



**Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"**

TULIO EVANGELISTA

**BITCOIN UTILIZADA COMO FERRAMENTA PARA REALIZAÇÃO DE
CRIME**

**Assis/SP
2020**



**Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"**

TULIO EVANGELISTA

**BITCOIN UTILIZADO COMO FERRAMENTA PARA REALIZAÇÃO DE
CRIME**

Projeto de pesquisa apresentado ao curso de Direito do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

**Orientando (a): Tulio Evangelista
Orientador (a): Fabio Pinha Alonso**

**Assis/SP
2020**

FICHA CATALOGRÁFICA

EVANGELISTA, Tulio.

Título do trabalho / Tulio Evangelista. Fundação Educacional do Município de Assis –FEMA – Assis, ano.

Número de páginas.

1. Palavra-chave. 2. Palavra-chave.

CDD:
Biblioteca da FEMA

TULIO EVANGELISTA

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: _____
Fabio Pinha Alonso

Examinador: _____
Cláudio José Palma Sanchez

AGRADECIMENTOS

Primeiramente agradecer a Deus pela coragem de encarar o desafio de fazer o trabalho de conclusão de curso, aos professores do curso de direito da FEMA, por tudo que foi ensinado e pela qualidade apresentada, em especial ao meu orientador Fabio Pinha Alonso.

À minha família por apoiar o curso que optei cursar, a minha namorada Isabele por ajudar e apoiar até o ultimo minuto, ao meu colega de turma Lucas por toda ajuda prestada sempre que ajudei.

Com a lei, pela lei e dentro da lei; porque fora da lei não há salvação.

BARBOSA, Ruy

RESUMO

Texto.

Palavras-chave: Bitcoin, peer-to-peer, blockchain, crimes

As moedas digitais (bitcoin, ethereum, litecoin e etc.) estão crescendo muito nos últimos anos, vem sendo muito utilizadas para compras, transações econômicas nacionais e internacionais e até mesmo em crimes, e por ela ser de fácil acesso no mundo inteiro, ela possibilita que o usuário possa fazer negócios legais e muitas vezes ilegais. Exemplo disso é “pirâmide financeira” de bitcoins, extorsão, lavagem de dinheiro, financiamento de crimes, como o terrorismo, tráfico de drogas, ou seja, qualquer coisa.

Essas moedas são mineradas com base em uma rede p2p(peer-to-peer) que é descentralizada, portanto não há necessidade de ter intermediário para a realização de transações financeiras, ou seja, não há taxas e pode ser usado em qualquer país e não há limites de valores e quantidade a ser utilizado pelo usuário. Elas ficam armazenadas nas carteiras virtuais, e todas as suas transações são reunidas em blocos, sendo que cada bloco se conecta ao anterior através de um código, formando uma rede de códigos conhecida como blockchain, o que torna mais difícil o rastreo.

ABSTRACT

Texto em inglês.

Keywords:

LISTA DE ILUSTRAÇÕES

FIGURA 1- REDE PEER-TO-PEER.....	16
FIGURA 2- TRANSAÇÕES BITCOIN.....	18
FIGURA 3- DETALHE DE DEADOS DE CADA BLOCO.....	19
FIGURA 4- PLACA DE VIDEO MINING-P106-6G.....	26
FIGURA 5- DOUBLE SPENDING OF BITCOIN.....	32
FIGURA 6- ESQUEMA DE PAGAMENTOS PARA CARL MARK FORCE.....	58

LISTA DE TABELAS

TABELA 1- GRAFICO COM O TOP 10 COUNTRIES WORLDWIDE BY NUMBER OF BITCOIN ATMs INSTALLED.....	23
TABELA 2- GRAFIC OF CRYPTO ATMA INSTALLATION GROWTH.....	24
TABELA 3- GRAFICO COM OS INCIDENTES DE TENTATIVAS DE FRAUDES REPORTADOS AO CERT.BR- JANEIRO A DEZEMBRO 2019.....	43
TABELA 4- GREAFICO COM OS INVESTIDORES ILUDIDOS.....	45
TABELA 5- GRAFICO DA ALÍQUOTA DO IMPOSTO DE RENDA.....	48
TABELA 6- GRAFICO COM OS INCIDENTES REPORTADOS AO CERT.BR DE TIPOS DE ATAQUE DE JANEIRO A DEZEMBRO DE 2019.....	53
TABELA 7- GRAFICO COM O TOTAL DE INCIDENTES REPORTADOS AO CERT.BR POR ANO DE 1999 A 2019.....	55
TABELA 8- TIPIFICAÇÕES DE FORMAS DE CRIMES CIBERNÉTICOS COMUNS.....	56

