

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
FACULDADE DE ECONOMIA, ADMINISTRAÇÃO, CONTÁBEIS E
ATUARIAIS

JOÃO VICTOR GARCIA COSTA E SILVA

ANÁLISE SOBRE A EVOLUÇÃO DO MERCADO DE CRIPTOMOEDAS E AS
PERSPECTIVAS DE TAXAÇÃO

SÃO PAULO

2024

JOÃO VICTOR GARCIA COSTA E SILVA

**ANÁLISE SOBRE A EVOLUÇÃO DO MERCADO DE CRIPTOMOEDAS E AS
PERSPECTIVAS DE TAXAÇÃO**

Monografia apresentada à banca examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para obtenção do título de bacharelado em **Ciências Econômicas**, sob a orientação do Prof., Dr. **Antônio Corrêa de Lacerda**.

SÃO PAULO

2024

Dedico esta monografia à Pontifícia
Universidade Católica de São Paulo, aos meus
professores, familiares e amigos.

AGRADECIMENTOS

Aos meu pais, Lilian Uglar Garcia e Luiz Eduardo Costa e Silva, que sempre me apoiaram durante essa graduação.

A minha irmã, Maria Luiza Garcia Costa e Silva, por estar sempre me aconselhar da melhor forma e apoiar as minhas ideias.

Ao meu irmão mais novo, Luiz Antônio de Carvalho Fernandes Costa e Silva, por sempre estar do meu lado.

Ao meu grande amigo, Murilo Duarte de Melo, por sempre estar presente em grandes momentos da minha vida e pelo apoio durante essa graduação.

A minha família e amigos, cujo amor inabalável e as experiências compartilhadas enriquecem a minha jornada pessoal.

*"O sucesso é a soma de pequenos esforços
repetidos dia após dia."*

Robert Collier

RESUMO

A presente monografia tem como objetivo mostrar o impacto das criptomoedas no mercado financeiro global, com foco principal no Bitcoin. Primeiramente contextualiza o aumento das criptomoedas desde o surgimento do Bitcoin em 2009, mostrando sua relevância como alternativa ao sistema financeiro convencional. Em seguida, explica-se a tecnologia base, a Blockchain, e suas características, e também outras tecnologias ligadas ao sistema financeiro de criptoativos. Posteriormente, a monografia mostra como foi a evolução da tributação dos ativos digitais no país, contando toda a história do imposto de renda e sua relação esses ativos. Ao final, são apontadas as conclusões resultantes dessa pesquisa, mostrando as perspectivas futuras das moedas no cenário econômico mundial, os desafios que as criptomoedas representam para as políticas de regulamentação e para o mercado financeiro.

Palavras-chave: Criptomoedas. Criptoativos. Moedas Digitais. Bitcoin. Blockchain. Mercado Financeiro. Tecnologia Digital. Tributação.

ABSTRACT

This dissertation aims to explore the impact of cryptocurrencies on the global financial market, with a primary focus on Bitcoin. It begins by contextualizing the rise of cryptocurrencies since Bitcoin's emergence in 2009, illustrating its relevance as an alternative to the conventional financial system. Subsequently, it elucidates the foundational technology, blockchain, and its characteristics, along with other technologies associated with the cryptocurrency financial system. Moreover, the monograph illustrates the evolution of digital asset taxation in the country, narrating the entire history of income tax and its relationship with these assets. Finally, it presents the conclusions drawn from this research, outlining the future prospects of cryptocurrencies in the global economic landscape and the challenges they pose to regulatory policies and the financial market.

Keywords: Cryptocurrencies. Cryptoasse. Digital Currencies. Bitcoin. Blockchain. Financial Market. Digital Technology. Taxation.

LISTA DE GRÁFICOS

Gráfico 1 Histórico do Bitcoin (2014-2024)	14
Gráfico 2 Número de criptomoedas a cada ano (2013-2024).....	16
Gráfico 3 Evolução do Ethereum (2015-2024).....	16
Gráfico 4 Volatilidade do Bitcoin (2017-2023).....	18
Gráfico 5 Transações do Bitcoin (2017-2022).....	19
Gráfico 6 Transações do Ethereum (2017-2022).....	20
Gráfico 7 Dificuldade de mineração do Bitcoin (2011-2024).....	21
Gráfico 8 Número de carteiras de criptomoedas em milhões (2016-2023).....	24

SUMÁRIO

INTRODUÇÃO	10
1. MERCADO DE CRIPTOATIVOS.....	12
1.1 O BITCOIN	12
1.2 PEER- TO-PEER (P2P).....	14
1.3 ALTCOINS.....	15
1.3.1 VANTAGENS E DESVANTAGENS DAS ALTCOINS	17
2 BLOCKCHAIN	18
2.1 O QUE É BLOCKCHAIN?	18
2.2 MINEIRAÇÃO DE BITCOIN	21
2.3 TIPOS DE BLOCKCHAIN	22
2.4 SEGURANÇA NO SISTEMA BLOCKCHAIN	22
2.5 PERIGOS DA BLOCKCHAIN	23
3 FUTURO DAS CRIPTOMOEDAS E A TAXAÇÃO	24
3.1 TRIBUTAÇÃO NO BRASIL.....	24
3.2 FUTURO DAS CRIPTOMOEDAS	27
CONCLUSÃO.....	28
REFERÊNCIAS.....	29

INTRODUÇÃO

Nas últimas décadas o mercado financeiro tem passado por uma transformação significativa, resultado da globalização econômica e do avanço das tecnologias digitais. O surgimento das criptomoedas é uma das inovações mais marcantes nesse cenário. Desde o lançamento do Bitcoin em 2009, esses ativos digitais tem ganhado uma grande importância, tanto como ferramenta para transações quanto como opção de investimento. A anonimidade, segurança e descentralização que as criptomoedas proporcionam acabam transformando-as em uma opção atraente ao sistema financeiro tradicional.

O aumento do interesse e da utilização das criptomoedas destacam a necessidade de estudos aprofundados de como elas funcionam, quais são seus riscos e quais são seus benefícios. Além disso, a dificuldade de criar uma regulamentação em muitos países e a volatilidade do mercado de criptoativos acabam levantando preocupações sobre a segurança e estabilidade financeira.

As criptomoedas oferecem uma forma nova para se transferir valor, o que acaba desafiando os sistemas bancários e cria novos paradigmas financeiros. A tecnologia Blockchain, que é o sistema que sustenta as moedas digitais, garante transações seguras e transparentes, mas também abre uma porta para a criação de contratos inteligentes, que podem ser utilizados para lavagem de dinheiro e a evasão fiscal. Dessa forma, a análise das criptomoedas é um assunto importante para investidores, legisladores, economistas e o público em geral.

Considerando o importante tema levantado, o objetivo principal deste trabalho é analisar o impacto das criptomoedas no mercado financeiro, com um foco particular no caso do Bitcoin. Para chegar a este objetivo a presente monografia será dividida em três capítulos, além da introdução e da conclusão.

