



UNIVERSIDADE FEDERAL DO CEARÁ
FACULDADE DE ECONOMIA, ADMINISTRAÇÃO, ATUÁRIA E CONTÁBEIS
DEPARTAMENTO DE TEORIA ECONÔMICA
PROGRAMA DE GRADUAÇÃO EM CIÊNCIAS ECONÔMICAS

DANIEL AGUIAR DE SOUSA

BITCOIN: PERSPECTIVAS FUTURAS DE USO

FORTALEZA

2021

DANIEL AGUIAR DE SOUSA

BITCOIN: PERSPECTIVAS FUTURAS DE USO

Monografia apresentada à Coordenação do Curso de Graduação em Ciências Econômicas da Universidade Federal do Ceará, como requisito parcial para obtenção do grau de Bacharel em Ciências Econômicas.

Orientador: Prof. Dr. Jair do Amaral Filho.

FORTALEZA

2021

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

A228b Aguiar de Sousa, Daniel.

Bitcoin : perspectivas futuras de uso / Daniel Aguiar de Sousa. – 2021.
58 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Economia, Administração, Atuária e Contabilidade, Curso de Ciências Econômicas, Fortaleza, 2021.

Orientação: Prof. Dr. Jair do Amaral Filho.

1. Bitcoin. 2. Blockchain. 3. Criptomoedas. 4. Economia Monetária. I. Título.

CDD 330

DANIEL AGUIAR DE SOUSA

BITCOIN: PERSPECTIVAS FUTURAS DE USO

Monografia apresentada à Coordenação do Curso de Graduação em Ciências Econômicas da Universidade Federal do Ceará, como requisito parcial para obtenção do grau de Bacharel em Ciências Econômicas.

Aprovada em: ___/___/_____.

BANCA EXAMINADORA

Prof. Dr. Jair do Amaral Filho (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Marcelo de Castro Callado
Universidade Federal do Ceará (UFC)

Profa. Dra. Maria Cristina Pereira de Melo
Universidade Federal do Ceará (UFC)

À minha mãe, Germana.

AGRADECIMENTOS

Agradeço ao meu orientador, professor Jair do Amaral Filho, pelos conselhos. Ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), pela bolsa na pesquisa do professor Jair do Amaral Filho. Agradeço também aos professores Marcelo de Castro Callado e Maria Cristina Pereira de Melo, pela atenção aos detalhes e pelas sugestões de melhorias para o trabalho. À minha mãe e à minha tia, pelo afeto incondicional. E aos grandes pensadores da Grécia Antiga, por me permitirem sonhar.

RESUMO

O objetivo deste trabalho é, após uma breve introdução da história e do funcionamento, criar perspectivas futuras de uso do Bitcoin. Para isso, serão utilizadas deduções a partir de conceitos gerais de teoria econômica, comparação com outros ativos econômicos e possíveis acontecimentos lógicos relativos (como uma intervenção governamental no setor). A partir da análise feita e caso os fundamentos permaneçam, podemos não ter certeza do que ocorrerá ao Bitcoin, mas, dadas suas características específicas e similaridades ao ouro, podemos inferir que ele poderá ser usado (em parte já é) como reserva de valor e como parte de investimentos em um portfólio bem administrado; e que possui muitos entraves para ser usado como meio de troca, mas estas adversidades podem ser superadas no futuro.

Palavras-chave: Bitcoin, Blockchain, Criptomoedas, Economia Monetária.

ABSTRACT

The objective of this work is, after a brief introduction of its history and functioning, to create future perspectives on the use of Bitcoin. For this, deductions will be used from general concepts of economic theory, comparison with other economic assets and possible relative logical events (such as government intervention in the sector). From the analysis made and if the fundamentals remain, we may not be sure what will happen to Bitcoin, but, given its specific characteristics and similarities to gold, we can infer that it can be used (in part it already is) as a store of value and as part of investments in a well-managed portfolio; and that it has many obstacles to be used as a mean of exchange, but these adversities can be overcome in the future.

Keywords: Bitcoin, Blockchain, Cryptocurrencies, Monetary Economics.

LISTA DE FIGURAS

Figura 1 – Modelos de privacidade nas transações	29
Figura 2 – Processo simplificado de transação e validação no <i>blockchain</i>	31
Figura 3 – Resumo de diferenças e similaridades entre ouro e bitcoin	46

LISTA DE GRÁFICOS

Gráfico 1 – Preço da unidade de bitcoin (BTC) em dólar (\$) de 30/09/2013 até 23/08/2021	24
Gráfico 2 – Volatilidade do preço do bitcoin (BTC) em dólar (\$) de 31/07/2016 até 30/06/2021 usando média móvel de 10 dias	24
Gráfico 3 – Valor de mercado do Bitcoin em dólar (\$) de abril de 2013 até agosto de 2021	25
Gráfico 4 – Transações de compra e venda relacionadas ao bitcoin (BTC) de acordo com o rank de moedas nos últimos 30 dias a partir de 23 de agosto de 2021; nos anos anteriores o domínio era da moeda chinesa renminbi (USD: dólar, EUR: euro, PLN: zloty polonês, AUD: dólar australiano, JPY: iene japonês, BRL: real brasileiro)	25
Gráfico 5 – Número total de transações confirmadas por dia	26
Gráfico 6 – Oferta total de bitcoins (curva escura e indicadores na vertical da esquerda) e taxa de crescimento da oferta de bitcoins (curva cinza e indicadores na vertical da direita) ao longo do tempo	35
Gráfico 7 – Recompensa por bloco x Recompensa por transações (considerando o incentivo a minerar) ao longo do tempo	36
Gráfico 8 – Consumo anualizado de energia do Bitcoin em Terawatt-hora (TWh)	40
Gráfico 9 – Divisão dos tipos de usuário de criptoativos em 2020 (Retail: Varejo (usuários comuns); Business and Institutional clientes: Negócios e Clientes institucionais; Unknown: Desconhecido)	50

LISTA DE TABELAS

Tabela 1 – Preço de 1 bitcoin (BTC) e valor de mercado da rede Bitcoin em dólar (\$) em 1 janeiro de 2014 a 2021	23
Tabela 2 – Componentes do Bitcoin	33

LISTA DE ABREVIATURAS E SIGLAS

B	Bilhão (ões)
BCB	Banco Central do Brasil
BTC	Bitcoin
CBDC	<i>Central Bank Digital Currency</i>
DeFi	<i>Decentralized Finance</i>
ETF	<i>Exchange-traded fund</i>
ETH	Ethereum
FED	Instituto Brasileiro de Geografia e Estatística
FTSE	<i>Financial Times Stock Exchange</i>
NFT	<i>Non-fungible token</i>
M	Milhão (ões)
PoS	<i>Proof-of-Stake</i>
PoW	<i>Proof-of-Work</i>
T	Trilhão (ões)
TWh	Terawatt-hora

LISTA DE SÍMBOLOS

\$	Dólar
¥	Iene
%	Porcentagem

SUMÁRIO

1	INTRODUÇÃO	16
2	BREVE HISTÓRIA	18
2.1	2009	19
2.2	2010-2013	20
2.3	2014-2017	21
2.4	2018-2021	22
2.5	Dados da rede Bitcoin ao longo do tempo	23
3	ASPECTOS TEÓRICOS E TÉCNICOS	27
3.1	Teoria Antecedente	28
3.2	O Sistema	29
3.3	Incentivos	34
4	PERSPECTIVAS FUTURAS DE USO	38
4.1	Principais adversidades ao Sistema Bitcoin	38
4.1.1	<i>Complexidade Técnica</i>	39
4.1.2	<i>Energia</i>	39
4.1.3	<i>Risco de brechas no Protocolo</i>	41
4.1.4	<i>Uso criminoso</i>	42
4.1.5	<i>Proibição e Regulação</i>	43
4.1.6	<i>Competição de outros criptoativos</i>	43
4.1.7	<i>Políticas Econômicas</i>	44
4.2	Reserva de Valor	45
4.3	Ativo pertencente a um Portfólio de Investimentos	47
4.4	Meio de Troca	50
5	CONCLUSÃO	53
	REFERÊNCIAS	56

1 INTRODUÇÃO

A moeda é um dos maiores avanços da humanidade, o meio de troca por excelência. A partir dela, nós não temos mais o problema de dupla coincidência de desejo para que transações sejam possíveis, também podemos nos especializar em nossas atividades de trabalho. O padeiro pode focar em produzir pão e fazer trocas com um pescador, mesmo que esse não queira peixe; tudo graças ao meio de troca. Podemos afirmar, sem dúvidas, que a moeda é um dos fulcros da civilização contemporânea, e que nos permite ter uma vivência, apesar de imperfeita, muito melhor do que a de nossos antepassados históricos.

[...] o dinheiro é a raiz da maior parte do progresso. [...] a ascensão do dinheiro tem sido essencial para a ascensão do homem. Longe de ser o trabalho de meros exploradores cuja intenção é sugar o sangue da vida das famílias endividadas ou jogar e especular com as poupanças de viúvas e órfãos, a inovação financeira tem sido um fator indispensável no avanço do homem, a partir da subsistência miserável aos picos vertiginosos da prosperidade material que tantas pessoas conhecem atualmente. (FERGUSON, 2009, p. 9)

Para ser moeda, algumas características devem ser obedecidas, como meio de troca, unidade de conta e reserva de valor, algo que é observado através da história humana. De forma mais completa, as principais características que fundamentam um bom meio de troca são: (1) utilidade e valor, (2) portabilidade, (3) indestrutibilidade, (4) homogeneidade, (5) divisibilidade, (6) estabilidade de valor, e (7) reconhecimento (JEVONS, 1875).

O avanço tecnológico nos proporcionou, durante a história, criações desde a roda à internet. Uma das mais novas tecnologias foi a das criptomoedas, com destaque para o Bitcoin, o primeiro deste tipo funcional. Esse propõe-se a ser, em sua fundamentação, uma moeda para o mundo digital que veio com a internet. Entretanto, há muito debate se isso será ou não alcançado.

O Bitcoin tem em sua premissa ser um meio de troca para o mundo digital, como foi postulado pelo seu criador em sua fundação, mas pode ter tomado rumos não previstos. Atualmente, o Bitcoin ganha cada vez mais notoriedade e adesão de investidores institucionais pelo mundo, mas sofre diversos ataques ao seu objetivo de ser meio de troca por conta de, entre outros fatores, sua volatilidade. Entretanto, como

veremos a seguir, o Bitcoin possui algumas características notáveis que poderão fazer com que ele se torne de grande utilidade no futuro.

A complexidade técnica e teórica do Bitcoin é considerável, além de envolver diversas disciplinas diferentes, como computação, matemática e economia. Ainda, une invenções complexas em si mesmas, as quais a internet e a criptografia são destaques. O trabalho aqui não almeja exaurir todos os conceitos técnicos e as suas respectivas fundamentações. Porém, para efeito de melhor entendimento das perspectivas futuras de uso propostas ao decorrer do trabalho, um breve resumo da história do Bitcoin e dos seus aspectos técnicos serão apresentados.

O trabalho objetiva, a partir de um breve preâmbulo em sua história e seu funcionamento, identificar os usos atuais, as adversidades ao sistema, e como serão as prováveis utilizações do Bitcoin no futuro. A estruturação se dará da seguinte forma:

- 1) Breve resumo da história do Bitcoin, de pouco antes da sua fundação até hoje.
- 2) Aspectos teóricos e técnicos, o que fundamenta o Bitcoin, suas características técnicas e como funcionam na prática.
- 3) Perspectivas de uso futuro, onde serão considerados conceitos econômicos, outros ativos para efeito comparativo, potenciais adversidades e inferências lógico-dedutivas a partir do que foi discutido; focaremos nos usos de meio de troca, reserva de valor e ativo em um portfólio de investimento.

Algumas considerações: Bitcoin (com “B” maiúsculo) trata do sistema como um todo e bitcoin (com “b” minúsculo) trata da unidade de conta que é utilizada dentro da rede; quaisquer erros, omissões e opiniões são de responsabilidade apenas do autor deste trabalho.

Ao final, não teremos certeza sobre o futuro do Bitcoin, mas teremos feito inferências com base na teoria econômica, nas características de outros ativos, e no comportamento humano. Afirmar categoricamente qual é o futuro de uma nova tecnologia é uma arrogância intelectual, porém devemos analisar as potencialidades de uso do Bitcoin no futuro, dado que é algo que, aparentemente, veio para fazer parte de mais uma etapa da história humana, seja como mais uma criação poderosa ou apenas uma curiosidade no meio do caminho.

2 BREVE HISTÓRIA

A história do Bitcoin, assim como de outras invenções e descobertas científicas, teve suporte através de conquistas dos mais diversos pesquisadores em diferentes áreas do conhecimento. Este aspecto será abordado com mais detalhes no próximo capítulo, mas basta pontuarmos que a fundamentação não surgiu do dia para a noite.

Nos anos 1990, um movimento intitulado *cypherpunk* começou a surgir nos Estados Unidos defendendo a liberdade de pesquisa e de publicações na área de criptografia, algo que o governo norte-americano estava se opondo. Este movimento defendia a ideia de que a criptografia seria uma base que fundamentaria novas mudanças na sociedade, principalmente no que concerne à anonimidade e à privacidade (FRANCO, 2015).

A ideia de uma moeda digital ou virtual não inicia no Bitcoin, e é anterior ao movimento *cypherpunk*. Entretanto, várias ideias que ajudaram ao desenvolvimento do conceito final de Bitcoin surgiram nesse grupo (FRANCO, 2015). Outros cientistas, pesquisadores e engenheiros tiveram essa ideia, como Adam Cash em 1997, Wei Dai em 1998 e Nick Szabo em 2005 (CLARK e NARAYANAN, 2017), mas haviam sempre aspectos técnicos que problematizavam a formulação concreta deste conceito. A principal adversidade era sempre a necessidade essencial de uma terceira parte envolvida para garantir a segurança das transações.

Uma proposta que objetivava tornar-se o dinheiro eletrônico de fato e solucionando problemas técnicos anteriores foi dada por Satoshi Nakamoto o Bitcoin. O nome do criador é um pseudônimo, podendo ser uma pessoa ou um grupo de pessoas; em seu perfil nos fóruns de criptografia, sua localização estaria situada no Japão, mas possivelmente era apenas uma dispersão. Ainda, pesquisas sobre seu nome não davam resultados (WALLACE, 2011). Entretanto, o que é relevante é que o criador (ou criadores) possuía conhecimento de altíssimo nível sobre diversos aspectos relevantes à criação do Bitcoin. Até hoje, apesar de várias investigações terem sido feitas, a identidade do criador da primeira criptomoeda é um mistério.