LISTA DE ABREVIATURAS E SIGLAS

ATM- AUTOMATED TELLER MACHINE (CAIXA ELECTRONICO)

BTC-BITCOIN

CPF

CVM- COMISSÃO DE VALORES MOBILIÁRIOS

DARF- DOCUMENTO DE ARRECADAÇÃO DA RECEITA FEDERAL

EUA- ESTADOS UNIDOS DA AMÉRICA

FBI- FEDERAL BUREU OF INVESTIGATION

MPF- MINITÉRIO PÚBLICO FEDERAL

P2P- PEER-TO-PEER

RFB- RECEITA FEDERAL BRASILEIRA

SUMÁRIO

1. INTRODUÇÃO	13
2. BITCOIN.....	14
2.1. O QUE É O BITCOIN?.....	14
2.2. REDE PEER-TO-PEER (PONTO A PONTO).....	15
2.3. BLOCKCHAIN	17
2.4. OPERAÇÕES FINANCEIRAS COM BITCOIN.	18
2.5. AS TRANSAÇÕES E A REDE	19
2.5.1. BITCOIN UTILIZADO COMO MEIO DE PAGAMENTO	20
2.5.2. BITCOIN PARA PAGAR IMPOSTOS	21
2.5.3. Restituição do imposto em Bitcoin	22
2.5.4. CAIXAS ELETRÔNICOS DE BITCOIN	23
2.6. COMO MINERAR BITCOIN.....	26
2.7. CONSEQUÊNCIAS COM O ULTIMO BITCOIN MINERADO	27
2.8. O QUE SÃO EXCHANGES	28
2.9. RASTREABILIDADE DA BITCOIN PARA RESPONSABILIZAÇÃO DE CRIME ²⁸	
2.9.1. ATAQUE DOS 51%.....	29
2.9.2. SELFISH MINING ATTACK	30
2.9.3. ECLIPSE ATTACK.....	31
3. REGULAÇÃO DO BITCOIN.....	33
3.1. ETIMOLOGIA DA PALAVRA REGULAÇÃO.....	33
3.2. NATUREZA JURÍDICA DA BITCOIN.....	34
3.3. BITCOIN COM NATUREZA JURÍDICA DE ATIVO	34
3.4. BITCOIN COM NATUREZA JURÍDICA DE COMMODITY	35
3.5. BITCOIN COM NATUREZA DE MOBILIÁRIO	36
3.6. A FALTA DE REGULAÇÃO DO BITCOIN.....	37
3.7. INSTRUÇÃO DA RECEITA FEDERAL	38
3.8. REGULAÇÃO NO BRASIL	38
3.9. PROJETO DE LEI Nº2.303/15.....	39
4. O BITCOIN NO COMETIMENTO DE CRIMES	39
4.1. LAVAGEM DE DINHEIRO UTILIZANDO BITCOIN	39

4.2.	FRAUDE USANDO BITCOIN	42
4.3.	PIRÂMIDES FINANCEIRAS E A BITCOIN	45
4.4.	BITCOIN E A SONEGAÇÃO FISCAL	47
4.5.	CRIMES CIBERNÉTICOS E A BITCOIN	52
4.5.1.	CASO WANNACRY	57
4.5.2.	CASO SILK ROAD	58
5.	CONSIDERAÇÕES FINAIS	59
6.	GLOSSÁRIO	63
7.	ANEXOS	64
7.1.	ANEXO A- INSTRUÇÃO NORMATIVA RECEITA FEDERAL.....	64
7.2.	ANEXO B- PROJETO DE LEI Nº 2.303/15	65
8.	REFERENCIAS.....	72

1. INTRODUÇÃO

O presente trabalho tem como intenção estudar como as intensas inovações tecnológicas que vem ocorrendo ao longo dos anos, mas - especificamente - tratando-se das moedas digitais, com foco na Bitcoin. Fizeram com que o mundo jurídico necessitasse de inovações, em razão das varias ocasiões do dia a dia em que os atuantes nas áreas do direito e do financeiro se esbarram nas situações que envolvem essas criptomoedas, e acabam se deparando com leis escassas e com a falta da adequada regulamentação.

Adiante será tratado o surgimento dessas moedas, contextualizando com o momento histórico em que vivíamos na época do seu surgimento, abordando o que é a bitcoin, quem a criou, como ela funciona e porque é tão atrativa.