O Primeiro capítulo mostra o histórico e a evolução do mercado de criptomoedas, contando desde o surgimento do Bitcoin até o desenvolvimento de outras principais moedas do mercado. Esta parte da monografia explora os marcos históricos mais importantes e conta sobre como a adoção e a popularidade das moedas digitais cresceram ao longo do tempo.

O Segundo capítulo tem o foco voltado para a tecnologia que está por trás das criptomoedas, explorando com detalhes o funcionamento da Blockchain, suas principais características e as inovações tecnológicas mais recentes. Além disso, o capítulo também mostra

outras tecnologias ligadas ao Blockchain que ajudam a sustentar o ecossistema dos criptoativos, apontando uma visão abrangente sobre os fundamentos técnicos.

O Terceiro e último capítulo é voltado para examinar a tributação de criptoativos no Brasil e qual é o possível futuro para esse mercado. É apresentado a evolução das leis tributárias em resposta do aumento na utilização de moedas digitais e aponta qual o papel das grandes empresas nesse setor. O capítulo enfatiza a importância de criar regulamentações eficazes para uma melhora do mercado de ativos digitais.

1 MERCADO DE CRIPTOATIVOS

Este capítulo está presente na pesquisa para dar um norte a ela, mostrando a trajetória das criptomoedas desde o início e falando um pouco sobre alguns tópicos importantes para o tema. O capítulo está dividido em três tópicos: O primeiro tópico conta como foi o início do mercado de criptoativos e mostra toda a história da moeda principal do mercado; O segundo tópico conta um pouco do sistema Peer-to-Peer e como ele é importante para o mundo de criptoativos; E o Terceiro fala um pouco sobre as altcoins e o porquê delas serem uma alternativa mais viável.

1.1 O BITCOIN

Muitos acreditam que as criptomoedas só apareceram agora, mas a ideia de criar uma moeda digital apareceu primeiro em 1982. Foi quando o cientista da computação David Chaum¹ surgiu com o conceito de e-Cash. Já no início da década de 1980, Chaum estava preocupado com a privacidade no mundo digital e publicou um artigo intitulado "Assinaturas cegas para pagamentos não rastreáveis"(Chaum,1983), detalhando uma nova forma de criptografia que, segundo ele, permite a implementação de um sistema de pagamento automatizado sem que terceiros vejam a informação de pagamento. Chaum tentou colocar em prática a ideia de criar um sistema de assinatura cega criando o DigiCash em 1990. A DigiCash, uma empresa fundada em Amsterdã, foi projetada como o Bitcoin, para ser uma moeda online segura. A reputação de Chaum de ser inteligente o suficiente atraiu funcionários e capitalistas de risco, mas o produto em si nunca pegou e, no final da década de 1990, o DigiCash faliu.

Mesmo com o fim do DigiCash, Chaum abriu portas para outras pessoas com visões semelhantes. Em 1997, o criptografo e cypherpunk² britânico Adam Back criou o Hashcash, um sistema “prova de trabalho” (Proof-of-work) que é muito semelhante ao que o Bitcoin usa.

Em 1998, surgiram duas ideias de criptomoedas. A primeira foi no final do ano, onde Wei Dai publicou um ensaio mostrando a sua ideia chamada de “B-Money”, uma criptomoeda cuja troca era muito parecida a Blockchain do Bitcoin. E logo depois o Nick Szabo divulgou

¹ David Lee Chaum é um inventor, cientista da computação e um criptografo. O cientista possui um PHD em ciências da computação pela Universidade de Berkeley e é reconhecido por ser o inventor do dinheiro digital. Chaum também possui trabalhos que foram fundamentais na inovação da criptografia, como por exemplo sistemas de votação seguros.

² Cypherpunk é o termo utilizado para ativistas do mundo da tecnologia. Esses indivíduos defendem o uso da tecnologia como uma forma de liberdade de expressão. Em 1993 o matemático Eric Hughes, conhecido por ser um dos fundadores do movimento, escreveu o chamado “manifesto Cypherpunk”, que contava como o uso da tecnologia unia as pessoas

uma proposta parecida, a “Bit Gold”, que seria uma moeda alternativa que não precisa de um terceiro para administrar(Szabo,1998). Por interessante que as duas ideias pareçam nenhuma delas se concretizou.

Em 2008, devido ao estouro de uma bolha imobiliária nos EUA, causada pelo aumento nos valores dos imóveis que não foi acompanhado pelo crescimento da renda da população, o mercado financeiro mundial sentiu o impacto da crise, sendo considerada a pior desde a Grande depressão de 1929.

Após esse grande marco do mercado financeiro as criptomoedas começaram a aparecer, sendo a primeira delas o Bitcoin. A principal ideia era criar um tipo de moeda digital descentralizada em uma rede Blockchain a partir de sistemas avançados de criptografia que fosse uma alternativa para as moedas tradicionais, sendo assim uma revolução monetária onde não existe controle de emissão e registro de transações.

O Bitcoin foi registrado em agosto de 2008, e em outubro do mesmo ano uma pessoa que usava o nome Satoshi Nakamoto, que é considerado o criador da moeda, publicou um artigo científico intitulado “Bitcoin: A Peer-to-Peer Electronic Cash System” (Nakamoto,2008), conhecido no mundo dos criptoativos como o “Whitepaper de Satoshi”³. O artigo falava sobre o conceito da tecnologia Blockchain criptográfica e descrevia a moeda como um recurso digital teórico de código aberto, que significa que ninguém o tinha e que todos podem participar no seu desenvolvimento e utilização.

O primeiro bloco do Bitcoin ficou conhecido como Bloco Genesis, e foi extraído no início de 2009. Em 9 de janeiro, a primeira inteiração do software Bitcoin foi lançada e poucos dias depois ocorreu a primeira transação da moeda, onde Nakamoto mandou 10 Bitcoins para o desenvolvedor e programador Hal Finney. Ao final do mesmo ano, o New Liberty Standard publicou a primeira taxa de câmbio da história da promissora criptomoeda, considerando US\$1 valiam 1.309 Bitcoins.

Depois que a taxa de câmbio foi definida, foi apenas uma questão de tempo até que alguém tentasse fazer uma compra real com o Bitcoin. Em maio de 2010, aconteceu, o programador Laszlo Hanyecz, da Flórida, enviou 10.000 Bitcoins para um homem em Londres em troca de duas pizzas no valor total de US\$ 25. Isso ainda torna o Bitcoin uma fração de seu valor, mas através da compra, as partes envolvidas veem o potencial do produto. Alguns meses

³ O termo “Whitepaper”, é utilizado para um documento informativo que mostra uma análise mais aprofundada sobre certo assunto. O livro “Bitcoin: A Peer-to-Peer Electronic Cash System” é considerado um whitepaper pois descreve como funciona a moeda com o intuito de incentivar as pessoas a usá-lo.

depois, o valor do Bitcoin finalmente quebrou o limite do centavo e a partir de 2014 começou a ganhar atenção no mercado (gráfico 1).

