara de transferências da Febraban), o que acaba resultando em maior velocidade de transação, abrindo a possibilidade de transferências de dinheiro de modo quase instantâneo, mesmo em dias não-úteis.[47]

Deste modo, não é nem um pouco irracional afirmar que a *blockchain* está superando o Bitcoin (ao menos em termos de aceitação). Resta agora explicar ao leitor o motivo de todo este entusiasmo da comunidade financeira em relação a esta nova tecnologia. E a excitação em relação ao seu potencial, sabe-se, não é pouca:

> *Blockchain technology has been called the greatest innovation since the internet. Proponents of the technology claim it will disrupt every industry that exists today and impact the lives of almost everybody on the planet within a*

[46] ROSA, Natalie. **Canaltech**. Banrisul, BB, Caixa, Sicoob e Santander se unem em projeto de blockchain. Disponível em: <https://canaltech.com.br/blockchain/banrisul-bb-caixa-sicoob-e-santander-se-unem-em-projeto-de-blockchain-114768/>. Acesso em: 24 nov 2019.

[47] **CONTA-CORRENTE**. Bancos anunciam Sistema Financeiro Digital para transferências. Disponível em: <https://www.conta-corrente.com/transferencia/sfd/bancos-anunciam-sistema-financeiro-digital-para-transferencias/>. Acesso em: 24 nov 2019.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

few decades. Is blockchain technology one of the greatest technological revolutions in history or is it just hype?[48] [49]

A proposta central desta sessão da monografia é construir algo próximo de uma resposta para a pergunta transcrita acima. Para tanto, dizem que o melhor jeito de atingir o fim pretendido é começar...bom, do começo.

A grande maioria das obras existentes sobre o assunto usam, como ponto de partida, o *paper* de Satoshi Nakamoto, que originou o Bitcoin, para explicar a *blockchain*. Apesar de esta colocação estar fundamentalmente correta, algumas observações devem ser feitas: como será relatado mais adiante, a função principal desta tecnologia é armazenar e transmitir dados de maneira mais eficiente, o que, em verdade, é uma preocupação constante da humanidade, que busca seguidamente se aperfeiçoar e desenvolver métodos mais seguros de realizar tais operações. Logo, não há como estabelecer um termo inicial para isso.

Esta é uma história que se confunde com as próprias origens da criptografia, começando com os códigos criptografados manualmente e chegando, finalmente, aos protocolos de assinatura e certificado digital. Portanto, o que Nakamoto apresentou ao mundo em 2008, embora seja brilhante, somente foi possível pelo estado avançado da internet e da criptografia. Sem estas tecnologias, o Bitcoin não teria existido. Entretanto, para não alongar demasiadamente as questões históricas, considerar-se-á, como ponto de partida, o *paper* de 2008.

Nos dias atuais, a *blockchain* já possui identidade própria e é conhecida de modo independente, sem estar atrelada ao Bitcoin. Como foi dito acima, a intenção por trás desta tecnologia é realizar armazenamentos e transferências de dados de modo mais seguro, eficiente e com menos riscos para os usuários. Entretanto, considerar a *blockchain* como apenas um "banco de dados" seria de um reducionismo extremo, de proporções iguais à frase "o e-mail é um meio de comunicação, tal como a carta".[50]

---

[48] "A tecnologia *Blockchain* é considerada a maior inovação [da humanidade] desde a internet. Entusiastas desta tecnologia dizem que ela irá romper todas as indústrias existentes hoje e impactará nas vidas de quase todas as pessoas no planeta em poucas décadas. A *blockchain* é realmente uma das maiores revoluções tecnológicas da história ou é apenas um exagero?" Tradução nossa.

[49] GATES, Mark. **Blockchain**: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. s/p. Edição do Kindle.

[50] CHIU, Jonathan; KOEPPL, Thorsten V. **The Economics of Cryptocurrencies – Bitcoin and Beyond**. BIS. Disponível em: <https://www.bis.org/events/eopix_1810/chiu_paper.pdf>. Acesso em: 18 nov 2019.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

Para explicar o seu funcionamento, tomar-se-á um exemplo prático: uma biblioteca. Imagine-se uma biblioteca tradicional, com um catálogo de livros disponíveis nas prateleiras e livros que se encontram emprestados para alguém, os respectivos prazos para a devolução, enfim, todas as informações armazenadas em um computador central, controlado pelo administrador da biblioteca.