A bitcoin foi criada em 2009 por Satoshi Nakamoto, após a crise econômica de 2008. Nakamoto inventou uma moeda descentralizada, ou seja, sem interferência do Estado, e que pode realizar transações sem intermediários, funcionando através de uma rede peer-to-peer, e armazenando as informações a respeito dessas transferências no *blockchain*, uma tecnologia inovadora. Essas moedas podem ser compradas ou mineradas. Essa mineração gera lucro para os mineradores e para indústrias no qual fornecem os equipamentos adequados para realização do mesmo. Será demonstrado que a bitcoin pode funcionar como meio de pagamento de contas e em alguns países como forma de pagar impostos, servindo até mesmo para restituições destes. Além disso, crescente demanda possibilitou a criação de caixas eletrônicos especializados nesse tipo de operação.

Logo após, será estudado as várias correntes de pensamento acerca dos possíveis enquadramentos da natureza jurídica desses *criptoativos*, utilizando-se de diversos autores importantes do cenário brasileiro e mundo afora. Observaremos que no Brasil há uma carência de regulação. Essa regulamentação será importante em razão da identificação da autoridade competente para tratar essas criptomoedas. Ademais, serão apontadas as manifestações das autoridades reguladoras deste país a respeito dessas moedas digitais.

O terceiro e ultimo capitulo, tratará a respeito dos crimes que envolvem a Bitcoin, destacando as características, tipificações e suas idiosincrasias próprias. Primeiramente abordaremos os crimes de lavagem dinheiro, um delito corriqueiro no cenário brasileiro,

comentando - principalmente - o que é esse delito, como ocorre e a partir daí discutir como as criptomoedas contribuem com a criminalidade.

Em sequência trataremos a respeito do crime de fraude cibernética, tópico que explicará no que consiste esse delito, apresentando gráficos de estatísticas e a relação dessa infração com as moedas digitais.

Dando continuidade, falaremos sobre o crime de pirâmide financeira - que é um tipo de fraude - destacando como ocorre nos casos envolvendo as moedas digitais. Logo após, estudaremos sonegação fiscal, tópico que esclarecerá como acontece a declaração das criptomoedas, compreendendo a forma e quando deve ser calculada.

Por fim, serão analisados os crimes cibernéticos, principalmente os que abrangem a invasão cibernética, inclusive suas classificações, apresentando gráficos com estáticas a respeito de tal delito, bem como casos famosos, como, por exemplo, o do *wannacry* e o *silk Road*, que envolve agentes federais.

2. BITCOIN

2.1. O QUE É O BITCOIN?

O Bitcoin nada mais é do que uma criptomoeda criada no ano de 2008 por Satoshi Nakamoto (desconhecido), sendo ele próprio a publicar em um fórum da internet chamado “*The Cryptography Mailing*” o *White paper* - documento oficial do Bitcoin - denominado como “Bitcoin: A *peer-to-peer* eletrônica cash system”. Encontra-se em formato aberto - open sourcer - na web, portanto, qualquer pessoa pode utiliza-lo ou até mesmo aprimora-lo, e assim a bitcoin nos mostrou que não estava subordinada a nenhuma instituição financeira, Estado ou qualquer sistema financeiro.

Nakamoto lançou a Bitcoin no começo da crise financeira mundial em 2008 – conforme mencionado acima - o qual foi responsável por quebrar várias instituições financeiras, em seu *White paper*, ele destaca sua crítica ao sistema financeiro tradicional e sua obrigatoriedade de estar ligada a alguma instituição financeira para realizar qualquer tipo de movimentação.

A Bitcoin por sua vez, não necessita de nenhuma vinculação, o que a torna uma inovação, possibilitando o usuário realizar uma transação financeira sem intermediários. Não há como reverter essa transferência, portanto, o desfrutador fica protegido de eventuais fraudes que poderiam ocorrer.

“Todas as transições que ocorrem na economia bitcoin são registradas em uma espécie de livro razão público e distribuído chamado blockchain - corrente de blocos, ou simplesmente um registro público de transações -” (Ulrich, 2014, “Bitcoin a moeda na era digita”)

A Bitcoin se configura na forma de várias regras que se comunicam por meio de computadores que se encontram esparsos pelo mundo, e permanecem conectados por uma rede peer-to-peer - ponto a ponto - de seu próprio sistema. (Nakamoto, 2008; Ulrich, 2014), visto que essas regras não tem um dono, torna nós usuários, os possuidores dele.

Entretanto, o fato de a bitcoin possuir a natureza descentralizada a transforma em um forte instrumento para o cometimento de crimes, como poderá ser visto adiante, no desenvolvimento do presente trabalho.