GRAFICO 1
EVOLUÇÃO DO BITCOIN (2014-2024)



FONTE: COINMARKETCAP(2024)

À medida que o Bitcoin cresceu em popularidade, as primeiras criptomoedas alternativas também surgiram durante esse período. Chamadas de “Altcoins”, essas tem tópicos principais melhorar o design original do Bitcoin, oferecendo maior velocidade, anonimato ou alguma outra vantagem. As primeiras moedas foram Namecoin e Litecoin. Atualmente, existem mais de 1.000 criptomoedas em circulação e novas estão surgindo com alta frequência.

1.2 PEER- TO-PEER (P2P)

O termo Peer-to-Peer (P2P), ou ponto a ponto, é muito importante tanto no contexto mercado de criptomoedas quanto para o mundo tecnológico. Em uma rede P2P, cada usuário tem seu papel como nó igualitário, ou seja, trabalham juntos para sustentar uma rede sem necessidade de depender de um servidor central. Isso oferece uma maneira descentralizada de compartilhar recursos e informações.

No mundo dos criptoativos, a Blockchain é grande exemplo do termo P2P. Todas as transações de criptomoedas são verificadas e registradas pelos usuários da rede, sem depender de um banco por exemplo, que seria uma autoridade central. Cada nó da Blockchain possui uma cópia do registro, que ajuda na transparência e segurança (Nakamoto,2008).

Além disso, o P2P também é utilizado no processo de negociação de moedas digitais. Em transferências P2P, os participantes negociam diretamente com outros, sem a necessidade de uma corretora de investimentos ou uma bolsa de valores. Com isso, os usuários são livres, permitindo que eles negociem os seus próprios termos e no final acabam evitando taxas de corretagem

Um item importante dessa plataforma é o catálogo P2P, onde os compradores de criptoativos encontram uma grande variedade de vendedores que estão dispostos a negociar. Esse catálogo possui uma interface que facilita a procura por produtos e vendedores, além recursos como informações sobre taxas, transações que já foram confirmadas e avaliações de vendedores para não cair em golpes.

No entanto, a negociação através do P2P possui seus próprios defeitos. A falta de uma organização ou um órgão intermediador confiável faz com os participantes tenham que confiar entre si para fechar transações de uma forma segura e justa. Levando em conta que no ambiente o anonimato é comum, a chance de dar algum problema é grande, aumentando assim os riscos de fraude e golpes.

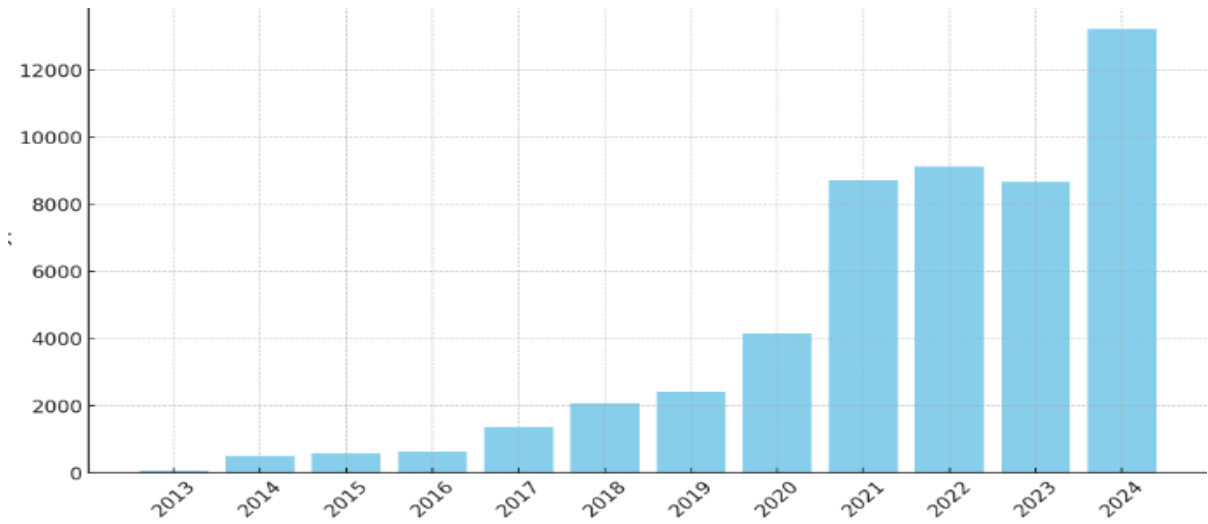
Para diminuir esses riscos, surgiram plataformas P2P onde são dedicadas para facilitar a transação entre usuários. Essas plataformas oferecem uma camada de proteção adicional proporcionando um ambiente mais regulado e seguro para todos os seus participantes.

Essa forma direta e descentralizada para realizar transações de criptoativos mostra uma modificação significativa quando comprado com os modelos tradicionais de negociação. Apesar de apresentar alguns desafios, o modelo P2P aparece como uma maneira flexível e inovadora, proporcionando uma alternativa mais acessível aos mercados financeiros.

1.3 ALTCOINS

No amplo espaço de criptomoedas, o Bitcoin foi primeiro ativo. Claro, também assumiu a posição número um em valor de mercado e se estabeleceu como um revolucionário em 2009. No entanto, existem milhares das mais diversas moedas digitais por aí. Considerados uma "alternativa" aos principais ativos de criptomoedas do mercado, eles são frequentemente chamados de Altcoins pela comunidade de criptomoedas e a cada ano aparecem mais (Gráfico 2).

GRÁFICO 2
NUMERO DE CRIPTOMOEDAS A CADA ANO (2013-2024)



FONTE: COINMARKETCAP 2024

Dados do CoinMarketCap de 2024 mostram que, além de ativos digitais e outras criptomoedas, existem mais de 12.000 criptoativos no mercado (CoinMarketCap, 2024).

Dentre todas as moedas criadas após o Bitcoin uma é conhecida por ser a mais inovadora e por ser a maior altcoin por capitalização de mercado, o Ethereum. Após o seu lançamento a moeda ganhou força e conquistou o seu lugar no mercado (Gráfico 3).

GRÁFICO 3
EVOLUÇÃO DO ETHEREUM (2015-2024)



FONTE: COINMARKETCAP 2024

Como é um produto criado após o Bitcoin, aliado à modernização da tecnologia, eles possuem maior velocidade de transação, criando assim uma maior demanda de mercado. Além disso, essas criptomoedas alternativas são mutáveis devido a melhorias em algoritmos, ferramentas ou proporcionando aos usuários maior segurança digital, o que é, em suma, um recurso aplicável que atrai a atenção da maioria dos investidores.

Mas um fator importante para o sucesso das Altcoins foi o declínio na mineração de Bitcoin, o processo de produção e retirada de criptomoedas. A criptomoeda mais famosa do mundo foi suspensa pela China, atormentada por preocupações ambientais devido ao uso de carbono em sua mineração. Outro ponto é que as autoridades chinesas afirmam que as criptomoedas causam caos econômico e facilitam transferências ilícitas de ativos e lavagem de dinheiro. Esse fator torna as altcoins uma opção viável, enquanto o Bitcoin busca energia renovável para sua produção.