Aplicando a *blockchain* neste cenário, a mudança de paradigma seria enorme. Não haveria mais um servidor central, dono de todas as informações relativas aos livros do catálogo daquela biblioteca, mas, sim, todas as pessoas envolvidas teriam acesso permanente ao histórico de empréstimos, saberiam quais livros estão disponíveis e quem tomou emprestado um determinado livro.[51] Logo, tudo o que ocorresse na biblioteca seria imediatamente notado por todos. O controle das ações seria dividido, e é precisamente por esta razão que ninguém teria o controle de coisa alguma.[52]

Com toda a construção realizada até este momento, o leitor já deve ter percebido que a essência e a ideologia da rede Bitcoin se baseiam em um fator, de importância imensurável: a confiança. A Primeira Moeda surgiu como uma alternativa aos falidos sistemas estatais, profundamente desprovidos da confiança dos cidadãos, que perderam a fé nas teorias econômicas mirabolantes dos sistemas financeiros centralizados.

Então, o objetivo buscado pelo Bitcoin e pela *blockchain* foi a criação de um modo de operação que garantisse a confiança do usuário, para atrai-lo. Ao invés de seguir os sistemas centralizados tradicionais, a *blockchain* oferece uma alternativa, em que as transações são confirmadas, ou negadas, pelo consenso dos usuários da rede.[53]

No exemplo da “biblioteca compartilhada”, imagine que determinada pessoa realize o empréstimo de um livro, pague por ele e, no espaço de tempo entre a confirmação da transação e a sua inclusão na *blockchain* (lembre-se: um novo bloco leva 10 minutos para ser adicionado na rede pelos mineradores), tome emprestado algum outro livro, usando a mesma quantia em dinheiro. No momento em que estas

[51] CAMPBELL-VERDUYN, Malcolm. **Bitcoin and Beyond**: Cryptocurrencies, Blockchains, and Global Governance. Routledge. 2018. s/p. Edição do Kindle.
[52] GATES, Mark. **Blockchain**: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. s/p. Edição do Kindle.
[53] NAKAMOTO, Satoshi. **Bitcoin**: A Peer-To-Peer Electronic Cash System. Bitcoin. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 17 nov 2019.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

duas transações forem verificadas, a rede perceberá que aquela pessoa não possui saldo suficiente para realizar as duas ações e, portanto, o segundo empréstimo será cancelado. Assim, Nakamoto conseguiu o impossível: criar um sistema distribuído, sem autoridades centrais, que se mostrou capaz de resolver o problema do gasto duplo.[54]

Isto só se torna possível graças ao mecanismo de consenso. Se mais de 50% da rede concordar que uma transação é inválida, ela não será adicionada na *blockchain*. Como já foi explicado no item 2.2.2, o "ataque de 51%" pode ocorrer em toda e qualquer *blockchain* existente, porém, quanto mais usuários estiverem envolvidos, mais esforço será necessário para fraudar o sistema.[55]

De forma básica, assim se dá o funcionamento da tecnologia que norteia este capítulo. Com esta primeira explicação feita, é momento de se aprofundar um pouco nos benefícios e nas desvantagens inerentes ao objeto.

Entre os pontos mais interessantes da *blockchain*, destaca-se a transparência que seu protocolo garante. Com uma operação descentralizada, todos os usuários estão aptos a participar mais ativamente daquilo que acontece na rede. O consenso, definido como a aceitação geral de um bloco de transações, é o que permite o bom funcionamento do sistema. Comparado aos sistemas tradicionais, em que todo o poder decisório está nas mãos de autoridades (geralmente despóticas), esta é uma excelente mudança.[56]

No mesmo sentido, a segurança da rede é outro item que merece destaque absoluto. Quando alguma transação é criada, alterá-la é uma tarefa hercúlea. Atualmente, após um bloco ser finalizado, ele só poderá ser alterado se não houver outros seis blocos posteriores àquele. Sabe-se que o tempo de criação de um novo bloco, no caso do Bitcoin, é de dez minutos, portanto, uma transação inserida na rede neste exato momento, poderá ser alterada, com extrema dificuldade, no prazo máximo

[54] GATES, Mark. **Blockchain**: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. s/p. Edição do Kindle.
[55] CHIU, Jonathan; KOEPPL, Thorsten V. **The Economics of Cryptocurrencies – Bitcoin and Beyond**. BIS. Disponível em: <https://www.bis.org/events/eopix_1810/chiu_paper.pdf>. Acesso em: 24 nov 2019.
[56] ULRICH, Fernando. **Bitcoin**: a moeda na era digital. São Paulo – SP: Instituto Ludwig von Mises Brasil. 2014. s/p. Edição do Kindle.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

de uma hora, pois o poder computacional exigido para alterar mais de seis blocos torna a operação inviável.[57]