A primeira postagem sobre Bitcoin foi feita por Satoshi Nakamoto em um fórum de criptografia em 2008 e, no mesmo ano, o domínio *bitcoin.org* foi registrado.

Através de seu *paper* (2008), ele definiu o que era Bitcoin e todo o seu funcionamento técnico (FRANCO, 2015).

Uma versão puramente ponto-a-ponto de dinheiro eletrônico permitiria pagamentos online serem enviados diretamente de uma parte para outra sem passar por uma instituição financeira. (NAKAMOTO, 2008, p. 1, tradução nossa)

O Bitcoin pretende ser uma rede descentralizada de assinaturas digitais e de livros contábeis esparsos baseada numa unidade de conta, o bitcoin – BTC (ŠURDA, 2012). Seu objetivo fundamental é a de ser um meio de troca eletrônico que não precise de intermediários (NAKAMOTO, 2008).

No contexto temporal à criação do Bitcoin, tivemos a Grande Crise Financeira de 2008, recuperação de bancos comerciais pelos governos e novas formas, ou maneiras mais incisivas, de políticas monetárias por parte dos Bancos Centrais, como o afrouxamento quantitativo (*quantitative easing*) que, em suma, cria moeda eletronicamente. Independente de certo ou errado, o fato é que essas políticas favorecem a ocorrência de inflação, e uma das ideias do Bitcoin é a de ser uma moeda livre de inflação, i.e. quantidade fixa e com ocorrência de deflação (ULRICH, 2014).

A divisão dos períodos nas seções a seguir é arbitrária, objetivando apenas uma maior organização.

2.1 2009

Em 3 de janeiro de 2009, Satoshi Nakamoto registra a primeira criação de bitcoins da rede Bitcoin no seu primeiro bloco de registros, o bloco gênese; e, poucos dias depois, o primeiro *software*, cliente Bitcoin v0.1, estava disponibilizado gratuitamente para *download* (ULRICH, 2014). Desta forma, estava oficialmente criada a rede Bitcoin.

A primeira transação de fato da rede ocorreu em 12 de janeiro de 2009, entre Nakamoto e Hal Finney, um dos colaboradores na criação do Bitcoin, de 10 BTC para testes no sistema. Em outubro de 2009, o *website* New Liberty Standard precificou, baseado nos custos envolvidos na criação de bitcoins, a primeira taxa de câmbio do

bitcoin em relação ao dólar americano, onde \$ 1 seriam equivalentes a 1309,03 BTC (GRAF, 2016).

O ano de 2009 destacou-se para a experimentação técnica da rede e observação de possíveis erros. Não haviam, de fato, transações ou investimentos, apenas entusiastas que enxergavam no Bitcoin uma inovação tecnológica ou um possível ativo de valor futuro (GRAF, 2016).

2.2 2010-2013

Em 2010, as primeiras casas de câmbio surgiram, destacando-se a MtGox no Japão (GRAF, 2016). Ainda em 2010, a icônica primeira transação com produto físico ocorreu. Tratava-se da compra de duas pizzas por 10.000 BTC (com a cotação de agosto de 2021, essa transação equivaleria a cerca de 2,5 bilhões de reais¹) pelo programador Laszlo Hanyecz (JENKINSON, 2018).

O ano de 2011 contou com a conquista da paridade de 1 BTC equivaler a \$ 1. A partir de então a volatilidade e a valorização do bitcoin em relação ao dólar não pararam de crescer. Também em 2011, a empresa Silk Road passou a aceitar Bitcoin; foi a partir disso que a rede Bitcoin passou a ter má fama, dado que este *site* de comércio eletrônico transacionava substâncias ilegais, de armas até drogas. O ano de 2011 foi um marco para a rede Bitcoin, onde, apesar de ter sido em parte utilizado de forma criminosa, constatou-se a possibilidade de atuar como meio de transação (GRAF, 2016).

Ainda em 2011, Satoshi Nakamoto manda mensagens para outros desenvolvedores para tomarem seu lugar no desenvolvimento do Bitcoin. Ele afirmava que iria seguir para outros projetos e então desapareceu. Seus bitcoins nunca foram usados.²

¹ Fonte: CoinMarket. Disponível em: <<https://coinmarketcap.com/currencies/bitcoin/>>. Acesso em: 23 ago. 2021.

² RIZZO, Pete. 10 years ago today, Bitcoin creator Satoshi Nakamoto sent his final message. Forbes, 2021. Disponível em: <<https://www.forbes.com/sites/peterizzo/2021/04/26/10-years-ago-today-bitcoin-creator-satoshi-nakamoto-sent-his-final-message/>>. Acesso em: 22 ago. 2021.

Em 2012 e 2013, várias empresas começaram a aceitar o Bitcoin como pagamento, como o Reddit e o Wordpress, são lançados novos aplicativos envolvidos na rede da criptomoeda para *smartphones* e computadores, é criada a Fundação Bitcoin e mais transações envolvendo usuários são detectadas (GRAF, 2016). Além disso, há a queda do mercado Silk Road, provocando volatilidade de curto prazo no preço do bitcoin (JENKINSON, 2018).

2.3 2014-2017

Em 2014, a MtGox, uma das maiores corretoras de bitcoins da época, perdeu várias moedas de seus clientes e culpou a rede por este acontecimento (a Fundação Bitcoin rebateu que foi irresponsabilidade da própria empresa), logo depois anunciou falência (JENKINSON, 2018). Ainda nesse ano, um marco regulatório: o primeiro instrumento do mercado financeiro com relação ao Bitcoin foi aprovado, um *swap* de troca de rentabilidades futuras relacionado o preço do bitcoin³.

O marco de mais de 100 mil comerciantes que aceitavam bitcoins foi obtido em 2015⁴. Ainda nesse ano, a primeira página da renomada revista de economia, The Economist, coloca a tecnologia do Bitcoin em sua página e fala sobre a sua capacidade de mudar o mundo (JENKINSON, 2018). Em 2016, o governo japonês reconhece que criptomoedas, como o Bitcoin, possuem função similar ao dinheiro⁵, e uma grande corretora de criptomoedas, Bitfinex, é *hackeada* e perde cerca de 120.000 BTC⁶.

³ CALLAWAY, Claudia. First Bitcoin Swap Proposed. The National Law Review, 2014. Disponível em: <<https://www.natlawreview.com/article/first-bitcoin-swap-proposed>>. Acesso em: 23 ago. 2021

⁴ CUTHBERTSON, Anthony. Bitcoin now accepted by 100,000 merchants worldwide. International Business Times, 2015. Disponível em: <<https://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613>>. Acesso em: 23 ago. 2021.

⁵ Japan Oks recognizing virtual currencies as similar to real money. TheJapanTimes, 2016. Disponível em: <<https://www.japantimes.co.jp/news/2016/03/04/business/tech/japan-oks-recognizing-virtual-currencies-similar-real-money>>. Acesso em: 23 ago. 2021.

⁶ COPPOLA, Frances. Theft And Mayhem In The Bitcoin World. Forbes, 2016. Disponível em: <<https://www.forbes.com/sites/francescoppola/2016/08/06/theft-and-mayhem-in-the-bitcoin-world>>. Acesso em: 23 ago. 2021.

Em 2017, o Japão passa uma lei para aceitar formalmente bitcoins como forma de pagamento, o bitcoin transacionado em iene japonês (¥) representava o 2º maior mercado da rede Bitcoin⁷.

2.4 2018-2021

George Soros, o grande investidor do mercado de capitais e de renome mundial, afirma em 2018 que o Bitcoin é uma bolha⁸.

De 2019 a 2021, vários produtos financeiros em mercados de capitais em diversos países do mundo foram surgindo, como o ETF (*Exchange-traded fund*) com *ticker* QBTC11 (100% alocado em bitcoins) no Brasil⁹; além disso, mais empresas passaram a aceitar bitcoins como forma de pagamento e/ou facilitar o uso através do seu sistema, como o PayPal¹⁰. Ainda em 2021, a China proíbe a atividade de mineração¹¹ da rede do Bitcoin em seu país, região onde havia mais da metade dessa atividade do sistema¹².

⁷ KHARPAL, Arjun. Bitcoin value rises over \$1 billion as Japan, Russia move to legitimize cryptocurrency. Disponível em: <<https://www.cnbc.com/2017/04/12/bitcoin-price-rises-japan-russia-regulation.html>>. Acesso em: 23 ago. 2021.

⁸ PORZECANSKI, Katia. Soros says Bitcoin bubble won't have 'Sharp Break' like others. Bloomberg, 2018. Disponível em: <<https://www.bloomberg.com/news/articles/2018-01-25/soros-says-bitcoin-bubble-won-t-have-sharp-break-like-others>>. Acesso em: 23 ago. 2021

⁹ RUBINSTEINN, Gabriel. Primeiro ETF de bitcoin do Brasil é anunciado e chega à B3 no dia 23. Exame, 2021. Disponível em: <<https://exame.com/future-of-money/criptoativos/primeiro-etf-de-bitcoin-do-brasil-ja-esta-em-oferta-e-chega-a-b3-no-dia-23/>>. Acesso em: 23 ago. 2021

¹⁰ IRRERA, Anna; WILSON, Tom. PayPal to open up network cryptocurrencies. Reuters, 2020. Disponível em: <<https://www.reuters.com/article/ctech-us-paypal-cryptocurrency-idCAKBN2761L6-OCATC>>. Acesso em: 23 ago. 2021

¹¹ O processo de mineração, atividade do *proof-of-work* será explicado na seção 3.2.

¹² SHEN, Samuel; GALBRAITH, Andre. Proibição da China faz mineradores se voltarem para o exterior. Reuters, 2021. Disponível em: <<https://www.reuters.com/article/tech-china-bitcoin-idBRKCN2E11RA-OBRIN>>. Acesso em: 24 ago. 2021.

Nesses últimos anos, o valor de mercado do Bitcoin atingiu preços inimagináveis até para a maioria de seus entusiastas iniciais como veremos na próxima seção.

2.5 Dados da rede Bitcoin ao longo do tempo

Nesta seção, serão apresentados dados relacionados à rede do Bitcoin, desde cerca de 2013-2014, pois pouco foi registrado de dados no início após sua criação em 2008 (caso existam dados desde a criação, estes serão apresentados), até atualmente, ano de 2021. Para efeito comparativo, hoje 23 de agosto de 2021, a unidade do bitcoin está valendo \$ 50 176,90 (inicialmente, em 2009, valia cerca de \$ 0,0004 como dito anteriormente), e o valor de mercado está em \$ 943,171 bilhões¹³.

Tabela 1: Preço de 1 bitcoin (BTC) e valor de mercado da rede Bitcoin em dólar (\$) em 1 janeiro de 2014 a 2021.

ANO	PREÇO UNITÁRIO DO BITCOIN - BTC (\$)	VALOR DE MERCADO (\$)
2014	\$ 802,39	\$ 9,781 B
2015	\$ 315,03	\$ 4,309 B
2016	\$ 433,44	\$ 6,517 B
2017	\$ 1 021,75	\$ 16,429 B
2018	\$ 14 982,10	\$ 251,377 B
2019	\$ 3 943,41	\$ 68,849 B
2020	\$ 6 985,47	\$ 126,699 B
2021	\$ 32 127,27	\$ 597,205 B

Fonte: Elaborado pelo autor com base em: <<https://coinmarketcap.com/currencies/bitcoin/>>. Acesso em: 23 ago. 2021.

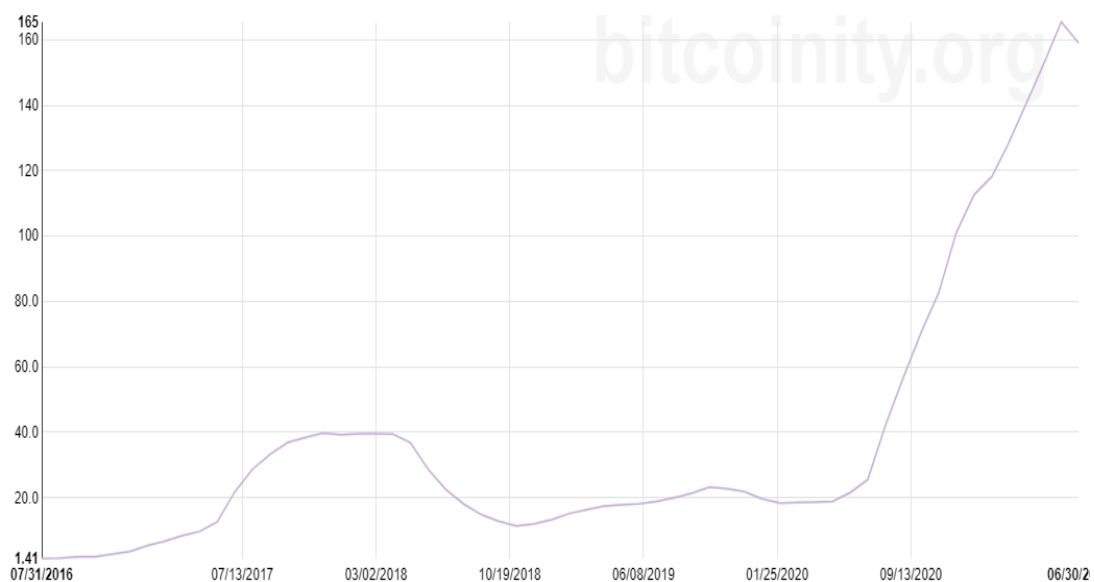
¹³ Fonte: CoinMarketCap. Disponível em: <<https://coinmarketcap.com/currencies/bitcoin/>>. Acesso em: 23 ago. 2021.

Gráfico 1: Preço da unidade de bitcoin (BTC) em dólar (\$) de 30/09/2013 até 23/08/2021.



Fonte: Coindesk. Disponível em: <<https://www.coindesk.com/pt/price/bitcoin>>. Acesso em: 23 ago. 2021.

Gráfico 2: Volatilidade do preço do bitcoin (BTC) em dólar (\$) de 31/07/2016 até 30/06/2021 usando média móvel de 10 dias.