“Por outro lado, a natureza descentralizada do Bitcoin também apresenta oportunidades ao crime. O desafio, então, é desenvolver processos que reduzam as oportunidades para criminalidade enquanto mantêm-se os benefícios que Bitcoin oferece.” (Ulrich, 2014, “bitcoin a moeda na era digital”).

2.2. REDE PEER-TO-PEER (PONTO A PONTO)

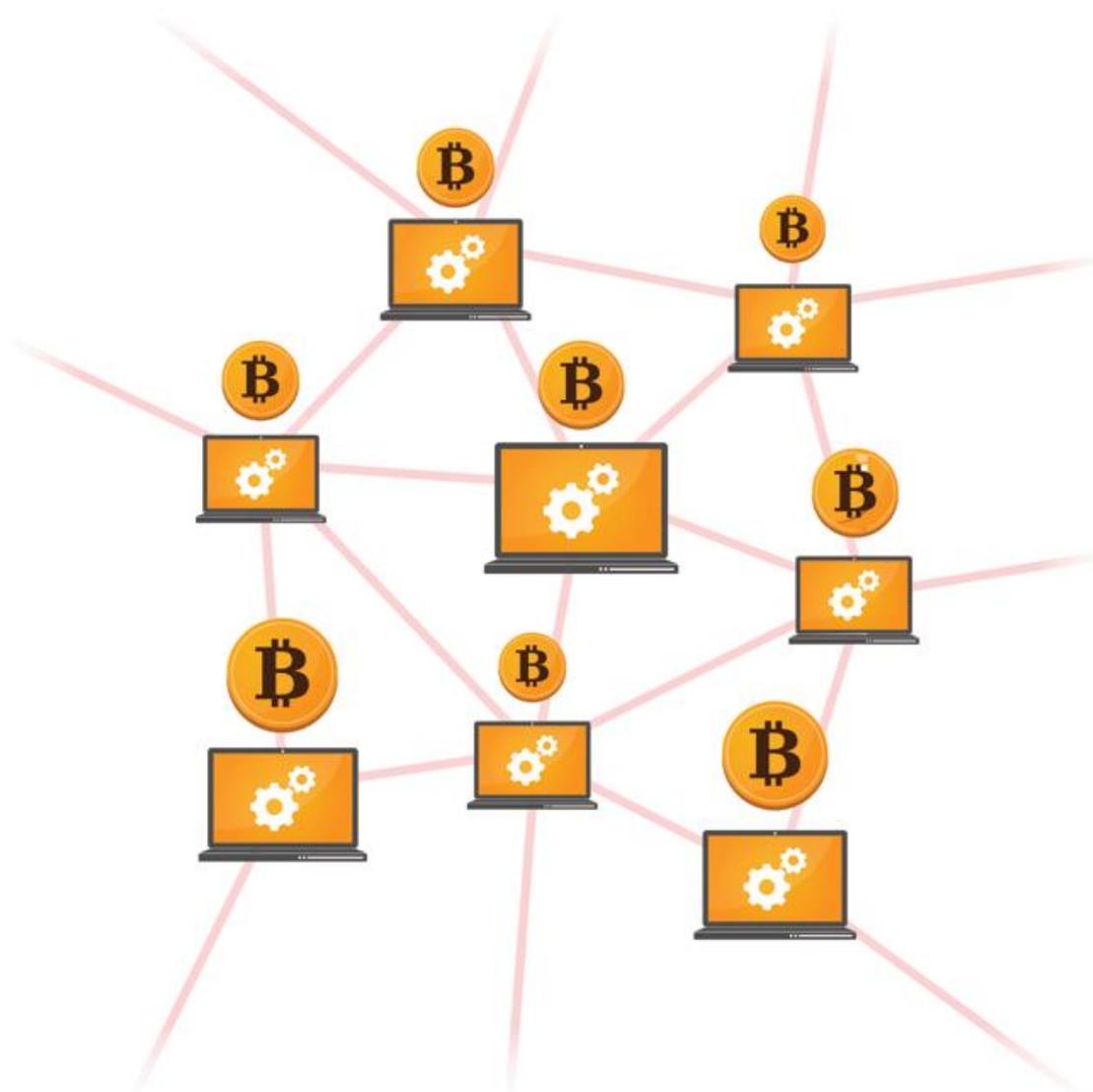
A rede peer-to-peer conhecida também como ponto a ponto ou P2P, é um sistema na qual possibilita a transferência de todos os dados sem a utilização de um intermediário. BEAL (2005) o define Como:

“Often referred to simply as peer-to-peer, or abbreviated P2P, peer-to-peer architecture is a type of network in which each workstation has equivalent capabilities and responsibilities. This differs from client/server architectures where some computers are dedicated to serving the others. “

Essa rede em se tratando de tecnologia financeira, em geral é utilizada para realização de transferências de criptomoedas, visto que não há a necessidade de terceiros, e torna as transações mais rápidas anonimamente.