Imprescindível destacar que não é possível alterar individualmente os blocos registrados na rede, pois cada um deles contém uma assinatura digital que o conecta ao bloco anterior e ao posterior.[58] Logo, uma pessoa que tentasse fraudar o sistema em benefício próprio, teria de desfazer todos os blocos registrados, até atingir aquele que efetivamente deverá ser cancelado, e toda esta operação seria extremamente custosa.[59]

Dito isto, existem certos aspectos negativos, igualmente importantes, que devem ser considerados. Enquanto a transparência da rede se mostra positiva de várias maneiras, ela também pode representar uma patente falta de privacidade. Imagine que você entre em alguma loja e queira pagar algum produto através de um sistema de *blockchain*. O vendedor da loja, com o endereço da sua carteira, saberia imediatamente qual o saldo atual que você possui, bem como o extrato completo de transações realizadas naquela mesma carteira.[60]

Esta falta de privacidade pode assustar e intimidar várias pessoas, em uma primeira vista. Entretanto, outra questão talvez seja ainda mais problemática: a segurança da *blockchain*, por ser tão meticulosa e bem-acabada, pode se revelar um problema.

Quando uma pessoa realiza um cadastro em algum banco, por exemplo, lhe é dada a opção de criar uma senha pessoal, que será utilizada para acessar a rede. Se, por qualquer motivo, esta senha for esquecida pelo usuário, basta que ele entre em contato com o banco para recuperar o acesso à sua conta. Na *blockchain*, isto não seria possível.

Como não há nenhuma entidade central, a consequência disto é que ninguém mais possui acesso às carteiras privadas dos usuários. Logo, se o proprietário não mais se recordar da sua senha, a consequência será a perda total do acesso e a impossibilidade de movimentar aquela quantia. Ironicamente, como os dados da

[57] CAMPBELL-VERDUYN, Malcolm. **Bitcoin and Beyond**: Cryptocurrencies, Blockchains, and Global Governance. Routledge. 2018. s/p. Edição do Kindle.
[58] NAKAMOTO, Satoshi. **Bitcoin**: A Peer-To-Peer Electronic Cash System. Bitcoin. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 17 nov 2019.
[59] GATES, Mark. **Blockchain**: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. s/p. Edição do Kindle.
[60] CAMPBELL-VERDUYN, Malcolm. **Bitcoin and Beyond**: Cryptocurrencies, Blockchains, and Global Governance. Routledge. 2018. s/p. Edição do Kindle.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

blockchain são públicos, ele poderá verificar qual o saldo atualizado da sua carteira, mas não terá acesso ao dinheiro.[61]

Apesar de todos estes contratempos citados, o "balanço geral" apresentado ainda se mostra favorável à *blockchain*. Desde a sua criação, seus métodos se encontram em constante evolução e atualização, o que resulta em uma confiança já consolidada nas suas operações. Eventualmente, o sistema financeiro tradicional deve acabar adotando o seu protocolo, mesmo que não utilizem o Bitcoin, e será interessante acompanhar se a *blockchain* se mostrará suficientemente eficiente para ser usada em operações de escalas maiores.

5 CONCLUSÃO

Levando em conta a complexidade do tema abordado, é óbvio que este diminuto número de páginas não se prestaria a explicar todas as minúcias do objeto apresentado. Entretanto, o nível de detalhes apresentado aqui foi denso o suficiente para preparar o leitor (e até o autor) para eventuais diligências futuras que podem ser realizadas no universo jurídico, buscando encontrar (ou criar) uma regulamentação adequada para o Bitcoin. Propor soluções jurídicas para esta problemática só seria possível após enfrentar, com certa profundidade, as questões técnicas do objeto.

Através de uma recapitulação que iniciou na crise financeira de 2008, buscou-se trazer ao leitor uma compreensão maior acerca da filosofia que envolve a ideia de uma moeda independente de qualquer autoridade estatal. Mais do que uma simples moeda e/ou forma de pagamento, o Bitcoin representa um protesto contra o despotismo estatal.

A sua mera existência é capaz de romper com conceitos há muito estabelecidos, ao mesmo tempo em que oferece tecnologias inovadoras e únicas, revelando novos meios de armazenar e transferir capital e informações. Mesmo uma década após a sua criação, ainda não há um consenso sobre a melhor maneira de tirar proveito das suas benesses, mas, de toda sorte, o Bitcoin apresentou um caminho que não admite volta.