1.3.1 VANTAGENS E DESVANTAGENS DAS ALTCOINS

As Altcoins possuem um modelo operacional próprio, utilizando um sistema diferente do Blockchain que permite rastrear o envio e recebimento de informações na internet. Outra questão é que as Altcoins podem ser negociadas a preços mais baixos ou oferecer maiores ganhos futuros.

Outro ponto é que certos tipos de Altcoins são baseados em tecnologia diferente do Bitcoin, chamados “Stablecoins”⁴. Algumas Stablecoins são até emparelhadas com o dólar americano, o que aumenta o poder das Altcoins e garante maior segurança aos investidores.

No entanto, os riscos associados ao investimento em Altcoins estão relacionados à falta de regulamentação, o que pode prejudicar a liquidez do investimento. Além do mais, os ativos digitais tem grandes flutuações em seu valor em curto período (Gráfico 4).

⁴ São moedas projetadas para manter um valor estável, normalmente esse tipo de ativo digital é associado a uma moeda já existente como o dólar americano. Essas moedas são uma alternativa menos volátil para realizar operações e contratos inteligentes na tecnologias Blockchain.

GRÁFICO 4
VOLATILIDADE BITCOIN (2017-2023)



FONTE: TRADINGVIEW 2023

Como é possível observar no gráfico o Bitcoin possui uma alta volatilidade, basta observar o ano de 2020, a moeda teve uma desvalorização significativa em um curto período e no começo de 2021 começou a se reerguer. Por um lado, é bom porque a volatilidade cria a sensação de que as criptomoedas podem trazer riqueza em um curto período, permitindo que elas cresçam e se valorizem. Por outro lado, gera ansiedade e dúvida ao investir dinheiro em ativos voláteis.

2 BLOCKCHAIN

Depois de apontar alguns dos principais pontos sobre a maior moeda do mercado digital é importante explicar como funciona o sistema por trás dela. Nesse segundo capítulo será explicado o que é o Blockchain, como ele funciona, quais são os seus tipos e quais os riscos desses sistemas.

2.1 O QUE É BLOCKCHAIN?

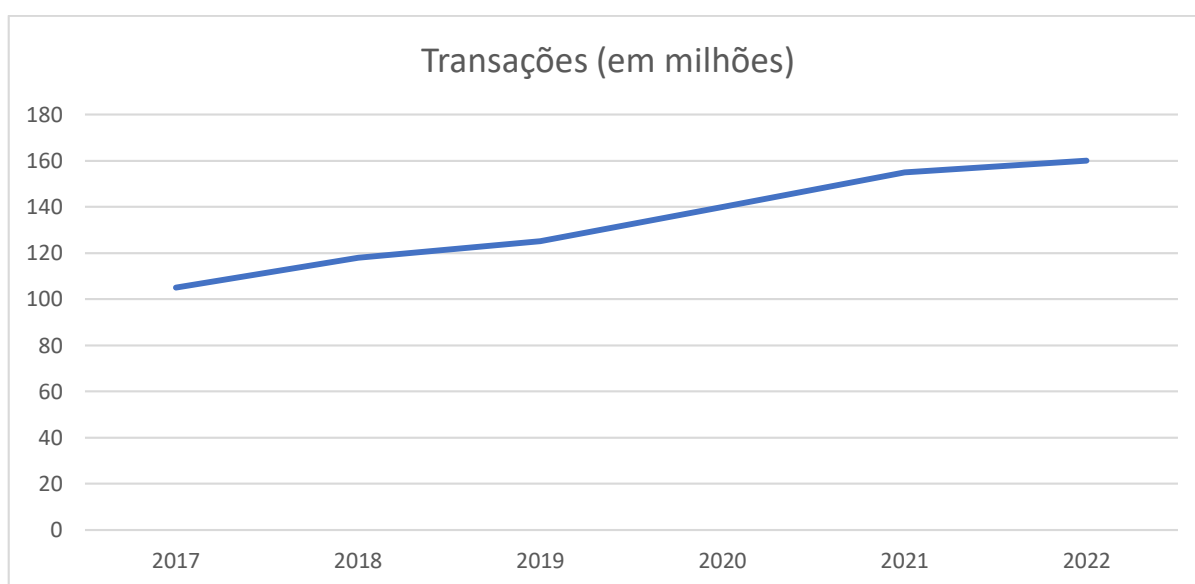
A Blockchain é considerada uma inovação revolucionária no mundo da tecnologia, representando um avanço importante na transparência de transações digitais. Em sua essência,

a Blockchain seria uma forma de livro-razão, composto por uma cadeia continua de blocos interligados. Essa tecnologia permite que todas as transações sejam gravadas de forma segura. (Antonopoulos, 2017).

Diferente dos bancos de dados tradicionais centralizados, onde todas as informações são armazenadas e controladas por uma entidade, esse sistema de Blockchain utiliza uma rede descentralizada de computadores, que são conhecido como “nós”. Cada nó desse sistema possui uma cópia do livro-razão, e isso garante que todas as transações seja verificadas uma por uma e validadas por múltiplos participantes. Com isso, acaba aumentando a segurança e a resistência da rede a ataques sem a necessidade de confiar em uma única autoridade.

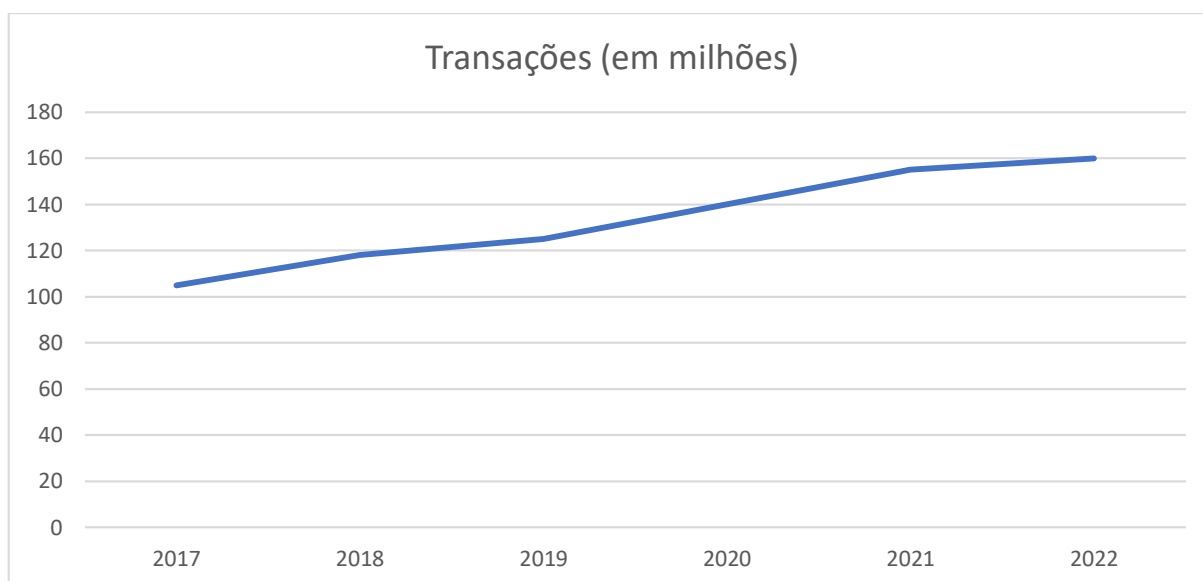
Uma característica única do sistema é a sua imutabilidade. Isso significa que uma vez que a transação foi realizada e registrada em um bloco, ela não pode ser alterada ou removida, tornando-se permanente na Blockchain. Com isso, a confiabilidade e integridade dos dados armazenados estão garantidos no sistema, transformando-o em uma solução confiável para uma grande variedade de aplicações. Ao longo dos anos as transações na Blockchain vem aumentando rapidamente, isso é possível analisar nos próximos dois gráficos relacionados as transações das duas maiores moedas do mercado, o Bitcoin e o Ethereum (Gráficos 5 e 6).