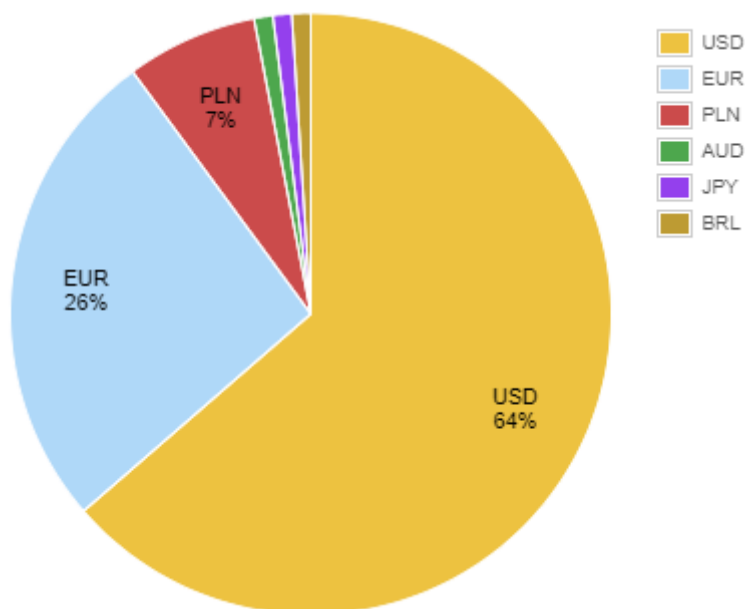
Fonte: Bitcoinity. Disponível em: <<https://data.bitcoinity.org/markets/volatility/5y/USD>>. Acesso em: 23 ago. 2021.

Gráfico 3: Valor de mercado do Bitcoin em dólar (\$) de abril de 2013 até agosto de 2021.



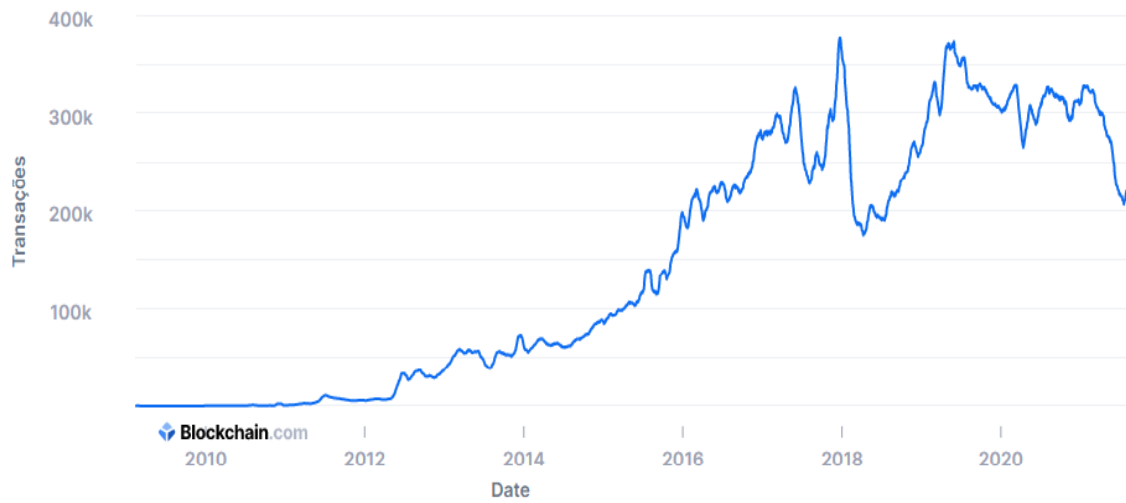
Fonte: CoinMarketCap. Disponível em: <<https://coinmarketcap.com/currencies/bitcoin/>>. Acesso em: 23 ago. 2021.

Gráfico 4: Transações de compra e venda relacionadas ao bitcoin (BTC) de acordo com o rank de moedas nos últimos 30 dias a partir de 23 de agosto de 2021; nos anos anteriores o domínio era da moeda chinesa renminbi (USD: dólar, EUR: euro, PLN: zloty polonês, AUD: dólar australiano, JPY: iene japonês, BRL: real brasileiro).



Fonte: BitcoinCharts. Disponível em: <<https://bitcoincharts.com/charts/volumepie/>>. Acesso em: 23 ago. de 2021.

Gráfico 5: Número total de transações confirmadas por dia.



Fonte: BlockChain.com. Disponível em: <<https://www.blockchain.com/charts/n-transactions>>. Acesso em: 27 ago. 2021.

3 ASPECTOS TEÓRICOS E TÉCNICOS

Ouro e prata são regidos pelas leis da natureza, física e química regem os fundamentos por trás desses elementos. Assim como estes, as criptomoedas (ou criptoativos) possuem uma espécie de leis (que podem ser mutáveis ou não) desse gênero que é o código aplicado em suas fundações na criação por *software*. Desta forma, cada ativo digital destes possuirá características próprias de acordo com a sua fundação, e pode permitir nenhuma alteração, poucas alterações e muitas alterações no seu futuro. Antes de entrar nos aspectos mais teóricos e técnicos que concernem ao Bitcoin, cabe salientar que trataremos apenas de um preâmbulo e não objetivamos exaurir os conceitos técnicos acerca de seu sistema, dado que foge da área do conhecimento econômico.

A invenção do Bitcoin não foi algo da noite para o dia, dado a sua complexidade técnica, várias teorias foram desenvolvidas com o tempo e se acumulando em um estoque de conhecimento até culminarem em sua criação. Podemos considerar o Bitcoin como uma inovação schumpeteriana, no sentido de que é um novo produto no mercado. A importância da figura de Satoshi Nakamoto (pseudônimo) foi a de reunir várias teorias dispersas e a de resolver o problema dos gastos duplos sem a necessidade de um terceiro envolvido; a partir disso, ele gera o sistema Bitcoin. O primeiro anúncio oficial sobre a ideia dessa rede foi em 2008 com o *paper* “Bitcoin: a peer-to-peer electronic cash system” de Nakamoto, este introduz suas concepções iniciais sobre a rede, a ideia de criar um meio de pagamentos para o mundo digital e os seus conceitos técnicos e teóricos. Em 2009, Satoshi Nakamoto comenta em um fórum online: “Eu desenvolvi um novo sistema de dinheiro virtual ponto-a-ponto de código aberto chamado Bitcoin. Ele é completamente descentralizado, sem servidor central ou partes de confiança, porque tudo é baseado em prova criptográfica ao invés de confiança.”¹⁴ (tradução nossa).

O Bitcoin é um protocolo (ou sistema) de comunicação descentralizada, ponto-a-ponto, e de código aberto. Nele, há informações que são geradas (*bites* computacionais – unidades de medida para o armazenamento de informações digitais), distribuídas entre esses pares, sem a necessidade de um terceiro de confiança envolvido,

¹⁴ NAKAMOTO, Satoshi. Bitcoin open source implementation of P2P currency. P2P Foundation, 2009. Disponível em: <<http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>>. Acesso em: 10 mar. 2021.

e atuam como um meio de pagamento, dado que o sistema impede gastos duplos. No protocolo Bitcoin é que entram as unidades bitcoins – BTC (BÖHME et al., 2015).

3.1 Teoria Antecedente

A ideia de um dinheiro virtual não é nova, existiram conceitos antecedentes ao Bitcoin. Adam Cash formulou a concepção de *hashcash* em 1997, Wei Dai idealizou o *b-money* em 1998 e Nick Szabo escreveu sobre *bit gold* em 2005 (CLARK e NARAYANAN, 2017). Estas ideias esbarravam em algumas adversidades, com destaque para o problema do gasto duplo, onde, caso não houvesse quem verificasse as transações (a terceira parte de confiança), poderia haver ocorrências em que usuários usassem sua quantia (informação de dados) para efetuar um pagamento duas vezes, por exemplo, copiando o arquivo de informações (ULRICH, 2014).

A estrutura de dados do livro-razão que viria a tornar-se o *blockchain* veio de conceitos de Haber e Stornetta, o *linked timestamping*. As chaves públicas e privadas, que são as identificações dos usuários, vieram de conceitos de David Chaum sobre endereços e pseudônimos digitais em 1981. E o conceito de *proof-of-work* (PoW), apesar de não ter esse nome ainda, veio inicialmente de Dwork e Naor em 1992 (CLARK e NARAYANAN, 2017). O que importa aqui não é entender todos os conceitos e as ideias que vieram anteriores ao Bitcoin, mas perceber que eles tiveram origem na pesquisa de outros cientistas e que acabaram fundamentando todo o sistema.

Satoshi Nakamoto formulou então uma solução para o problema do gasto duplo que não necessite de uma terceira parte de confiança envolvida, que normalmente são instituições financeiras, como um banco comercial (NAKAMOTO, 2008). Outro problema solucionado por Nakamoto, e que atormentava a comunidade de criptografia e de computação, foi o “Problema dos Generais Bizantinos”, onde todas as partes envolvidas devem concordar em apenas uma estratégia ou então haverá completa falha no sistema; a solução dada para esse problema foi o mecanismo de consenso e o *proof-of-work* (PoW)¹⁵, que serão explicados nas próximas seções.

¹⁵ MOSKOV, Alex. What is the Byzantine Generals Problem? Coincentral, 2018. Disponível em: <<https://coincentral.com/byzantine-generals-problem/>>. Acesso em: 23 ago. 2021.

[...] Bitcoin foi incomum e sucedido não porque estava na vanguarda da pesquisa em qualquer de seus componentes, mas porque ele combinava ideias antigas de vários campos sem relação. (CLARK e NARAYANAN, 2017, p. 45, tradução nossa)

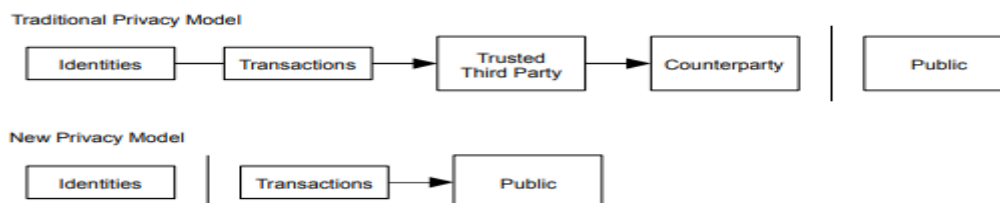
3.2 O Sistema

O Bitcoin, como sistema, envolve basicamente dois elos principais: o *blockchain* e os pares de chaves digitais, público e privado. Estes dois componentes possibilitam as transações. O livro-razão (*blockchain*) é distribuído de forma descentralizada entre os componentes da rede (*nodes*) – sem precisar de um terceiro envolvido, de forma que não haja erros e gastos duplos, e o *blockchain* registra as transações entre as assinaturas digitais (chaves) (ŠURDA, 2012). Os bitcoins não podem ser falsificados ou tomados de volta após uma transação por conta desses mecanismos. Além disso, o Bitcoin¹⁶ é uma rede de código aberto que possui desenvolvedores espalhados pelo mundo que fazem contribuições de melhorias.

As transações são feitas dentro do sistema e suas unidades são denominadas de bitcoins, que são “pacotes” de informação computacional representando uma fração do total, onde 1 bitcoin (BTC) pode ser dividido 100 milhões de vezes até atingir 1 satoshi (0,00000001 BTC) (ULRICH, 2014). Toda a oferta de bitcoins está limitada em 21 milhões BTC desde sua criação, e este limite vai aproximando-se com a atividade dos mineradores ao longo do tempo (AMMOUS, 2018).

Uma das principais questões que Nakamoto preocupava-se e resolveu implementar no sistema do Bitcoin foi a privacidade para os seus usuários. Em seu modelo, as transações são públicas e as identidades dos usuários privadas; diferente do usual (NAKAMOTO, 2008), como demonstrado nessa figura:

Figura 1: Modelos de privacidade nas transações.



Fonte: NAKAMOTO (2008, p. 6).

¹⁶ Para baixar o *software* do Bitcoin, onde há a validação do *blockchain* e *wallet* para bitcoins, acesse: <<https://bitcoincore.org/>>.

Para que ocorram transações ponto-a-ponto, são necessários os pares de chaves criptográficas: públicas e privadas. Cada usuário, possui uma chave pública e uma privada. A chave pública é responsável por receber as transações, enquanto a chave privada é responsável por fazer transações e administrar os seus recursos (ŠURDA, 2012). De certa forma, a chave pública é o endereço e a privada é a assinatura. Ninguém é capaz de descobrir a chave privada de alguém e os usuários não devem passá-la a outros (a não ser que queiram perder seus bitcoins); e a chave pública pode ser divulgada sem problemas para receber os pagamentos. O usuário deve sempre resguardar sua chave privada (anotando em um papel, fazendo *backups* etc.), pois os bitcoins serão perdidos para sempre caso esta chave seja perdida.

As *wallets*¹⁷ são mecanismos que guardam o par de chaves (ou pares, pois uma pessoa pode ter vários pares de chaves) do sistema do Bitcoin, podendo ser *software* (apenas digital) ou *hardware* (vinculado a um objeto, muitas vezes similar a um *pen drive*) (BÖHME et al., 2015). Existem formas de se proteger melhor com a utilização das *wallets*, uma delas é a de possuir uma *hot wallet* (conectada na internet) usada para transações e outra *cold wallet* (não conectada na internet) para guardar os recursos como cofre ou fazer transferências pessoalmente¹⁸.

¹⁷ Para criar uma *wallet* virtual, acesse: <<https://bitcoin.org/en/choose-your-wallet>>.

¹⁸ CONWAY, Luke. What are the Safest Ways to Store Bitcoin? Investopedia, 2021. Disponível em: <<https://www.investopedia.com/news/bitcoin-safe-storage-cold-wallet/>>. Acesso em: 24 ago. 2021.

Figura 2: Processo simplificado de transação e validação no *blockchain*.



Fonte: Braiscompany. Disponível em: <<https://g1.globo.com/pb/paraiba/especial-publicitario/braiscompany/braiscompany/noticia/2021/04/07/blockchain-quis-os-segredos-da-tecnologia-mais-segura-do-mundo.ghtml>>. Acesso em: 24 ago. 2021.

O termo *blockchain*¹⁹ não possui ainda uma definição padrão, mas ele foi a solução para o problema de gastos duplos e surgiu na rede do Bitcoin; inclusive, Nakamoto não utiliza esse termo (CLARK e NARAYANAN, 2017). Nele, todas as transações, desde a criação do sistema até as últimas atualmente, estão gravadas em vários blocos de informação que são unidos em uma corrente, de forma ponto-a-ponto através dos *nodes* e descentralizadamente (LEWIS, 2018). O *blockchain* pode ser entendido como uma aplicação tecnológica que funciona nos protocolos da *internet*, e possibilita diversos usos, como o registro de transações (o caso do Bitcoin), registro de inventário e outras funções envolvendo registro, rastreo e monitoramento, e pode ser privado diferindo do caso do Bitcoin (SWAN, 2015).

Os *nodes* são os verificadores da rede do *blockchain* e podem ser *fullnodes* ou apenas *nodes*. O *fullnode*²⁰ possui o registro de todas as transações do *blockchain* e o

¹⁹ Para acessar o *blockchain* do Bitcoin e suas transações de forma simplificada acesse: <<https://blockstream.info/>>.