REFERÊNCIAS

[61] GATES, Mark. **Blockchain**: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. s/p. Edição do Kindle.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

AMADEO, Kimberly. **What Was the Fannie Mae and Freddie Mac Bailout?** The Balance. Disponível em: <https://www.thebalance.com/what-was-the-fannie-mae-and-freddie-mac-bailout-3305658>. Acesso em: 11 de nov 2019.

ANDROULAKI, Elli; et al. **Evaluating User Privacy on Bitcoin**. Disponível em: <https://eprint.iacr.org/2012/596.pdf>. Acesso em: 18 nov 2019.

ANTONOPOULOS, Andreas. **Mastering Bitcoin**. O'Reilly Media Inc. 2. ed. s/p. Edição do Kindle

BBC News. **Northern Rock gets bank bail out**. Disponível em: <http://news.bbc.co.uk/2/hi/business/6994099.stm>. Acesso em: 11 de nov 2019.

BERNANKE, Ben S. **The Community Reinvestment Act:** Its Evolution and New Challenges. Federal Reserve System. Disponível em: <https://www.federalreserve.gov/newsevents/speech/Bernanke20070330a.htm>. Acesso em: 09 nov 2019.

BOOTH, Philip. **Verdict on The Crash**: Causes and Policy Implications. The Institute of Economic Affairs: Great Britain, 2009.

CAMPBELL-VERDUYN, Malcolm. **Bitcoin and Beyond**: Cryptocurrencies, Blockchains, and Global Governance. Routledge. 2018. s/p. Edição do Kindle

CHIU, Jonathan; KOEPPL, Thorsten V. **The Economics of Cryptocurrencies – Bitcoin and Beyond**. BIS. Disponível em: <https://www.bis.org/events/eopix_1810/chiu_paper.pdf>. Acesso em: 24 nov 2019.

COINMARKETCAP. Disponível em: <https://coinmarketcap.com/charts/>. Acesso em: 18 nov 2019.

CONTA-CORRENTE. Bancos anunciam Sistema Financeiro Digital para transferências. Disponível em: <https://www.conta-corrente.com/transferencia/sfd/bancos-anunciam-sistema-financeiro-digital-para-transferencias/>. Acesso em: 24 nov 2019.

GATES, Mark. **Blockchain**: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. s/p. Edição do Kindle.

LIEBOWITZ, Stan J. **Anatomy of a Train Wreck**: Causes of the Mortgage Meltdown. Independent Policy Report. Disponível em: <http://www.independent.org/pdf/policy_reports/2008-10-03-trainwreck.pdf>. Acesso em: 11 nov 2019.

_____. **The Real Scandal**. New York Post. Disponível em: <https://nypost.com/2008/02/05/the-real-scandal/>. Acesso em: 09 nov 2019.

ISSN 2525-4243 / Nº 4 / Ano 2019 / p. 132-152

LIVECOINS. Descubra quantas criptomoedas existem hoje. Disponível em: <https://livecoins.com.br/mercado-de-criptomoedas-ja-soma-mais-de-5000-altcoins/>. Acesso em: 18 nov 2019.

MERCADO BITCOIN. Disponível em: <https://www.mercadobitcoin.com.br/negociacoes/bitcoin>. Acesso em: 24 nov 2019.

_____. Disponível em: <https://www.mercadobitcoin.com.br/negociacoes/ethereum>. Acesso em: 24 nov 2019.

NAKAMOTO, Satoshi. **Bitcoin**: A Peer-To-Peer Electronic Cash System. Bitcoin. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 17 nov 2019.

ROSA, Natalie. **Canaltech**. Banrisul, BB, Caixa, Sicoob e Santander se unem em projeto de blockchain. Disponível em: <https://canaltech.com.br/blockchain/banrisul-bb-caixa-sicoob-e-santander-se-unem-em-projeto-de-blockchain-114768/>. Acesso em: 24 nov 2019.

THE GUARDIAN. **Lehman Brothers goes bankrupt, 15 September**. Disponível em: <https://www.theguardian.com/world/2008/dec/28/lehman-brothers-bankrupt-eyewitness-account>. Acesso em: 11 de nov 2019.

ULRICH, Fernando. **Bitcoin**: a moeda na era digital. São Paulo – SP: Instituto Ludwig von Mises Brasil. 2014. s/p. Edição do Kindle.