GRÁFICO 5
TRANSAÇÕES DO BITCOIN(2017-2022)



FONTE:DADOS RETIRADOS DO BLOCKCHAIN.COM

GRÁFICO 6
TRANSAÇÕES DO ETHEREUM(2017-2022)



FONTE:DADOS RETIRADS DO ETHERSCAN.IO

De acordo com os seus usuários, a Blockchain é transparente por natureza. Todas as transações que são registradas nos blocos são acessíveis e visíveis para todas as pessoas da rede. Isso faz com que a confiança aumente, pois qualquer usuário pode verificar transações e garantir sua legitimidade.

Como uma forma de afirmar a segurança da rede, o sistema usa algoritmos de consenso, sendo o mais tradicional o “Proof-of-Work”⁵. Esse tipo de algoritmo monta etapas para organizar as informações que são recebidas para depois serem validadas, diminuindo assim a chance de ataques cibernéticos.

Paralelamente à Blockchain, os “smart contracts”, ou contratos inteligentes, fazem parte de uma inovação importante para esse sistema. Esses contratos inteligentes são programas autônomos armazenados na Blockchain que automaticamente entram em ação quando determinadas condições predefinidas são cumpridas. Esses contratos possibilitam a automatização de acordos, deixando de lado a necessidade de intermediários. Além disso, os smart contracts possuem vasta possibilidade de aplicações em setores diversos, como saúde, imobiliário, logística e finanças (Antonopoulos, 2017).

⁵ Em 1993, Moni Naor e Cynthia Dwork postaram um artigo com o objetivo de mostrar uma nova forma de combater o spam utilizando funções vinculadas a memória. Essa ideia inspirou o conceito de Proof of Work utilizado em blockchains.

2.2 MINEIRAÇÃO DE BITCOIN

A mineração na Blockchain vem sendo um ponto essencial desde os primeiros dias desse sistema. No começo, apenas utilizando um computador doméstico era possível minerar, mas com o aumento da popularidade das moedas digitais, a atividade acabou se tornando ainda mais competitiva e complexa. Hoje em dia, essa atividade está dominada por grandes grupos conhecidos como fazendas de mineração, que usam e abusam de equipamentos específicos para minerar a maior quantidade de moedas em um curto período.

A mineração na Blockchain está interligada diretamente com o mecanismo de consenso Proof-of-Work. De acordo com o que está escrito no “White Paper do Bitcoin”, a mineração se baseia na resolução de cálculos complexos para conseguir validar transações e assim adicionar novos blocos à cadeia (Nakamoto, 2008). Essa atividade requer um alto consumo de energia e um alto nível de computadores. No próximo gráfico é possível perceber que no começo do Bitcoin a mineração era acessível, mas foi se dificultando ao longo da valorização da moeda (Gráfico 7).

GRÁFICO 7
DIFICULDADE DE MINEIRAÇÃO DE BITCOIN (2011-2024)



FONTE:BITBO.IO

No gráfico, a linha verde significa o valor da moeda, enquanto a linha marrom mostra a dificuldade de mineração. De 2011 até 2017, é possível reparar que a dificuldade não teve uma diferença na mineração da moeda. No entanto, a partir de 2018, com sua popularização, acontece um alto crescimento na dificuldade de mineração que acaba igualada ao seu preço em 2024.

Com o aumento da dificuldade dos cálculos exigidos em cada operação e o crescente número de mineradores, a mineração acabou se transformando em trabalho especializado e de

alto investimento. Hoje em dia, fazendas de mineração são comuns e juntam milhares de máquinas que trabalham para aumentar as chances de pegar recompensas associadas a novos blocos do sistema.

Além disso, a mineração da Blockchain não está limitada somente para o Bitcoin. Existem muitas outras moedas que utilizam o método de mineração como forma de garantir a segurança e validar suas transações.

2.3 TIPOS DE BLOCKCHAIN

No mercado de criptomoedas existem vários modelos de Blockchain, mas elas podem ser divididas principalmente entre duas categorias: privadas ou públicas.

Com o alta popularização das moedas, poderes centralizados, como empresas e governos, tem explorado a tecnologia Blockchain. Alguns deles estão optando por implementar sistemas de Blockchain privadas, e isso acaba indo totalmente contra a ideia inicial do sistema pois controla quem pode utilizá-la.

Os sistemas de Blockchains públicos são denominados dessa jeito pois são abertas para todos os participantes. Desta forma, todas as transações que acontecem neste sistema são visíveis para todos os seus usuários e não existe nenhuma autoridade central para regular qualquer tipo de informação. De acordo com Nakamoto(2008) no white paper, essas Blockchains visam a descentralização e a transparência total.

2.4 SEGURANÇA NO SISTEMA BLOCKCHAIN

A segurança da tecnologia Blockchain está diretamente associada a maior parte do número e da distribuição de servidores conectados ao sistema. Isso acontece pois quanto maior o número de servidores que estão conectados, mais difícil será o trabalho dos invasores para comprometer a estrutura da rede. Na Blockchain do Bitcoin por exemplo, todos os blocos estão vinculados uns aos outros, formando uma cadeia continua que dificulta qualquer tipo de invasão (Antonopoulos, 2017).

Esse sistema garante que para ocorrer qualquer tipo de alteração de um bloco pedirá a modificação de todos os outros blocos seguintes, o que é praticamente impossível pois seria necessário um poder computacional gigante.

A descentralização do sistema também ajuda, como todas as transações são registradas publicamente, isso acaba montando uma camada de segurança a mais. Com essa estrutura é

possível ter auditorias contínuas e a rápida detecção de atividades relacionadas a fraude, contribuindo assim para a confiança no sistema Blockchain.

2.5 PERIGOS DA BLOCKCHAIN

Apesar da tecnologia Blockchain ser inovadora, ela não está totalmente segura contra riscos e ataques. Uma das principais ameaças é o “ataque 51%”, que acontece quando um grupo ou uma organização de mineradores toma mais da metade do poder computacional do sistema. Caso isso aconteça, os invasores tem o poder de mudar partes da Blockchain, conseguindo utilizar a prática do gasto duplo, ou seja, gastar a mesma criptomoeda várias vezes. Embora esse tipo de ataque seja muito difícil de acontecer na rede Bitcoin, por conta do seu tamanho e de sua descentralização, Blockchains pequenas que não possuem a mesma estrutura podem ser alvos mais vulneráveis (Eyal & Sirer, 2014)⁶.