²⁰ SHARMA, Rakesh. Running a Full Bitcoin Node for Investors. Investopedia, 2021. Disponível em:

node possui registro de parte das transações do *blockchain*. Ambos garantem a segurança do sistema de forma descentralizada e podem validar novas transações através do *proof-of-work* (prova de trabalho que também é chamada de mineração) (BÖHME et al, 2015). Caso alguém queira trapacear de alguma forma, como lançar transações que não existem, os *nodes* verificam, identificam essa tentativa e eliminam do sistema (AMMOUS, 2018). Esse sistema de confiança entre os *nodes* na rede do Bitcoin é chamado de mecanismo de consenso²¹ e possíveis alterações na rede, como uma aceleração do processo de verificação das transações, precisa atender ao consenso da maioria.

No que concerne à segurança do Bitcoin: quanto mais tempo passa e mais blocos são adicionadas ao *blockchain*, mais seguro ele se torna. Em um possível ataque ao sistema, o atacante deveria refazer todos os blocos feitos até então e depois ultrapassar a velocidade de criação dos novos blocos criados, isso requereria um poder computacional bem improvável de se obter, dado à descentralização do sistema (NAKAMOTO, 2008).

O *proof-of-work* do Bitcoin faz parte do sistema de *blockchain* para validação (fazer com que ocorram) transações; estas são validadas em um tempo médio de 10 minutos (algumas demoram menos e outras mais) – esse tempo é ajustado pela própria dificuldade já estabelecida no código do Bitcoin para permanecer próximo a esse tempo médio (BÖHME et al., 2015). O “minerador”, em alusão ao processo de minerar ouro, faz o *proof-of-work*, que é um processo matemático de solução da transação no sistema (este é um problema que exige poder computacional para ser resolvido, por isso o gasto de energia e *hardware* especializado), valida a transação, coloca em um bloco e une ao *blockchain*, e então recebe uma recompensa por isso; ainda, a dificuldade de mineração aumenta com o aumento do poder computacional da rede, fazendo com que permaneça próximo da média de tempo supracitada (ULRICH, 2014).

Podemos resumir que as transações ocorrem no sistema do Bitcoin da seguinte forma: (1) uma transação é requerida através do uso de uma chave privada em um endereço (chave pública); (2) os mineradores fazem o *proof-of-work* (solução matemática para validação) da transação; (3) um bloco é criado registrando a transação (ou informação é enviada para um bloco pré-existente); (4) o bloco com o registro da

<<https://www.investopedia.com/news/running-full-bitcoin-node-investors/>>. Acesso em: 24 ago. 2021.

²¹ FRANKENFIELD, Jake. Consensus Mechanism (Cryptocurrency). Investopedia, 2021. Disponível em: <<https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp>>. Acesso em: 24 ago. 2021.

transação é enviado para os participantes da rede (*nodes*) que aceitam (ou rejeitam); (5) os mineradores recebem uma recompensa (taxa de transação e/ou geração de novos bitcoins) pelo seu trabalho (*proof-of-work*); (6) o bloco com o registro da transação é então unido a todos os outros blocos de transação no *blockchain*; (7) a informação é transmitida no sistema para todos os participantes; (8) a transação é concluída.

Tabela 2: Componentes do Bitcoin.

Componentes do Bitcoin	Descrição
Bitcoin	Bitcoin (“b” maiúsculo) envolve todos os componentes do sistema, dos mineradores às unidades transacionais.
bitcoins	As unidades transacionais do sistema, pedaços de informação.
Pares de Chaves	Chave pública é o equivalente ao endereço para recebimento, e chave privada a senha para efetuar transações.
<i>Blockchain</i>	Registro descentralizado de todas as transações da rede do Bitcoin.
Blocos	“Locais” onde são registradas as transações.
Nodes	Validadores da rede, podem ser <i>nodes</i> (possuem parte do <i>blockchain</i>) ou <i>fullnodes</i> (possuem todo o registro do <i>blockchain</i>); garantem o mecanismo de consenso e a estabilidade do sistema.
Minerador	<i>Nodes</i> que fazem a prova de trabalho (<i>proof-of-work</i>) para validar as transações em blocos que irão para o <i>blockchain</i> . São remunerados com novos bitcoins e/ou taxas de transação.
<i>Proof-of-Work</i>	Solução matemática para a transação ser validada em um bloco de registro que irá para o <i>blockchain</i> .

Fonte: Elaborado pelo autor.

Nakamoto (2008, p. 8, tradução nossa), ao concluir seu *paper* de apresentação do Bitcoin, resume as principais características do sistema:

Nós propusemos um sistema para transações eletrônicas sem depender de [terceiro de] confiança. Nós começamos com a estrutura usual de moedas feitas a partir de assinaturas digitais, que fornecem um forte controle de propriedade, mas é incompleto sem uma forma de prevenir o gasto duplo. Para resolver isso,

nós propusemos uma rede ponto-a-ponto usando prova de trabalho [*proof-of-work*] para registrar o histórico público de transações que rapidamente torna-se computacionalmente impraticável para um invasor alterar esses nós [*nodes*] honestos que controlam a maioria do poder computacional. A rede é robusta em sua simplicidade não estruturada. [...] Eles [*nodes*] votam com seu poder computacional, expressando sua aceitação de blocos válidos ao trabalhar para estendê-los e rejeitando blocos inválidos ao recusar em trabalhar neles. Qualquer regra e incentivos necessários podem ser aplicados com este mecanismo de consenso.”

Outro resumo do sistema é dado por Lewis (2018, p. 20, tradução nossa):

[...] Protocolos do Bitcoin são escritos como o Código Bitcoin que funciona como o *Software* Bitcoin que cria Transações Bitcoin contendo dados sobre Moedas Bitcoin na *Blockchain* Bitcoin.

3.3 Incentivos

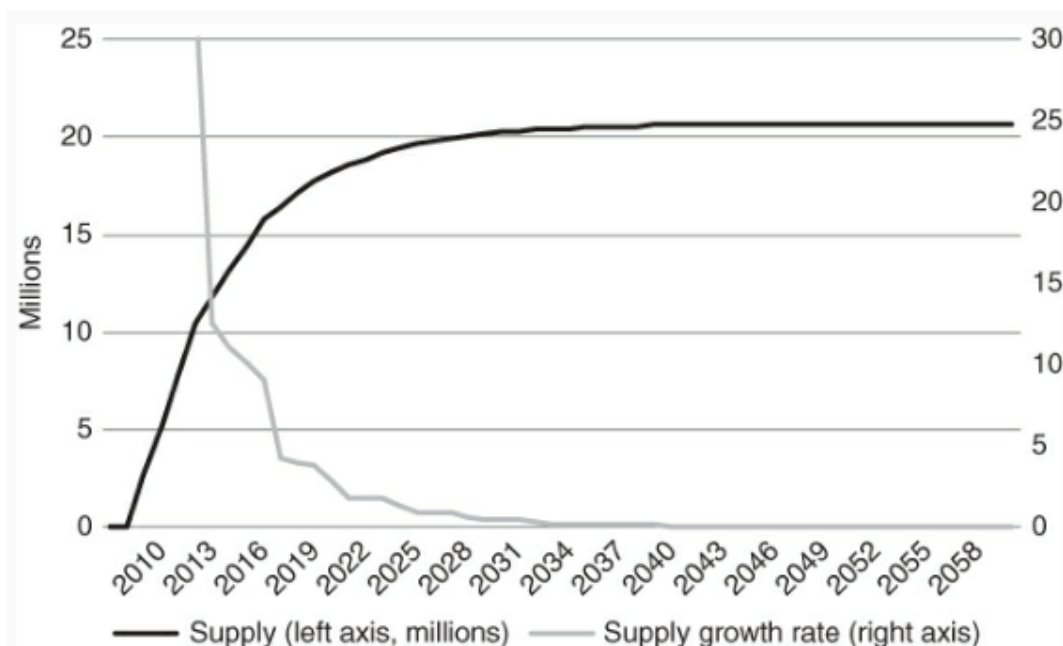
O Bitcoin gera incentivos para que os agentes, fundadores da rede, mantenham o próprio sistema seguro, livre de falhas e operacional. Dito assim, o Bitcoin possui algo de fiduciário em seu sistema, dado que depende da confiança que todos os agentes possuem no sistema. As moedas fiduciárias emitidas por Bancos Centrais não possuem a confiança baseada no lastro em algo (anteriormente havia o ouro estabelecendo essa paridade²²), mas na capacidade de seus emissores serem protetores com a moeda e não fazerem emissões descontroladas e políticas desastrosas.

A oferta total de bitcoins será 21 milhões BTC, e é estimado que isso ocorra no ano de 2140 (ULRICH, 2014). Atualmente (data em que este trabalho é escrito), foram

²² Em 1971, Nixon (presidente dos Estados Unidos na época) rompeu o acordo de Bretton-Woods que era a última conexão com o chamado padrão-ouro monetário, onde o dólar estabelecia paridade com o ouro e outras moedas ao dólar. Ainda assim, hoje em dia os Bancos Centrais possuem reservas de valor baseadas em outras moedas estrangeiras, ouro e outros ativos. Fonte: GHIZONI, Sandra K. Nixon Ends Convertibility of US Dollars to Gold and Announces Wage/Prices Controls. Federal Reserve History, 1971. Disponível em: <<https://www.federalreservehistory.org/essays/gold-convertibility-ends>>. Acesso em: 24 ago. 2021.

gerados (minerados) 18,798 M BTC²³. Com isso, o intuito do criador era criar uma escassez absoluta e que, conseqüentemente, os bitcoins fossem valorizados. Ainda, a maioria em consenso dos agentes que fundamentam a rede poderiam inflar a oferta do Bitcoin para uma quantia maior, mas seria irracional, dado que diminuiria o valor dos bitcoins.

Gráfico 6: Oferta total de bitcoins (curva escura e indicadores na vertical da esquerda) e taxa de crescimento da oferta de bitcoins (curva cinza e indicadores na vertical da direita) ao longo do tempo.



Fonte: AMMOUS (2018, p. 179).

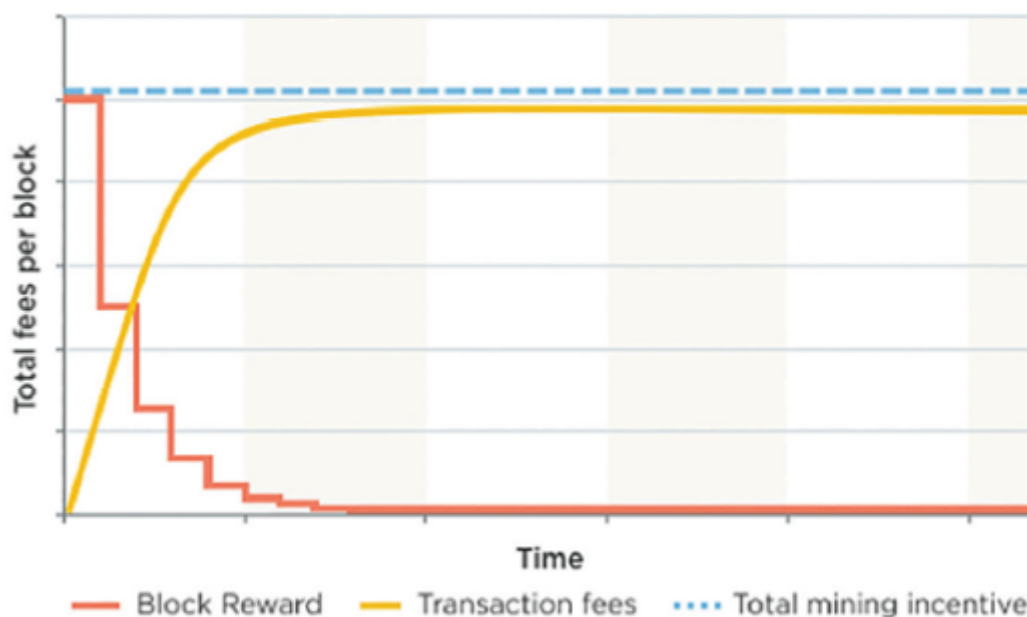
Os mineradores, aqueles que fazem o *proof-of-work* para registrar as transações, recebem como recompensa novos bitcoins gerados e/ou taxas de transação (ULRICH, 2014). As taxas de transação são escolhidas pelos envolvidos, mas há um consenso de qual é o melhor valor para as taxas em determinado momento e essas que seguem a maioria são registradas mais rapidamente (BÖHME et al., 2015). A geração de novos bitcoins (e recompensa para os mineradores) diminui pela metade (*halving*) de 4 em 4 anos até não haver mais recompensa de novos bitcoins²⁴. Após todos os bitcoins

²³ Fonte: CoinMarketCap. Disponível em: <<https://coinmarketcap.com/currencies/bitcoin/>> Acesso em: 25 ago. 2021.

²⁴ Fonte: TOLOTTI, Rodrigo. O que é o halving do Bitcoin e como ele afeta o mercado da criptomoeda.

serem gerados, os mineradores ainda serão necessários no sistema e apenas receberão recompensas de taxas de transação (ULRICH, 2014).

Gráfico 7: Recompensa por bloco x Recompensa por transações (considerando o incentivo a minerar) ao longo do tempo.



Fonte: LEWIS (2018, p. 155).

A dificuldade de gerar bitcoins em termos de *hardware* e de energia aumenta com o aumento de poder computacional na rede – e vice-versa (ULRICH, 2014), tudo para o registro das transações permanecer próximo de 10 minutos e, assim, aumentar a especialização desse mecanismo com o aumento de agentes envolvidos. Em outras palavras: quanto maior a dificuldade para minerar, maior a especialização, maior o investimento para minerar, maior o incentivo para permanecer honesto e ter bitcoins valorizados.

O mecanismo de consenso da rede, no que concerne ao poder computacional usado para fundamentar a rede e tomar decisões, precisa que a maior parte seja “honesta” para que não haja problemas na rede. Então, o que ocorre é que os *nodes* fundamentam a

Infomoney, 2020. Disponível em: <<https://www.infomoney.com.br/mercados/o-que-e-o-halving-do-bitcoin-e-como-ele-afeta-o-mercado-da-criptomoeda/>>. Acesso em: 26 ago. 2021.

rede e possuem incentivos para serem honestos, pois, caso não sejam, o sistema Bitcoin de que eles participam e possuem bitcoins perderá valor; além disso, os mineradores perderiam todo o trabalho usado (que é cada vez mais especializado e custoso em termos de energia e *hardware* computacional com o aumento de dificuldade) para minerar novos bitcoins e ganhar bitcoins de taxas de transação (outro que foi honesto ganhará estes bitcoins) (NAKAMOTO, 2008). Ainda, no menor sinal, a rede perceberá e inutilizará a possível fraude. Caso existam erros no sistema, o Bitcoin como um todo perderia valor. Em outras palavras, os agentes possuem incentivo para manter o sistema seguro e, conseqüentemente, ter bitcoins com valor, o que equivale a terem ganhos pecuniários com isso.