Outro fator muito relevante para essa discussão é o risco relacionado à segurança dos smart contracts. Caso esses contratos apresentem algum tipo de falha nos códigos, podem ser violados por invasores resultando em perdas financeiras significantes. Um caso famoso e que pode ser usado como exemplo é o ataque ao “DAO” (Decentralizes Autonomous Organization) em 2016, onde invasores aproveitaram falhas em smart contracts resultando na perda de milhões de dólares (Siegel, 2016)⁷.

A questão de não poder reverter uma transação também representa um risco. Uma vez registrada na Blockchain a transação não pode ser cancelada. Embora isso sirva como uma segurança contra fraudes, também pode apresentar erros, como por exemplo a transferência de fundos para um endereço errado. Esse ponto acabou colocando uma certa responsabilidade em seus usuários para certificar que todas as transações sejam precisas.

Existem também preocupações com o nível de privacidade do sistema. Apesar de todas as operações feitas na rede Blockchain sejam realizadas de forma anônima, uma vez que um usuário é associado a um endereço, todas as transferências feitas para este endereço podem ser rastreadas, levantando assim questões em relação a privacidade dos usuários da rede. Essa questão é um ponto muito sério, ainda mais pensando que dados recentes de mercado apontam

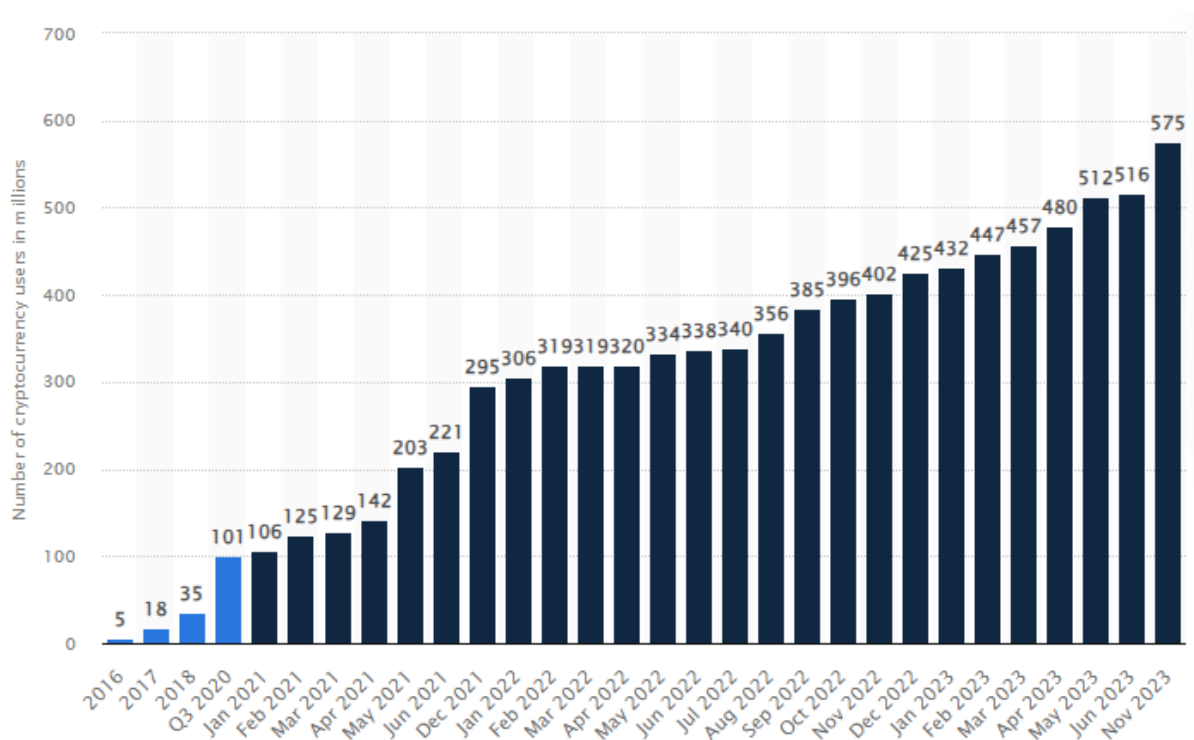
⁶ Eyal, I., & Sirer, E. G. (2014). Majority is not Enough: Bitcoin Mining is Vulnerable. *Financial Cryptography and Data Security*, 2014. Disponível em: <https://arxiv.org/abs/1311.0243>.

⁷ Siegel, M. (2016). 'The DAO: A Tale of Incompetence and Exploitation'. Disponível em: <https://www.coindesk.com/learn/understanding-the-dao-attack/>.

um aumento no número de pessoas que usam os criptativos, como é mostrado no gráfico abaixo (Gráfico 8).

GRÁFICO 8

NÚMERO DE CARTEIRAS DE CRIPTOMOEDAS EM MILHOES(2016-2023)



FONTE: STATISTA.COM

Esses riscos e o aumento de usuário no mercado mostram a necessidade de uma cautela ao utilizar e desenvolver tecnologias Blockchain. É sempre importante reforçar que medidas de segurança devem ser melhoradas para diminuir assim o perigo para seus usuários.

3 FUTURO DAS CRIPTOMOEDAS E A TAXAÇÃO

Depois de explicar as principais características das criptomoedas e mostrar como o sistema de Blockchain funciona para melhorar a circulação e os meios de negociação delas, o capítulo seguinte mostra como funciona a tributação no Brasil, e qual será o futuro do mercado de criptoativos,

3.1 TRIBUTAÇÃO NO BRASIL

Em 2022, o aumento na utilização das moedas digitais como alternativa de investimento fez com que o Brasil ficasse na sétima posição no ranking mundial de adoção de criptomoedas,

de acordo com a terceira edição do “Global Adoption Index” da Chainalysis. Essa posição no ranking é resultado do grande volume de valores negociados em criptoativos no país. Esse aumento não apenas mostra que o brasileiro está interessado nas criptomoedas, mas também está em busca de uma participação ativa no mercado mundial.

O brasileiro enxerga os ativos digitais como uma liberdade financeira, trazendo novas possibilidades que são totalmente diferentes do mercado tradicional. Apesar disso, não significa que as moedas serão isentas de serem declaradas e tributadas. Com o aumento do número de corretoras no Brasil e a necessidade de arrecadação estatal, a Receita Federal do Brasil (RFB) normatizou a necessidade de declarar e tributar as moedas digitais no imposto de renda.

O imposto de renda começou no Brasil em 1922, com a criação da Lei nº 4.625⁸, que visava a tributação da renda e dos proventos que fossem obtidos por pessoas físicas e jurídicas. No começo, o sistema de tributação do Brasil era muito simples e focava principalmente em arrecadar novos recursos para utilizar em despesa públicas. Com o passar do tempo, o imposto de renda passou a ser mais complexo e abrangente, pois precisou passar por reformas para conseguir se aclimar com o número de mudanças sócias e econômicas.