Em suma, o Bitcoin busca incentivar os seus agentes fundadores para que eles tenham recompensas e algo a perder caso façam algo errado ou desonesto. Então, os que fundamentam o sistema agem se fiscalizando e garantindo a unidade correta do Bitcoin. Isso é chamado na teoria dos jogos de “Equilíbrio de Nash”, onde nenhum jogador tem a ganhar caso mude sua estratégia unilateralmente. No caso do Bitcoin, os agentes só têm a ganhar se agirem em consenso e de forma que a estabilidade do sistema seja mantida.

Esta forma de incentivos dentro do Bitcoin foi pensada em sua fundação por Satoshi Nakamoto, alguns detalhes podem ter passado despercebidos quanto a suas conseqüências incentivadoras, mas o fulcro foi dimensionado.

No que concerne ao valor do Bitcoin, que é subjetivo, mas relaciona-se inicialmente ao custo operacional para manter o sistema, podemos, resumidamente, dimensionar seu possível ciclo virtuoso de valoração e valorização da seguinte forma (potencializado pelo *design* do Bitcoin e pelo efeito de rede por ter sido o primeiro criptoativo): (1) primeiros usuários aderem ao Bitcoin pelos mais diversos motivos (aspecto científico e tecnológico, perspectiva de uso econômico, curiosidade estranha etc.); (2) mais valor é agregado à rede (por possuir mais agentes fundadores); (3) mais usuários entram; e então repete-se (2) e (3) em alternância. Isso não significa que isso ocorra frequentemente ou que não terá fim, apenas que, baseado nos incentivos proporcionados pelo Bitcoin, é assim que deveria funcionar.

4 PERSPECTIVAS FUTURAS DE USO

Entender um pouco da sua história e dos fundamentos do Bitcoin é essencial para criar expectativas futuras sobre os usos do sistema de forma mais factível. Entretanto, de tudo que foi comentado, o mais importante é que: os bitcoins são escassos em sua fundação, os agentes que sustentam a rede têm incentivos para continuarem nesta tarefa, o sistema é descentralizado e não possui um comando central, e a rede como um todo já possui valor percebido por várias pessoas, apesar de valorarem e de utilizarem de forma diferente.

O processo inicial de criação de valor do Bitcoin iniciou-se com pessoas interessadas em diferentes aspectos do sistema, como aspecto técnico, possibilidade de uso econômico, bitcoins como forma de propriedade da rede, curiosidade etc. (GRAF, 2016). Nakamoto (2008) visou em sua criação um meio de troca digital e descentralizado. A criação do *blockchain* gerou diversos usos que podem ainda ser ampliados; e a primeira criptomoeda abriu um leque de diferentes ativos, os criptoativos (moedas, artes, *smart contracts* etc.). Na nossa análise, lidaremos apenas com os usos econômicos do Bitcoin em termos de sua unidade de transação, o bitcoin – BTC.

A seguir, falaremos das possíveis adversidades que o Bitcoin como sistema possui, indicando se realmente é um problema e se há solução. Depois falaremos dos usos para bitcoins: meio de troca, reserva de valor e ativo em um portfólio de investimento. Mais especificamente, se já são usados, o que foi encontrado por alguns pesquisadores, comparações com outros ativos dentro desse uso, os respectivos entraves e concluiremos cada seção destas indicando se há utilização presente e o que podemos esperar no futuro dado tudo que foi visto.

Alguns detalhes: quando falamos de perspectivas de uso futuro, nos referimos ao longo prazo mesmo que seja problemática esta visão para um artifício tecnológico; Bitcoin é novo (criado em 2008) em termos de tempo funcional e de novidade tecnológica, isso faz com que sua análise com base em dados passados possa não gerar conclusões significantes para o futuro (apesar de serem necessárias para as inferências).

4.1 Principais adversidades ao Sistema Bitcoin

Antes de lidar com os usos, trataremos das adversidades que o Bitcoin como sistema possui, destacaremos: complexidade técnica, energia, riscos de brecha no protocolo, uso criminoso, proibição e regulação, competição de outros criptoativos e políticas econômicas.

4.1.1 Complexidade Técnica

O sistema Bitcoin possui muitas inovações e utiliza de vários campos do conhecimento. Consequentemente, existe uma dificuldade para o entendimento de todos os seus mecanismos (tecnologia, teoria, incentivos etc.). Então, é argumentado que esta complexidade técnica pode ser repulsiva para possíveis usuários.

Na prática, entretanto, o que é necessário é uma adoção inicial por indivíduos entendidos nos aspectos técnicos. Após essa primeira adesão, mais revisões e análises são feitas para disseminação para o público comum. Caso eficiente e sem problemas visíveis, as mais diversas pessoas passam a adotar o sistema se perceberem utilidade.

A complexidade técnica do Bitcoin existe, mas não é um problema para o seu uso. Basta fazermos analogias às tecnologias recentes que são extremamente complexas, como *smartphone*, *internet* e aviões. Não precisamos nos tornar especialistas em algo complexo para poder utilizar e aproveitar seus benefícios.

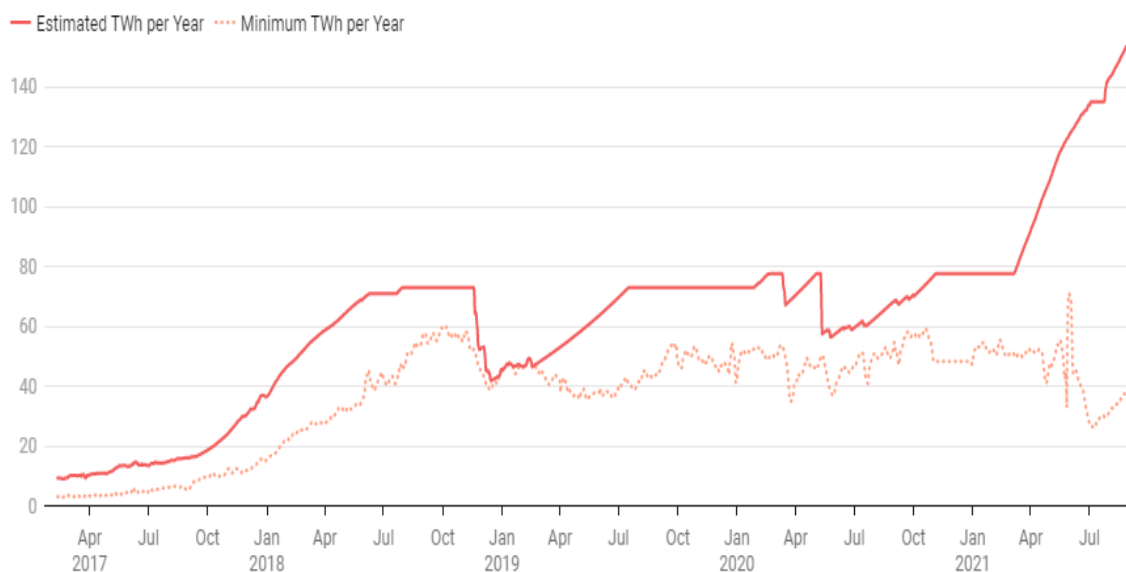
4.1.2 Energia

O uso de energia no Bitcoin é extremamente elevado. Isto ocorre pelos incentivos presentes no sistema, especificamente o ajuste de dificuldade da rede e o *proof-of-work*. Por conta destes, há uma necessidade cada vez maior de especialização no que concerne ao *hardware*, e estes equipamentos computacionais exigem maior consumo de energia.

O Bitcoin consome em energia elétrica, atualmente, equivalente à Malásia²⁵ (2021) e cerca de apenas 38% a menos do que a mineração de ouro²⁶ (2019). A utilização de energias renováveis varia em torno de 39%²⁷, mas é algo difícil de ser verificado.

Gráfico 8: Consumo anualizado de energia do Bitcoin em Terawatt-hora (TWh).

Bitcoin Energy Consumption



Fonte: Digiconomist. Disponível em: <<https://digiconomist.net/bitcoin-energy-consumption/>>. Acesso em: 28 ago. 2021.

O fato de utilizar energia não constitui um problema na suposição de que falte a energia elétrica, muito do que é usado e essencial na sociedade depende de energia elétrica (o mesmo vale para a *internet*). O consumo energético é realmente elevado e pode ser um problema no estado atual. Entretanto, esta alta especialização cria incentivos para

²⁵ Fonte: Digiconomist. Disponível em: <<https://digiconomist.net/bitcoin-energy-consumption/>>. Acesso em: 28 ago. 2021.

²⁶ Fonte: Cambridge Bitcoin Electricity Consumption Index. Disponível em: <<https://cbeci.org/cbeci/comparisons>>. Acesso em: 28 ago. 2021.

²⁷ Fontes: CLIFFORD, Catherine. China, Elon Musk raise alarm about bitcoin energy use: Here's how it could be made more 'green'. CNBC, 2021. Disponível em: <<https://www.cnbc.com/2021/06/30/china-musk-raise-alarm-on-bitcoin-energy-use-how-to-make-it-greener.html>>. Acesso em: 28 ago. 2021. ; SCHMIDT, John. Bitcoin's Energy Usage, Explained. Forbes, 2021. Disponível em: <<https://www.forbes.com/advisor/investing/bitcoins-energy-usage-explained/>>. Acesso em: 28 ago. 2021.

utilização de energias renováveis, que já é relevante para o sistema, e equipamentos mais eficientes em relação ao consumo energético. Além disso, existem possíveis melhorias no sistema que podem diminuir a utilização de energia elétrica no futuro, como uma alteração de como ocorre o *proof-of-work*, ou uma mudança do processo de validação para o *proof-of-stake* (PoS)²⁸. Esta forma é utilizada por outros criptoativos e valida a rede a partir da comprovação de posse de acúmulos da unidade transacional (e.g. posse de ether (unidade transacional) na rede Ethereum). O importante aqui é salientar que o *proof-of-stake* é utilizado com um processo mínimo de gasto energético e existem alternativas ao PoW.

4.1.3 Risco de brechas no Protocolo

O fato de ser de código aberto tem o benefício de que há uma cooperação entre vários usuários para aumentar a segurança do sistema. Entretanto, isso também poderia ajudar *hackers* a identificar falhas. Possíveis aproveitamentos de falhas no protocolo seriam quebra da criptografia e aproveitamento de *bugs* (erros), além do próprio uso pelos usuários através de computadores e de *smartphones* que são suscetíveis a invasões. Ainda, há a incipiente computação quântica que poderia quebrar qualquer criptografia atual existente.

Como Graf (2016) argumenta, existem muitos colaboradores na segurança do sistema Bitcoin, dado que a maioria deles possui bitcoins, ou seja, algo a perder caso o sistema falhe. Existem formas inclusive de restaurar todo o sistema em caso de colapso total através de replicação do *blockchain* anterior, onde tudo continuaria válido, chaves e quantias (GRAF, 2015).

Possíveis quebras no protocolo do Bitcoin são possíveis. Porém, quanto mais o tempo passa, mais ele consagra-se seguro. O problema de computação quântica²⁹ seria adversidade para tudo que possui criptografia, todos os sistemas de segurança do mundo poderiam ser invadidos (arsenais nucleares, bancos centrais etc.), a humanidade estaria

²⁸ Para mais informações, acesse: <<https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/>>.

²⁹ Computação quântica é um novo conceito muito complexo, mas que poderia ser resumido como um “super computador”. Fonte: Aaronson, Scott. What Makes Quantum Computing So Hard to Explain? Quantamagazine, 2021. Disponível em: <<https://www.quantamagazine.org/why-is-quantum-computing-so-hard-to-explain-20210608/>>. Acesso em: 28 ago. 2021.

em caos, o menor dos problemas seria o Bitcoin. Entretanto, é totalmente factível de imaginar que os protocolos de segurança de toda a *internet* acompanharão o avanço da computação quântica, tornando-os adequados para esta nova tecnologia. Os problemas que concernem à segurança do uso pelo próprio usuário, porém, deve ser atentada pelo mesmo. Em suma, os riscos relacionados ao protocolo devem ser sempre levados em conta, mas não constituem um grande problema à sobrevivência do Bitcoin.

4.1.4 Uso criminoso

A atividade criminosa por usuários do Bitcoin ficou famosa a partir do site *Silk Road*, que vendia itens ilícitos (ULRICH, 2014). Pela descentralização e falta de fiscalização, algumas utilizações podem ser feitas objetivando práticas ilegais, como evasão de impostos, lavagem de dinheiro e financiamento de terrorismo.

O que permite o Bitcoin ser usado por criminosos é sua descentralização e maior anonimidade, mas essas características também impedem (ou dificultam) ditaduras e governos autoritários de proibirem seu uso. Incluindo todos os outros criptoativos além do Bitcoin, a atividade ilícita de todo esse mercado foi de 0,8% em 2017, 0,4% em 2018, 2,1% em 2019 e 0,3% em 2020³⁰. Colocando em perspectiva, todo o agregado de atividade fraudulenta dos cartões de crédito e de débito nos Estados Unidos representavam 13,46% do total³¹.

Os problemas que concernem ao uso criminoso são muito sérios e existem de fato. Entretanto, cabe a regulação diminuir esse efeito. A eliminação total nunca será possível, assim como não é com as moedas utilizadas atualmente; utilizar uma moeda física para transacionar algo ilícito é muito mais potencialmente efetivo. Mais, a percepção de que o Bitcoin é totalmente anônimo não confere. Segundo BÖHME et al. (2015), análises de *wallets* e comportamento dos usuários podem permitir identificar cerca de 50% dos usuários. Ainda, o governo e as instituições competentes podem acessar

³⁰ Fonte: Bitcoin: At the Tipping Point. Citibank, 2021. Disponível em: <<https://www.citivelocity.com/citigps/bitcoin/>>. Acesso em: 19 ago. 2021.

³¹ Changes in US Payments Fraud from 2012 to 2016: Evidende from the Federal Reserve Payments Study. Federal Reserve, 2018. Disponível em: <<https://www.federalreserve.gov/publications/files/changes-in-us-payments-fraud-from-2012-to-2016-20181016.pdf>>. Acesso em: 28 ago. 2021.

mais informações sobre corretoras de criptoativos (*exchanges*) e obter informações concernentes aos usuários, além disso já existem listas na rede de endereços usados com fim criminoso (*blacklists*) (BÖHME et al., 2015).

No que concerne a golpes aplicados usando o sistema, não foi o Bitcoin que roubou essas pessoas, mas criminosos aproveitando da crescente popularidade da rede e de sua complexidade para enganá-las, principalmente prometendo ganhos fáceis. Sempre haverá enganadores enquanto houver pessoas querendo lucros rápidos. A história humana é repleta de exemplos de enganações envolvendo os mais diversos produtos, e.g. ouro e petróleo. O problema neste aspecto não é do Bitcoin, mas da própria criminalidade que usará de qualquer meio para enganar as pessoas.

4.1.5 Proibição e regulação

A regulação não deve ser problema ao Bitcoin. Caso essa seja bem fundamentada e aliada às características que o sistema possui, será um benefício para o Bitcoin. Tiraria o Bitcoin da zona cinzenta de regulação e o traria para a luz. Daria maior segurança para sua utilização, principalmente como ativo de investimento, o que aumentaria sua adoção.

Voltando ao aspecto do uso por criminosos: as novas tecnologias também ajudam criminosos a cometerem crimes, como motocicletas, *internet* e dinheiro, e nem por isso iremos banir tudo, o benefício supera o malefício. O que resta são formas de conscientização, como uma maior educação no que concerne o Bitcoin, e de regulação competente que atenuar este problema.

A proibição total pode ser encarada como uma adversidade muito hipotética. Vários agentes utilizam atualmente do sistema, inclusive investidores institucionais e bancos. Além disso, banir o uso de bitcoins seria uma restrição extrema de liberdade. O caminho é a regulação e a educação.

4.1.6 Competição de outros criptoativos

Após ter criado todo um novo mercado, o Bitcoin possui concorrências de diversos ativos com diferentes funções. A criação de um criptoativo é muito fácil, bastando inclusive copiar códigos base de outros protocolos. Atualmente, existem criptoativos dos mais diversos objetivos, como, por exemplo, colecionáveis (*Non-fungible tokens* - NFTs)³², contratos (*smartcontracts*)³³ e serviços financeiros (*Decentralized Finance* – DeFi)³⁴. Ethereum, Cardano, Tether, Dogecoin, a lista de possíveis concorrentes é grande e não para de crescer. Se formos comparar com todo o mercado de criptoativos, sem distinguir os diferentes, teríamos que o *market share* do Bitcoin está declinando, indo de 70% no começo de 2021 para 48% em julho de 2021³⁵.

Entretanto, nem todos são concorrentes. Como dito anteriormente, existem várias funções atualmente para os criptoativos e muitos tentam, inclusive, complementar a utilização do Bitcoin. A segunda maior criptomoeda, por exemplo, ether da rede Ethereum, atua em um segmento totalmente diferente do Bitcoin, que é a utilização de *smartcontracts*. Ainda, a perda de *market share* do Bitcoin também está associada ao aumento de *market cap* total, onde ele perde dominância, mas também ganha capitalização.

Desta forma, a concorrência de outros criptoativos não é uma ameaça ao Bitcoin, além de ajudar a trazer mais agentes econômicos para esse mercado, o que levará mais usuários aos bitcoins. Ainda, o Bitcoin possui vantagem por ter sido o primeiro, o que leva a um efeito de rede, onde mais usuários possuem maior confiança e valor atribuído ao sistema por já possuir usuários. Vale lembrar que é preciso ter cuidado com este mercado, vários novos criptoativos não foram testados ou sequer possuem utilização.

4.1.7 Políticas Econômicas

³² Para saber mais, acesse: <<https://coinmarketcap.com/alexandria/glossary/non-fungible-token>>.

³³ Para saber mais, acesse: <<https://ethereum.org/en/developers/docs/smart-contracts/>>.

³⁴ Para saber mais, acesse: <<https://ethereum.org/en/defi/>>.

³⁵ Fonte: SIGALOS, MacKenzie; ZHANG, Natalie. How altcoins such as ether captured more and more of the crypto market. CNBC, 2021. Disponível em: <<https://www.cnbc.com/2021/08/06/how-altcoins-such-as-ether-captured-more-and-more-of-the-crypto-market.html>>. Acesso em: 28 ago. 2021.

A moeda é um bem social necessário para a atuação de diversas políticas econômicas. Se o governo perder o controle sobre ela, perderá muito de sua capacidade atuante. Independente de isso ser positivo ou negativo, isto provavelmente não ocorrerá. Pelo fato de que, como veremos posteriormente, o Bitcoin possui muitos entraves para ser usado como meio de troca, inclusive a lei de curso forçado que impede qualquer outra moeda de circular livremente por um país. E para ser um entrave às políticas econômicas, o Bitcoin deveria atuar livremente como meio de troca.

As principais características de uso atual e, possivelmente futuro, são a utilidade como reserva de valor e como ativo de investimento. A função de reserva de valor, algo que o ouro exerce, poderá ser utilizada pelo Bitcoin e os governos poderão incluir em suas reservas, o que não apresentará um problema, mas um sustentáculo para os governos e suas políticas governamentais.

4.2 Reserva de Valor

Um ativo que é caracterizado como reserva de valor é aquele que possui seu valor estável ou crescente ao longo do tempo³⁶. Este tipo serve de *hedge* (proteção) para momentos de crise econômica. O ouro é um exemplo de reserva de valor, como afirma Assaf Neto (2014) de que nos momentos de turbulência é que o ouro se torna uma reserva de valor. Outros ativos podem ser considerados como tal, mas atentaremos ao ouro e ao Bitcoin pelas suas semelhanças, como veremos adiante.

A principal característica que fornece a fundamentação para tornar-se uma reserva de valor, tanto no caso do ouro quanto no do Bitcoin, é a escassez. Ambos possuem isso e o Bitcoin ainda consegue ser superior nesse aspecto, dado que seu limite foi fixado em 21 M BTC, apesar de que isso só ocorrerá em 2140 através de taxas de emissão cada vez menores; enquanto o ouro ainda possui uma taxa de aumento de oferta de cerca de 2% ao ano (AMMOUS, 2018).

Pode ser argumentado que a grande volatilidade do Bitcoin o torna inútil como reserva de valor. Entretanto, a tendência observada até agora com relação ao Bitcoin é de valorização, um poder deflacionário (considerando o aumento do poder de compra)

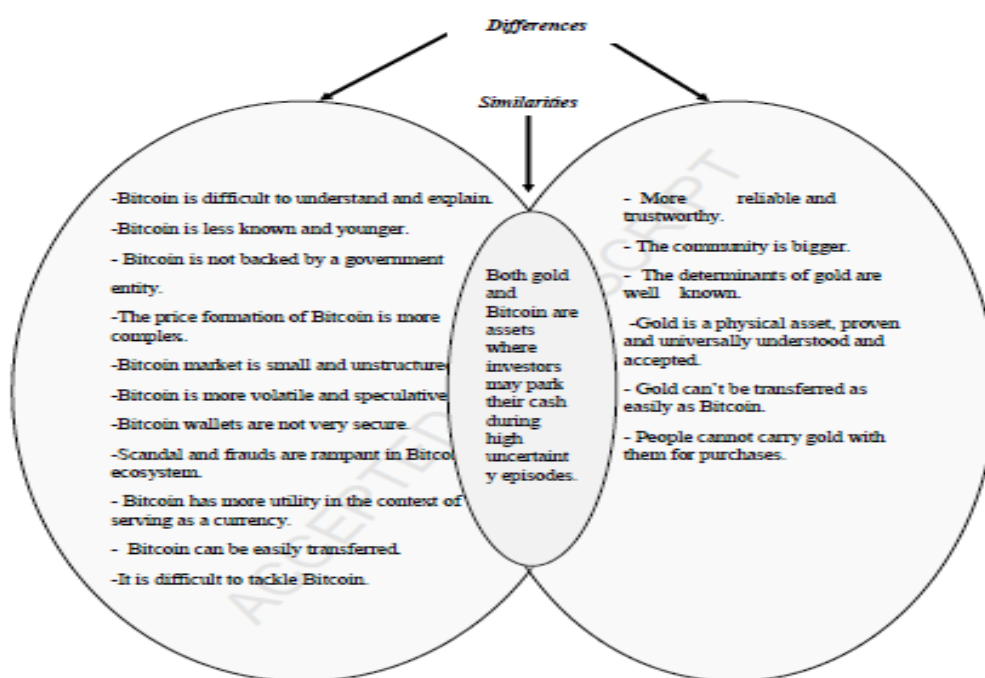
³⁶ DOWNEY, Lucas. Store of Value. Investopedia, 2020. Disponível em: <<https://www.investopedia.com/terms/s/storeofvalue.asp>>. Acesso em: 29 ago. 2021.

muito maior do que qualquer moeda fiduciária (inflacionária), e a questão de reserva de valor refere-se a longos prazos. Ainda, o próprio ouro possui volatilidade, apesar de bem menor.

Dyhrberg (2016a), utilizando de modelo econométrico GARCH e dados de 2010 a 2015, identifica em sua análise sobre o Bitcoin questões concernentes a gerenciamento de risco, análise de portfólio e capacidade de moeda. Principalmente em relação ao preço do ouro e à taxa de câmbio do dólar. Ela identifica que o Bitcoin possui várias similaridades com ambos, dólar e ouro. Segundo a autora, o Bitcoin possui características de meio de troca e de reserva de valor, comportando-se como um intermediário entre o dólar (maiores características de meio de troca) e o ouro (maiores características de reserva de valor). Pelo fato de ser descentralizado e sem regulação, dificilmente se comportará como as moedas atuais. Além disso, o Bitcoin possui várias características que são similares ao ouro, no que concerne à capacidade de *hedge* e reações positivas e negativas de acordo com o noticiário relevante.

Selmi et. al (2018), Dyhrberg (2016b), Shahzad (2019) e Brière et al. (2015) também identificam características de reserva de valor no Bitcoin. Selmi et al. (2018) resumiram as diferenças e similaridade entre o ouro e o Bitcoin:

Figura 3: Resumo de diferenças e similaridades entre ouro e bitcoin.



O ouro possui um histórico consagrado, é amplamente aceito como reserva de valor pelos agentes econômicos, como governos (utilizado largamente por estes como reservas de valor) e investidores, mas existem algumas características em que o Bitcoin é superior. Transações públicas, escassez limitada e não manipulável (existem instrumentos no mercado financeiro, como o *paper gold* (derivativo no mercado de ouro), que não lastreiam em paridade 1 para 1 com o ouro), facilidade de transacionar em longas distâncias (AMMOUS, 2018), divisibilidade e durabilidade maior (ULRICH, 2014). Mas isso também não significa que apenas existirá um ou o outro, os dois podem atuar em conjunto, inclusive como reserva de valor. No momento em que este trabalho é escrito, o Bitcoin possui um valor de mercado de \$ 912,37 M, enquanto o ouro está avaliado em \$ 11,56 T³⁷.

Resumidamente, o Bitcoin é considerado como reserva de valor por alguns agentes econômicos. Isto é fundamentado pelas suas características semelhantes e outras superiores ao ouro, apesar de não chegar ao patamar do ouro no que concerne a essa utilização. Entretanto, o Bitcoin ainda precisa passar pelo teste do tempo, nada garante que ele será de fato usado como tal no futuro, mas podemos inferir que, caso os fundamentos persistam ou melhorem, ele terá essa utilização em maior destaque.

4.3 Ativo pertencente a um Portfólio de Investimentos

A função reserva de valor cabe dentro de um portfólio de investimento, mas veremos outras características relevantes para o pertencimento do Bitcoin neste enquadramento. Muitas pessoas estão apenas interessadas no aspecto de investimento do Bitcoin, e não se preocupam em utilizá-lo como meio de troca; assim surgem as *exchanges* para negociar criptoativos e custodiar no lugar do usuário (ŠURDA, 2012).

Ativo é um recurso econômico em que é esperado que traga algum benefício no futuro, como fluxo de caixa, reserva de valor ou valorização. A Teoria Moderna do Portfólio de Markowitz (1952) fornece uma construção de portfólio usada até hoje. Nela, é visado determinado retorno dado o mínimo de risco possível, ou seja, uma relação risco-

³⁷ Fonte: Infinite Market Cap. Disponível em: <<https://8marketcap.com/>>. Acesso em: 29 ago. 2021.

retorno atraente para o investidor em específico. Basicamente, utiliza-se ativos de correlação e volatilidade diferentes para poder obter um bom portfólio de investimentos.

Selmi et al. (2018) identificaram através de *conditional Value-at-Risk* que o ouro e o Bitcoin servem de proteção (*hedge*) e um bom diversificador em portfólios de investimento contendo ativos relacionados ao petróleo, além de trazerem oportunidades em termos de risco-retorno para o portfólio, apesar de, afirmam, ser possível que essas características não perdurem no tempo.

Sobre a questão de mercado eficiente no caso do Bitcoin, Urquhart (2016) analisou o Bitcoin sob a ótica desta hipótese desenvolvida por Fama (1970). Essa teoria, em suma, afirma que o preço de um ativo representa todas as informações relevantes disponíveis. Urquhart analisou econometricamente dados de 2010 a 2016 e concluiu que o Bitcoin é mercado ineficiente com similaridades a um mercado emergente, dado que é um novo ativo, mas que possui indicativos de aumento de eficiência em seu mercado à medida que os investidores vão aumentando o interesse e aprendendo mais sobre o Bitcoin.

Glaser et al. (2014) analisaram as intenções dos usuários ao adquirir Bitcoin. Eles concluem que a maioria dos que compram bitcoin tem intenção de possuir um ativo, em especial um instrumento de investimento diferente dos ofertados. Shahzad (2019) identifica que o Bitcoin é melhor usado como ativo de diversificação em um portfólio de investimento, dado que suas características de reserva de valor não se aplicam a mercados desenvolvidos.

Kristoufek (2015) identifica o Bitcoin como um ativo de propriedades comuns a outros instrumentos financeiros. O autor identificou que transações, oferta e nível de preços desempenham um papel significativo no preço do Bitcoin em longo prazo, o que condiz com a teoria econômica e monetária mais ortodoxa. Outro fator importante no preço é o interesse em criptoativos pelos investidores; logo, investidores veem no Bitcoin uma forma de entrarem num novo mercado.

Brière et al. (2015) analisaram o Bitcoin como investimento em um portfólio diversificado de 2010 a 2013 utilizando dados do mercado dos Estados Unidos. Eles concluíram que o Bitcoin possui um alto retorno médio, uma baixa correlação com outros ativos e uma alta volatilidade. Ele pode ser considerado um ativo com certo aspecto de

reserva de valor e com ótima utilização quando se trata de portfólio de investimento bem diversificado, aumentando drasticamente o risco-retorno.