Em 1988, houve a publicação da Constituição Federal, que reforçou o sistema tributário brasileiro conseguindo dar mais liberdade para a RFB trabalhar na fiscalização e arrecadação de tributos (Brasil, 1988)⁹. Logo depois veio a Lei nº 9.250, de 1995¹⁰, trazendo alterações relevantes na legislação do imposto de renda para pessoas físicas, como a tabelada progressiva atualizada e entrada de deduções com mais detalhes, todas reforçando e apontando para a importância de um sistema de tributação mais justo (Brasil, 1995).

Nos anos 2000, o sistema tributário brasileiro seguiu evoluindo focando na modernização e simplificação do sistema. Em 2005, apareceu a chamada Lei do Bem¹¹, ou Lei nº 11.196, que introduziu novos incentivos fiscais para a inovação tecnológica, com o intuito de mostrar que o governo estava tentando acompanhar o desenvolvimento tecnológico do país

⁸ BRASIL. Lei nº 4.625, de 31 de dezembro de 1922. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/1901-1929/l4625.htm.

⁹ BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

¹⁰ BRASIL. Lei nº 9.250, de 26 de dezembro de 1995. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9250.htm.

¹¹ BRASIL. Lei nº 11.196, de 21 de novembro de 2005. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Lei/L11196.htm

(Brasil, 2005). Essas alterações foram muito importantes para preparar o sistema para novos tipos de ativos ou rendimentos que iriam aparecer, como as moedas digitais.

Na última década, com o avanço rápido da globalização, a RFB vem tentando acompanhar as novos ativos financeiros e as novas formas de se criar renda. Um Exemplo disso é a Lei nº 12.973, de 2014¹², que trouxe grandes mudanças na tributação dos lucros no exterior e de ativos financeiros. Apesar da lei não falar especificamente de moedas digitais, ela aponta uma certa preocupação do sistema em adaptar a tributação às novas realidades econômicas (Brasil, 2014).

A regulamentação no Brasil sobre as criptomoedas é um tópico mais recente. Em 2019, foi publicado a Instrução Normativa nº 1.888¹³, que estabelecia a obrigação dos cidadãos brasileiros de prestar informações sobre operações envolvendo ativos digitais à Receita Federal do Brasil, de acordo com artigo 1º da referida instrução normativa. Nos artigos 6º e 7º, é detalhado a obrigatoriedade de prestar informações não apenas às corretoras de ativos digitais que estão no Brasil, mas também pessoas jurídicas e físicas residente ou domiciliadas no país, quando as transferências forem realizadas em corretoras no exterior.

Essa legislação mostra um avanço importante na regulamentação do ativos digitais no Brasil, dando permissão para que à RFB possa fiscalizar e monitorar de forma mais eficaz todas as transferências envolvendo esses ativos.

Atualmente, ainda utilizando a Instrução Normativa nº 1.888, é obrigatório a prestação de informações para operações que ultrapassam o valor de 30 mil reais, mesmo quando são realizadas em corretoras que estão baseadas fora do país ou não são feitas por uma corretora (Receita Federal do Brasil, 2023).

De acordo com dados fornecidos pela RFB em 2023, foram registrados mais de 230 mil investidores de Bitcoin no processo de declaração de imposto de renda de pessoas físicas, que acumulam um montante de mais de 20 bilhões de reais e criptoativos (Receita Federal do Brasil, 2024). Esses números mostram a vontade e o interesse dos brasileiros pelas moedas digitais, e a importâncias deles no panorama econômico nacional.

¹² BRASIL. Lei nº 12.973, de 13 de maio de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Lei/L12973.htm.

¹³ BRASIL. *Instrução Normativa nº 1.888*. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=100592>

A tributação de ativos digitais no Brasil mostra que precisa de uma adaptação do sistema fiscal a novas forma de geração de renda. A transparência é um fator essencial para um desenvolvimento saudável do mercado de ativos digitais, sendo importante um monitoramento constante das regulamentações para assegurar sua eficácia.

3.2 FUTURO DAS CRIPTOMOEDAS

O Bitcoin mudou de várias maneiras desde seu lançamento em 2009. Aos poucos, ganhou novos adeptos e um local para aceitar pagamentos em moeda corrente. No entanto, o processo matemático utilizado pela mineração tornou-se mais complexo, exigindo máquinas mais potentes para criar Bitcoins e verificar as transações feitas com a moeda virtual. Atualmente, o Bitcoin ainda está pairando como uma tendência que pode ou não aumentar no futuro próximo.

Os governos ainda parecem estar muito apavorados com o advento do Bitcoin, talvez porque não saibam como incorporá-lo à economia nacional, como regulá-lo, ou mesmo como evitar que ele se torne não apenas a moeda padrão do mercado digital mundial, mas também nas transações.

O mercado de criptoativos está passando por momento de transformação. Hoje em dia, muitas empresas estão inovando em serviços e liderando o setor, isso aponta para um cenário promissor para o futuro. A entrada de grandes empresas tradicionais no mundo de criptoativos mostra uma tendência de crescimento e consolidação do setor (Ghose, 2018). O fato é que o futuro das criptomoedas dependerá da evolução mercado e do investimento em educação para mais pessoas.

Falando principalmente do Bitcoin, que basicamente comanda o mercado, seu futuro ainda é incerto apesar de seu potencial. Alguns usuários enxergam a moeda como uma tendência passageira, mas outros acreditam que o ativo tem potencial para se tornar uma espécie de “euro digital”, facilitando transações e ganhando cada vez mais o seu espaço no mercado (Antonopoulos, 2017).

CONCLUSÃO

A evolução do mercado financeiro nos últimos anos tem sido palco de transformações significativas que foram impulsionadas pela globalização econômica e pela quantidade de novas tecnologias. A abordagem das diferentes características das criptomoedas, desde o sistema Blockchain até as questões econômicas e regulatórias, mostra o tamanho da complexidade e a relevância desse assunto nos dias atuais.

É inegável o tamanho do impacto no sistema financeiro causado pelas criptomoedas. Esses ativos não só batem de frente com os modelos tradicionais de transação e moeda, mas também conseguem criar novos caminhos para a inovação e inclusão financeira. Apesar disso, a história das criptomoedas está só começando. Os temas como segurança, estabilidade e regulamentação precisam ser mais discutidos para que os ativos digitais possam atingir um potencial ainda maior do que já possuem.

Sobre a regulamentação, é necessário que governos, empresas e indivíduos colaborem entre si para a criação de uma infraestrutura que promova a inovação e que ao mesmo tempo protege os interesses dos usuários e a estabilidade econômica.

No entanto, é importante perceber que a busca pela regulamentação excessiva das criptomoedas por parte dos governos poderia acabar com a ideia principal desse mercado, a descentralização. A retirada dessa essência dos criptoativos poderia resultar na desconfiança dos usuários. Sendo assim, para garantir a aceitação a longo prazo, é essencial encontrar um equilíbrio entre os princípios fundamentais das moedas digitais e a regulamentação.