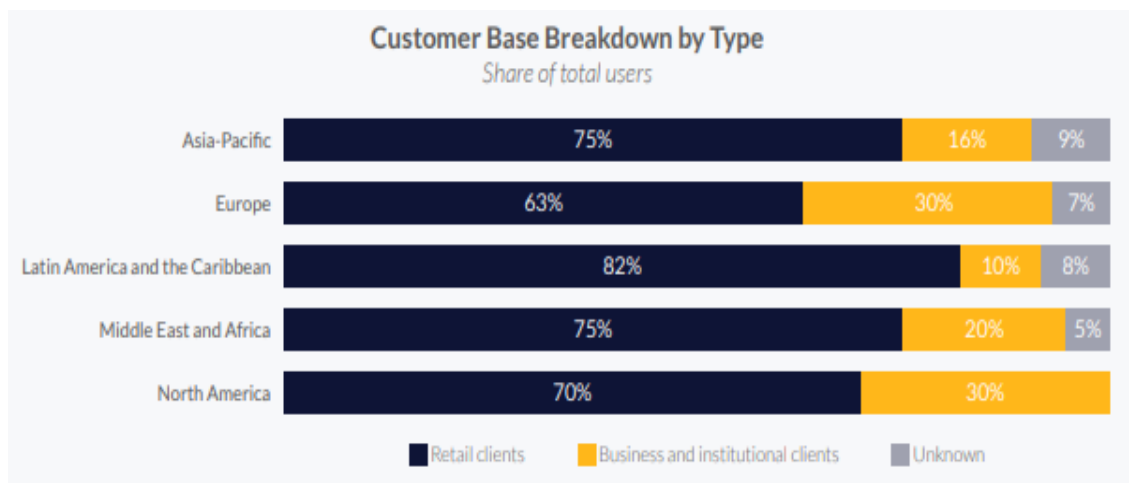
Dyhrberg (2016a) conclui que o Bitcoin possui características intermediárias entre meio de troca e reserva de valor, e, desta forma, é um ativo útil para gerenciamento de portfólio de investimentos, análise de riscos e análise de mercado. Dyhrberg (2016b) analisa a capacidade do Bitcoin de servir de *hedge*, uma das características do ouro, aplicando às ações da bolsa de Londres - *Financial Times Stock Exchange* (FTSE). Ela conclui que o Bitcoin, até o momento da análise, conseguiu servir de *hedge* para o índice da FTSE e demonstrou potencial de *hedge* contra a variação do dólar americano no curto prazo, mas este aspecto não foi conclusivo.

Os estudos apresentados demonstram que o Bitcoin possui características relevantes a serem consideradas em um gerenciamento de portfólio de investimentos, incluindo capacidade de reserva de valor, e não deve ser descartado. O tempo de posse de bitcoins em relação ao total é de 10% acima de 5 anos e de cerca 20% acima de 3 anos³⁸, o que podemos entender como uma maior percepção de reserva de valor e de ativo de investimento, e menos de meio de troca e de ativo especulativo. Existem atualmente instrumentos de investimento envolvendo o Bitcoin, e.g. derivativos, fundos e *ETFs*, o que facilita sua adesão.

Em suma, o Bitcoin é um ativo muito novo e deve passar por várias provas com o passar do tempo. Considerando apenas que possui uma característica de reserva de valor já percebida pelo mercado, apesar de não superar o ouro, ele seria relevante para investimentos. O Bitcoin possui características de correlação e de volatilidade diferentes de vários outros ativos, e.g. ações, o que o torna interessante para a utilização em um portfólio de investimentos. Mas, além disso, considerando características como risco-retorno, o Bitcoin possui um espaço em um portfólio de investimentos, algo que foi identificado por investidores institucionais que estão aumentando sua alocação neste criptoativo.

³⁸ Fonte: Bitcoin: At the Tipping Point. Citibank, 2021. Disponível em: <<https://www.citivelocity.com/citigps/bitcoin/>>. Acesso em: 19 ago. 2021.

Gráfico 9: Divisão dos tipos de usuário de criptoativos em 2020 (Retail: Varejo (usuários comuns); Business and Institutional clientes: Negócios e Clientes institucionais; Unknown: Desconhecido).



Fonte: BLANDIN, Apolline et al. (2020, p. 46).

4.4 Meio de Troca

Um meio de troca é algo que atua como um intermediador entre as transações e, para isso, ele deve possuir algumas características, como portabilidade, reserva de valor e durabilidade. Como foi comentado, o objetivo inicial do criador do Bitcoin era de torná-lo um meio de troca para o mundo digital.

A liquidez do Bitcoin é algo que aumentou consideravelmente desde sua criação, o que é uma característica necessária para atuar como meio de troca eficiente. Mas não possui a mesma liquidez que o dólar ou o euro, por exemplo, constituindo uma adversidade para atuação como meio de troca. O número de transações, como visto no Gráfico 5, aumentou muito desde sua criação, mas isso não confere necessariamente o atributo de meio de troca, sendo mais factível inferir que ocorreu sob os aspectos de especulação e de investimento. Além disso, Bitcoin não serve como unidade de conta, dado que precisa ser amplamente utilizado como meio de troca para isso.

Os pagamentos que ocorrem na rede do Bitcoin são irreversíveis, o que confere um risco para consumidores para fraudes e roubos. Ainda, transfere maior parte da responsabilidade para o usuário. Estes dificultam mais ainda uma possível adoção como meio de troca.

As transações do Bitcoin custam atualmente cerca de 2,39 dólares, mas chegou a custar 60 dólares em 2017³⁹. O que não é alto para transações de grandes quantias, mas um impeditivo para transações cotidianas.

O Bitcoin possui capacidade de melhorar as lentas transações que possui fundamentadas no seu protocolo através do mecanismo de consenso. Isto já ocorre em parte; El Salvador, por exemplo, aceita Bitcoin como meio de troca através de facilitadores de transação e tornou-se o primeiro país do mundo a aceitar como moeda funcional no país⁴⁰. Além disso, existem melhorias que colocam outras camadas de protocolo acima da camada do Bitcoin, como é o caso da *Lightning Network*. Nela, são espalhados pela rede canais de micropagamentos para que ocorram rápidas transações com apenas 1 satoshi – menor unidade do Bitcoin (POON, DRYJA; 2016).

O Bitcoin possui uso crescente como reserva de valor, o que é uma característica anterior à utilização mais ampla como meio de troca. Como Jevons (1875) afirma, o ouro primeiro foi aceito como *commodity* de valor ornamental (algo como a adoção de valor inicial dada pelos primeiros entusiastas do Bitcoin), depois como reserva de valor e terceiro como meio de troca. Se tiverem a possibilidade, as pessoas não escolhem um meio de troca arbitrariamente, mas de acordo com suas melhores características, o que não é o caso ainda do Bitcoin.

Bitcoin também não é dinheiro, caso entendamos dinheiro como um meio de troca amplamente aceito por um número considerável de agentes econômicos. Lentas transações, altos custos e volatilidade são os principais entraves ao Bitcoin tornar-se aceito em maior escala como meio de troca. Porém, não existe uma classificação binária, meio de troca ou não meio de troca, bitcoins atuam como tal, porém em menor grau comparado às moedas fiduciárias, como dólar, libra e euro.

Como comentado anteriormente, o Bitcoin possui adversidades que prejudicam vir a tornar-se mais usado como meio de troca. Ainda, a volatilidade (outro entrave) só diminuirá com a maior adesão ao Bitcoin e o maior entendimento do seu funcionamento, o que é uma questão sem garantias de solução. As lentas transações

³⁹ Fonte: Y charts. Disponível em: <https://ycharts.com/indicators/bitcoin_average_transaction_fee>.

Acesso em: 29 ago. 2021.

⁴⁰ Fonte: Bitcoin: El Salvador makes cryptocurrency legal tender. BBC, 2021. Disponível em: <<https://www.bbc.com/news/world-latin-america-57398274>>. Acesso em: 29 ago. 2021.

podem ser solucionadas com alterações no sistema, assim como os altos custos de transação. Entretanto, caso venham a ser solucionados, alguns governos provavelmente não aceitarão a utilização em larga escala dentro de seus países, como os Estados Unidos, dado que diminuiria seu poder político. Então, é mais factível de imaginar que, de acordo com a características do Bitcoin, ele torne-se um meio de troca mais usado para grandes transações e envolvendo grandes distâncias, dado sua maior eficiência e menores custos relativos de transação nesse quesito. No que concerne a uma possível espiral deflacionária, isso não seria problema caso ele seja mais utilizado como reserva de valor, ativo de investimento e meio de troca para transações específicas, dado que assim atuaria ao lado da moeda fiduciária.

5 CONCLUSÃO

O Bitcoin é um sistema de código aberto e descentralizado a partir de conexões ponto-a-ponto. Em seu protocolo, há a possibilidade de enviar unidades de informação que atuam como moeda, os bitcoins. O Bitcoin gerou a primeira criptomoeda, além de inovações tecnológicas, e.g. *blockchain*, esta que está sendo usado por empresas e governos pelo mundo.

A história do Bitcoin teve (e tem) várias pessoas suportando diretamente através de contribuições técnicas. Para que houvesse progresso científico e tecnológico que ocasionasse no Bitcoin, foi necessário um processo de difusão tecnológica para domínio de tecnologias e de conhecimento anterior; e isso só é possível (dado sua complexidade técnica) com estoque de conhecimento prévio na sociedade e capital humano relevante.

Entretanto, a figura de destaque é a de Satoshi Nakamoto (pseudônimo) que solucionou problemas antigos da computação e uniu distintos campos do conhecimento. Não sabemos se era uma pessoa ou várias, ele sumiu em 2011 e nunca mais retornou. Ao longo de sua história, o Bitcoin sofreu muitos ataques e foi usado por criminosos, mas atualmente está sendo aderido por diversos agentes econômicos, tornando-se algo sério.

O sistema Bitcoin foi criado com vários incentivos para que os agentes que fundamentassem inicialmente, pelos mais diversos motivos, fossem ganhando alguma forma de retorno, como uma parte de propriedade da rede, onde eles possuem vantagens por serem honestos e desvantagens caso tentem subverter o sistema. Isso gerou um ciclo virtuoso de geração de valor à rede que se mantém e atrai mais usuários; tornou-se uma forma de “Equilíbrio de Nash”, onde qualquer mudança de atitude irá piorar a situação do usuário que deixar de contribuir para o Bitcoin.

Vários dos problemas que o Bitcoin sofre são passíveis de melhoria (como o alto uso de energia) ou não afetam apenas a este, mas a outras tecnologias (como a computação quântica). As principais adversidades do sistema são: o uso criminoso, regulação mal executada e como governos encarariam um possível concorrente a suas moedas fiduciárias. O uso criminoso pode ser atenuado através de legislação concernente adequada e de atenção às corretoras de criptoativos, como foi visto, a situação de anônimo

do usuário do Bitcoin não é garantida e a maior parte pode ser rastreada. Caso os governos entendam o Bitcoin como ativo (reserva de valor e investimento para os agentes econômicos), a regulação que atua nele pode ser adaptada para entendê-lo, *de jure*, como tal, dado que a maior parte da legislação atuante sobre o Bitcoin é fígada de outros objetos econômicos. Dito isso, o Bitcoin teria mais incentivo pra permanecer como ativo de investimento e atuar como meio de troca apenas em situações de maiores quantias e longas distâncias, o que provavelmente não afetaria o poder das políticas econômicas.

O Bitcoin teve como objetivo em sua fundação tornar-se meio de troca para o mundo digital, mas está sendo mais usado como reserva de valor e ativo de investimento. Apesar de seu futuro não estar definido totalmente.

Como reserva de valor, foi visto que o Bitcoin possui características similares ao ouro, e este é conhecido pelo mercado como um dos principais ativos de reserva de valor. O Bitcoin possui algumas propriedades melhores que a do ouro e outras piores. Ele já é usado de forma reduzida com tal função, mas ainda precisa de mais história para ser comprovado digno de tornar-se reserva de valor.

Como ativo em um portfólio de investimento é onde o Bitcoin destaca-se. Ele possui várias características que, aliadas a um portfólio bem diversificado, torna-o excelente para alocação. Propriedades como baixa correlação com outros ativos e boa taxa de retorno.

Bitcoin não é dinheiro, no sentido de ser largamente aceito como meio de troca, possui a função meio de troca, mas em baixo grau de utilização. Ainda, possui muitas dificuldades para vir a tornar-se um meio de troca efetivo, porém o sistema permite atualizações que garantam um melhor funcionamento neste aspecto, algo que já está ocorrendo. Os governos perderiam muito do poder de políticas econômicas, então é provável que não permitam o estabelecimento com tal função em larga escala; entretanto, caso venha a tornar-se mais utilizado como meio de troca, é factível imaginar que seja focado em transações não-cotidianas de valores altos e de grandes distâncias, onde possui vantagem competitiva. Além disso, os governos ganhariam mais adotando o Bitcoin dentro do seu sistema financeiro como complementar à moeda fiduciária; o Bitcoin atuaria como meio de troca para grandes transações, reserva de valor, como o ouro, e ativo de investimentos no mercado financeiro.

Dito isso, Bitcoin pode ser classificado como moeda, criptomoeda, e criptoativo. Vale lembrar que ser moeda não significa que tenha todas as funções esperadas de forma perfeita (basta ver o caso recente do bolívar venezuelano⁴¹), mas que possui características melhores ou piores dependendo da moeda em comparação.

Finalmente, considerando que suas características persistirão no futuro, o Bitcoin: (1) possui alguma utilização percebida como reserva de valor e isto deve aumentar no longo prazo; (2) é um ótimo ativo para ser alocado em um portfólio de investimento e tem uma adoção crescente como tal; (3) não é meio de troca relevante e possui muitas dificuldades para atuar como um, poderá ser usado com transações específicas e atuar ao lado de moedas fiduciárias, mas é algo muito incerto.

O Bitcoin trouxe consigo inovações tecnológicas (e.g. *blockchain*), que reverberarão por muito tempo, e novos elementos para economia, a criptomoeda e o mercado de criptoativos. Condicionantes institucionais são necessários para a maior propagação do uso do Bitcoin, como regulação relevante e, conseqüentemente, uma confiança maior (por parte dos usuários que não o conhecem) no seu sistema. Existem muitos percalços a serem superados, mas devemos tentar compreender mais este novo universo de criptoativos, economicamente e tecnologicamente, e não desmerecer sem uma maior análise apenas por ser digital e descentralizado (nem todos são). Apesar de não sabermos com certeza se o Bitcoin em específico persistirá aos desafios que possui ou se será dominante contra os novos concorrentes (criptomoedas privadas, descentralizadas ou estatais (*Central Bank Digital Currency* - CBDC), podemos afirmar que a digitalização do mundo, nas suas mais diversas formas, veio para fazer parte de mais uma etapa da história da civilização humana⁴².

⁴¹ A inflação venezuelana chegou a 9585,5% em 2019 e 2958,8% em 2020. Fonte: In thirteen years Venezuela has eliminated 14 zeroes from the Bolivar currency. MercoPress, 2021. Disponível em: <<https://en.mercopress.com/2021/08/06/in-thirteen-years-venezuela-has-eliminated-14-zeroes-from-the-bolivar-currency>>. Acesso em: 27 ago. 2021.

⁴² Como foi afirmado em um artigo na revista *The Economist*: mesmo que falhe, o Bitcoin deixará marcas no mundo financeiro. Fonte: Mining digital gold. The economist, 2013. Disponível em: <<https://www.economist.com/finance-and-economics/2013/04/13/mining-digital-gold>>. Acesso em: 27 ago. 2021.

REFERÊNCIAS

- AARONSON, Scott. **What Makes Quantum Computing So Hard to Explain?** Quantamagazine, 2021. Disponível em: <<https://www.quantamagazine.org/why-is-quantum-computing-so-hard-to-explain-20210608/>>. Acesso em: 28 ago. 2021.
- ALBUQUERQUE, Bruno Saboia de; CALLADO, Marcelo de Castro. **Understanding Bitcoins: Facts and Questions.** Revista Brasileira de Economia, v. 69, n. 1, p. 3-16, 2015.
- AMMOUS, Saifedean. **The Bitcoin Standard: the decentralized alternative to central banking.** New Jersey: John Wiley & Sons, 2018.
- ASSAF NETO, Alexandre. **Mercado Financeiro.** São Paulo: Atlas, 2014.
- Bitcoin: At the Tipping Point.** Citibank, 2021. Disponível em: <<https://www.citivelocity.com/citigps/bitcoin/>>. Acesso em: 19 ago. 2021.
- Bitcoin: El Salvador makes cryptocurrency legal tender.** BBC, 2021. Disponível em: <<https://www.bbc.com/news/world-latin-america-57398274>>. Acesso em: 29 ago. 2021.
- BLANDIN, Apolline, et al. **3rd Global Cryptoasset Benchmarking Study.** University of Cambridge, 2020. Disponível em: <<https://www.jbs.cam.ac.uk/wp-content/uploads/2021/01/2021-ccaf-3rd-global-cryptoasset-benchmarking-study.pdf>>. Acesso em: 28 ago. 2021.
- BÖHME, Rainer, et al. **Bitcoin: economics, technology, and governance.** The Journal of Economic Perspectives, v. 29, n. 2, p. 213–238, 2015.
- BOYAPATI, Vijay. **The Bullish Case for Bitcoin.** Washington: Vijay Boyapaty, 2021.
- BRIÈRE, Marie, et al. **Virtual Currency, Tangible Return: Portfolio Diversification with Bitcoin.** Journal of Asset Management, v. 16, n. 6, p. 365-373, 2015.
- CALLAWAY, Claudia. **First Bitcoin Swap Proposed.** The National Law Review, 2014. Disponível em: <<https://www.natlawreview.com/article/first-bitcoin-swap-proposed>>. Acesso em: 23 ago. 2021.
- Changes in US Payments Fraud from 2012 to 2016: Evidende from the Federal Reserve Payments Study.** Federal Reserve, 2018. Disponível em: <<https://www.federalreserve.gov/publications/files/changes-in-us-payments-fraud-from-2012-to-2016-20181016.pdf>>. Acesso em: 28 ago. 2021.
- CLARK, Jeremy; NARAYANAN, Arvind. **Bitcoin’s academic pedigree.** Communications of the ACM, v. 60, n. 12, p. 36–45, 2017.
- CLIFFORD, Catherine. **China, Elon Musk raise alarm about bitcoin energy use: Here’s how it could be made more ‘green’.** CNBC, 2021. Disponível em: <<https://www.cnbc.com/2021/06/30/china-musk-raise-alarm-on-bitcoin-energy-use-how-to>>

make-it-greener.html>. Acesso em: 28 ago. 2021.

CONWAY, Luke. **What are the Safest Ways to Store Bitcoin?** Investopedia, 2021. Disponível em: <<https://www.investopedia.com/news/bitcoin-safe-storage-cold-wallet/>>. Acesso em: 24 ago. 2021.

COPPOLA, Frances. **Theft And Mayhem In The Bitcoin World.** Forbes, 2016. Disponível em: <<https://www.forbes.com/sites/francescoppola/2016/08/06/theft-and-mayhem-in-the-bitcoin-world>>. Acesso em: 23 ago. 2021.

CUTHBERTSON, Anthony. **Bitcoin now accepted by 100,000 merchants worldwide.** International Business Times, 2015. Disponível em: <<https://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613>>. Acesso em: 23 ago. 2021.

DAI, Wei. **B-money.** 1998. Disponível em: <<https://nakamotoinstitute.org/b-money>>. Acesso em: 14 ago. 2021.

DOWNEY, Lucas. **Store of Value.** Investopedia, 2020. Disponível em: <<https://www.investopedia.com/terms/s/storeofvalue.asp>>. Acesso em: 29 ago. 2021.

DYHRBERG, Anne H. **Bitcoin, Gold and the Dollar: A GARCH volatility analysis.** Finance Research Letter, v. 16, n. 1, p. 85-92, 2016a.

DYHRBERG, Anne H. **Hedging capabilities of bitcoin.** Is it the virtual gold? Finance Research Letter, v. 16, n. 1, p. 139-144, 2016b.

FAMA, Eugene F. **Efficient Capital Markets: A Review of Theory and Empirical Work.** The Journal of Finance, v. 25, n. 2, p. 383-417, 1970.

FERGUSON, Niall. **A ascensão do dinheiro: a história financeira do mundo.** São Paulo: Editora Planeta do Brasil, 2009.

FISHER, Irving. **The Purchasing Power of Money: its determination and relation to credit, interest and crises.** New York: Macmillan, 1922.

FRANCO, Pedro. **Understanding Bitcoin: cryptography, engineering and economics.** West Sussex: John Wiley & Sons, 2015.

FRANKENFIELD, Jake. **Consensus Mechanism (Cryptocurrency).** Investopedia, 2021. Disponível em: <<https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp>>. Acesso em: 24 ago. 2021.

FROYEN, Richard T. **Macroeconomia: teorias e aplicações.** 2 ed. São Paulo: Saraiva, 2013.

GHIZONI, Sandra K. **Nixon Ends Convertibility of US Dollars to Gold and Announces Wage/Prices Controls.** Federal Reserve History, 1971. Disponível em: <<https://www.federalreservehistory.org/essays/gold-convertibility-ends>>. Acesso em: 24 ago. 2021.

GLASER, Florian, et al. **Bitcoin – Asset or Currency?** Revealing users hidden intentions.

European Conference on Information Systems, v. 22, 2014.

GRAF, Konrad S. **Sobre as Origens do Bitcoin: Estágios da Evolução Monetária – Parte I.** Mises: Revista Interdisciplinar de Filosofia, Direito e Economia, v. 3, n. 2, p. 427-440, 2015.

GRAF, Konrad S. **Sobre as Origens do Bitcoin: Estágios da Evolução Monetária – Parte II.** Mises: Revista Interdisciplinar de Filosofia, Direito e Economia, v. 4, n. 1, p. 121-139, 2016.

In thirteen years Venezuela has eliminated 14 zeroes from the Bolivar currency.

Mercopress, 2021. Disponível em: <<https://en.mercopress.com/2021/08/06/in-thirteen-years-venezuela-has-eliminated-14-zeroes-from-the-bolivar-currency>>. Acesso em: 27 ago. 2021.

IRRERA, Anna; WILSON, Tom. **PayPal to open up network cryptocurrencies.** Reuters, 2020. Disponível em: <<https://www.reuters.com/article/ctech-us-paypal-cryptocurrency-idCAKBN2761L6-OCATC>>. Acesso em: 23 ago. 2021.

JENKINSON, Gareth. **Uma breve história do Bitcoin: 10 anos de altos e baixos.** CoinTelegraph Brasil, 2018. Disponível em: <<https://cointelegraph.com.br/news/a-brief-history-of-bitcoin-10-years-of-highs-and-lows>>. Acesso em: 21 ago. 2021.

Japan Oks recognizing virtual currencies as similar to real money. TheJapanTimes, 2016. Disponível em: <<https://www.japantimes.co.jp/news/2016/03/04/business/tech/japan-oks-recognizing-virtual-currencies-similar-real-money>>. Acesso em: 23 ago. 2021.

JEVONS, William S. **Money and the Mechanism of Exchange.** New York: D. Appleton and Co., 1875.

KHARPAL, Arjun. **Bitcoin value rises over \$1 billion as Japan, Russia move to legitimize cryptocurrency.** Disponível em: <<https://www.cnbc.com/2017/04/12/bitcoin-price-rises-japan-russia-regulation.html>>. Acesso em: 23 ago. 2021.

KRISTOUFEK, Ladislav. **What Are the Main Drivers of the Bitcoin Price?** Evidence from Wavelet Coherence Analysis. Plos One, v. 10, 2015.

LEWIS, Antony. **The Basics of Bitcoin and Blockchain.** Florida: Mango Publishing Group, 2018.

LOPES, João do Carmo; ROSSETTI, José Paschoal. **Economia monetária.** 7 ed. São Paulo: Atlas, 1998.

MARKOWITZ, Harry. **Portfolio Selection.** The Journal of Finance, v. 7, n. 1, p. 77-91, 1952.

Mining digital gold. The economist, 2013. Disponível em: <<https://www.economist.com/finance-and-economics/2013/04/13/mining-digital-gold>>. Acesso em: 27 ago. 2021.

MOSKOV, Alex. **What is the Byzantine Generals Problem?** Coincentral, 2018. Disponível em: <<https://coincentral.com/byzantine-generals-problem/>>. Acesso em: 23 ago. 2021.

NAKAMOTO, Satoshi. **Bitcoin**: a peer-to-peer electronic cash system. 2008. Disponível em: <<https://bitcoin.org/bitcoin.pdf>>. Acesso em: 10 mar. 2021.

NAKAMOTO, Satoshi. **Bitcoin open source implementation of P2P currency**. P2P Foundation, 2009. Disponível em: <<http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>>. Acesso em: 10 mar. 2021.

POON, Joseph; DRYJA, Thaddeus. **The Bitcoin Lightning Network**: scalable off-chain instant payments. 2016. Disponível em: <<https://lightning.network/lightning-network-paper.pdf>>. Acesso em: 18 ago. 2021.

PORZECANSKI, Katia. **Soros says Bitcoin bubble won't have 'Sharp Break' like others**. Bloomberg, 2018. Disponível em: <<https://www.bloomberg.com/news/articles/2018-01-25/soros-says-bitcoin-bubble-won-t-have-sharp-break-like-others>>. Acesso em: 23 ago. 2021.

Proof-of-stake. Ethereum, 2021. Disponível em: <<https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/>>. Acesso em: 1 set. 2021.

RIZZO, Pete. **10 years ago today, Bitcoin creator Satoshi Nakamoto sent his final message**. Forbes, 2021. Disponível em: <<https://www.forbes.com/sites/peterizzo/2021/04/26/10-years-ago-today-bitcoin-creator-satoshi-nakamoto-sent-his-final-message/>>. Acesso em: 22 ago. 2021.

RUBINSTEINN, Gabriel. **Primeiro ETF de bitcoin do Brasil é anunciado e chega à B3 no dia 23**. Exame, 2021. Disponível em: <<https://exame.com/future-of-money/criptoativos/primeiro-etf-de-bitcoin-do-brasil-ja-esta-em-oferta-e-chega-a-b3-no-dia-23/>>. Acesso em: 23 ago. 2021.

SCHMIDT, John. **Bitcoin's Energy Usage, Explained**. Forbes, 2021. Disponível em: <<https://www.forbes.com/advisor/investing/bitcoins-energy-usage-explained/>>. Acesso em: 28 ago. 2021.

SELMI, Refk, et al. **Is Bitcoin a hedge, a safe haven or a diversifier for oil price movements?** A comparison with gold. Energy Economics, v. 74, n. 1, p. 787-801, 2018.

SHAHZAD, Syed J. H., et al. **Is Bitcoin a better safe-haven investment than gold and commodities?** International Review of Financial Analysis, v. 63, n. 1, p. 322-330, 2019.

SHARMA, Rakesh. **Running a Full Bitcoin Node for Investors**. Investopedia, 2021. Disponível em: <<https://www.investopedia.com/news/running-full-bitcoin-node-investors/>>. Acesso em: 24 ago. 2021.

SHEN, Samuel; GALBRAITH, Andre. **Proibição da China faz mineradores se voltarem para o exterior**. Reuters, 2021. Disponível em: <<https://www.reuters.com/article/tech-china-bitcoin-idBRKCN2E11RA-OBRIN>>. Acesso em: 24 ago. 2021.

SIGALOS, MacKenzie; ZHANG, Natalie. **How altcoins such as ether captured more**

and more of the crypto market. CNBC, 2021. Disponível em: <<https://www.cnn.com/2021/08/06/how-altcoins-such-as-ether-captured-more-and-more-of-the-crypto-market.html>>. Acesso em: 28 ago. 2021.

ŠURDA, Peter. **Economics of Bitcoin:** is Bitcoin an alternative to fiat currencies and gold? WU Vienna University of Economics and Business, 2012. Disponível em: <<https://nakamotoinstitute.org/static/docs/economics-of-bitcoin.pdf>>. Acesso em: 18 ago. 2021.

SWAN, Melanie. **Blockchain:** blueprint for a new economy. California: O'Reilly Media, 2015.

SZABO, Nick. **Bit Gold.** 2005. Disponível em: <<https://nakamotoinstitute.org/bit-gold>>. Acesso em: 14 ago. 2021.

TOLOTTI, Rodrigo. **O que é o halving do Bitcoin e como ele afeta o mercado da criptomoeda.** Infomoney, 2020. Disponível em: <<https://www.infomoney.com.br/mercados/o-que-e-o-halving-do-bitcoin-e-como-ela-afeta-o-mercado-da-criptomoeda/>>. Acesso em: 26 ago. 2021.

ULRICH, Fernando. **Bitcoin:** a moeda na era digital. São Paulo: Instituto Ludwig von Mises Brasil, 2014.

URQUHART, Andrew. **The inefficiency of Bitcoin.** Economic Letters, v. 148, n. 1, p. 80-82, 2016.

VARIAN, Hal R. **Microeconomia:** uma abordagem moderna. 9 ed. Rio de Janeiro: Elsevier, 2016.

VELDE, François R. **Bitcoin:** A primer. Chicago Fed Letter, v. 317, n. 1, p. 1-4, 2013.

WALLACE, Benjamin. **The rise and fall of Bitcoin.** Wired, 2011. Disponível em: <<https://www.wired.com/2011/11/mf-bitcoin/>>. Acesso em: 12 ago. 2021.

WICKSELL, Knut. **Interest and Prices:** a study of the causes regulating the value of money. New York: Sentry Press, 1936.