Portanto, com o avanço das tecnologias, é importante manter uma interpretação crítica e informada sobre a forma de como as criptomoedas podem ser inseridas de forma eficiente e segura no mercado financeiro. Com o objetivo de tentar maximizar os benefícios que as moedas digitais podem trazer para a sociedade, o futuro delas depende somente de estudos contínuos e debates abertos entre as partes interessadas.

REFERÊNCIAS

ANTONPOULOS, Andreas. **Mastering Bitcoin**. O'Reilly Media, 2017. Disponível em: <https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf>. Acesso em: 20 mar. 22

Nakamoto, S. (2008). **Bitcoin: A Peer-to-Peer Electronic Cash System**. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 15 mar. 2022.

BARBOSA, Tatiana. **A Revolução das Moedas Digitais Bitcoins e Altcoins**. Revoar, 2016

KELLY, Brian. **The Bitcoin Big Bang: How Alternative Currencies Are about to Change the World**. Wiley, 2014

VIGNA, Paul; CASEY, Michael. **The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order**. St. Martin's Press, 2015. Disponível em: https://www.academia.edu/98851085/Cryptocurrency_how_Bitcoin_and_digital_money_are_challenging_the_global_economic_order. Acesso em: 15 fev. 2024

BROCHADO, Ana. **Snapshot da Indústria das Criptomoedas**. Comissão do Mercado de Valores Mobiliários, 2018

BURNINSKE, Chris; TATAR, Jack. **Criptoativos: o guia do investidor inovador para bitcoin e além**. Alta Books, 2019

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 fev. 2023.

BRASIL. Lei nº 9.250, de 26 de dezembro de 1995. **Dispõe sobre a alteração da legislação do imposto de renda das pessoas físicas e dá outras providências**. Brasil, 1995. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9250.htm. Acesso em: 10 jan. 2024.

BRASIL. Lei nº 11.196, de 21 de novembro de 2005. **Institui o Regime Especial de Tributação para a Plataforma de Exportação de Serviços de Tecnologia da Informação - REPES e dá outras providências**. Brasil, 2005. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Lei/L11196.htm. Acesso em: 27 mar. 2023.

BRASIL. Lei nº 12.973, de 13 de maio de 2014. **Altera a legislação tributária federal relativa ao Imposto sobre a Renda das Pessoas Jurídicas (IRPJ) e dá outras providências**. Brasil, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Lei/L12973.htm. Acesso em: 5 nov. 2023.

BRASIL. Lei nº 4.625, de 31 de dezembro de 1922. **Brasil**, 1922. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/1901-1929/l4625.htm. Acesso em: 12 dez. 2023.

BRASIL. Instrução Normativa nº 1.888. **Dispõe sobre a prestação de informações relativas às operações realizadas com criptoativos**. Receita Federal, 2019. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=100592>. Acesso em: 22 jan. 2024.

SIEGEL, D. **Understanding The DAO Attack**. Coindesk, 2016. Disponível em: <https://www.coindesk.com/understanding-dao-hack-journalists>. Acesso em: 6 set. 2022

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). **Alerta sobre os riscos associados a operações com criptoativos**. 10 maio 2018. Disponível em: https://www.investidor.gov.br/publicacao/Alertas/alerta_CVM_CRIPTOATIVOS_10052018.pdf. Acesso em: 15 fev. 2023.

BANCO CENTRAL DO BRASIL (BCB). **Esclarecimentos sobre moedas virtuais**. Disponível em: http://www.bcb.gov.br/Pre/bc_atende/port/moedasvirtuais.asp#2. Acesso em: 20 jan. 2024.

COINMARKETCAP. **Bitcoin**. Disponível em: <https://coinmarketcap.com/pt-br/currencies/bitcoin/>. Acesso em: 15 maio 2024.

COINMARKETCAP. **Ethereum**. Disponível em: <https://coinmarketcap.com/pt-br/currencies/ethereum/>. Acesso em: 15 maio 2024.

CHAUM, David. Disponível em: <https://chaum.com/>. Acesso em: 18 fev. 2024.

JOVEM NERD. **O que é Cypherpunk?** Disponível em: <https://jovemnerd.com.br/noticias/ciencia-e-tecnologia/o-que-e-cypherpunk>. Acesso em: 20 fev. 2023.

RBE - REVISTA BRASILEIRA DE EDUCAÇÃO. **História do metaverso**. Disponível em: [https://rbe.mec.pt/np4Admin/%7B\\$clientServletPath%7D/?newsId=2987&fileName=Hist_ria_do_metaverso.pdf](https://rbe.mec.pt/np4Admin/%7B$clientServletPath%7D/?newsId=2987&fileName=Hist_ria_do_metaverso.pdf). Acesso em: 25 maio. 2024.

BITBO. **Gráfico de Dificuldade de Mineração**. Disponível em: <https://charts.bitbo.io/mining-difficulty/>. Acesso em: 05 maio. 2024.

ZOHAR, A. **Bitcoin: Under the Hood**. Communications of the ACM, v. 58, n. 9, p. 104-113, 2015. Disponível em: <https://dl.acm.org/doi/10.1145/2701411>. Acesso em: 15 fev. 2024.

STATISTA. **Global cryptocurrency user base from Q3 2016 to Q1 2021**. Disponível em: <https://www.statista.com/statistics/1202503/global-cryptocurrency-user-base/>. Acesso em: 05 maio. 2023.

SWAN, Melanie. **Blockchain: Blueprint for a New Economy**. 2015. Disponível em: https://www.academia.edu/44112222/Melanie_Swan_Blockchain_BLUEPRINT_FOR_A_NEW_ECONOMY. Acesso em: 6 out. 2023.

Eyal, I., & Sirer, E. G. **Majority is not Enough: Bitcoin Mining is Vulnerable**. *Financial Cryptography and Data Security*, 2014. Disponível em: <https://arxiv.org/abs/1311.0243>. Acesso em: 5 out. 2022.

CHAINALYSIS. **Global Crypto Adoption Index. 2022**. Disponível em: <https://www.chainalysis.com/blog/2022-global-crypto-adoption-index/>. Acesso em: 20 fev. 2024.

GHOSE, T. **The Bitcoin Market and Cryptocurrency Prices Reflect Investor Sentiment**. 2018.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World**. 2016. Disponível em: https://itig-iraq.iq/wp-content/uploads/2019/05/Blockchain_Revolution.pdf. Acesso em: 15 jun. 22.

RECEITA FEDERAL DO BRASIL. **Receita Federal esclarece sobre declaração de operações com criptoativos. 2023**. Disponível em: <https://www.gov.br/receitafederal/pt-br/assuntos/noticias/2023/marco/receita-federal-esclarece-sobre-declaracao-de-operacoes-com-criptoativos>. Acesso em: 10 abril 2024.

RECEITA FEDERAL DO BRASIL. **Declaração de imposto de renda 2013: bitcoins e outros criptoativos precisam ser informados. 2024**. Disponível em: <https://www.gov.br/receitafederal/pt-br/assuntos/noticias/2024/janeiro/declaracao-de-imposto-de-renda-2013-bitcoins-e-outros-criptoativos-precisam-ser-informados>. Acesso em: 15 março 2023.