Nakamoto no início da Bitcoin o definiu como “um sistema peer-to-peer de dinheiro eletrônico” (Nakamoto, 2008), o que possibilitou que ela pudesse ser transferida no mundo todo com mais segurança.

Por não haver um “comando central” o uso do peer-to-peer nos blockchain, nos propicia segurança a qualquer tipo de intervenção de autoridades centrais, ou seja, as carteiras dessas moedas não podem vir a sofrer congelamento ou interferência pelo governo, plataformas privadas de pagamento ou provedores de qualquer tipo.



1

2.3. BLOCKCHAIN

O blockchain é uma rede de blocos que registra todas as transações envolvendo bitcoin, ou seja, é como um livro de razão pública ou contábil. Esse registro acontece de forma auditada por qualquer pessoa – basta acessar os

1 **PORTAL DO BITCOIN.** Transações não confirmadas do Bitcoin batem recorde e chegam a 155mil. Portal do Bitcoin. Acessado dia 24 de agosto de 2020. Disponível em: <https://portaldobitcoin.uol.com.br/transacoes-nao-confirmadas-bitcoin-batem-recorde-e-chegam-155mil/>.

sites Blockchain.info ou Blockcypher e digitar o número de sua respectiva “hash” - e é inviolável e imutável, o que torna as transferências seguras, pois impede que a mesma moeda seja usada duas vezes, mas - na teoria - é possível utilizar, como veremos mais adiante.

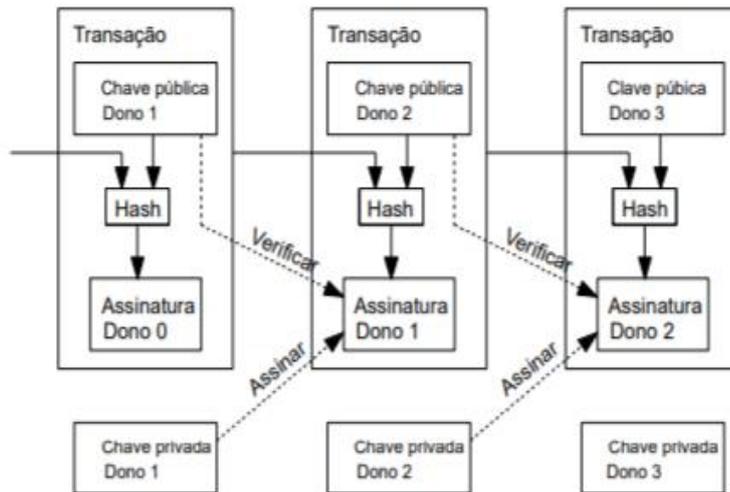
O registro de informações consiste na quantidade de moedas transacionadas, ou seja, quem enviou e quem recebeu; quando foi realizada a transação e em qual parte do livro está registrada. Essas informações são armazenadas em cadeias de blocos que são marcados com hora e data, onde todos os computadores que pertencem à rede possuem uma cópia do banco de dados, sendo assim, o blockchain é uma tecnologia de peer-to-peer.

Portanto, o blockchain é uma tecnologia que transformou a maneira de realizar transações, facilitando a aceitação da Bitcoin, pois se demonstrou ser uma rede segura com um grande poder computacional.

2.4. OPERAÇÕES FINANCEIRAS COM BITCOIN.

As transações da bitcoin funcionam com a utilização de duas chaves: a chave pública e a chave privada, sendo que a privada permite que somente seu usuário acesse a rede e nenhum outro utilizador sabe a quem pertence essa tranca. Já a pública aparece na rede, possibilitando que qualquer utente possa verificar que houve a transferência e o valor.

Em sua White paper, Nakamoto (2008, p.2) explica que “We define an electronic coin as a chain of digital signatures”, ou seja, a moeda eletrônica é definida como uma cadeia de assinaturas, sendo assim cada usuário realiza a transferência utilizando uma assinatura digital denominada de hash do usuário anterior e também a chave pública de quem irá recebê-la, e então essas autenticações são adicionadas no fim da moeda, isso permite que quem for receber consiga averiguar as assinaturas e saber a cadeia de propriedade.



2

2.5. AS TRANSAÇÕES E A REDE

Para se executar a rede de maneira eficiente é necessário observar alguns passos, que Nakamoto mostra em seu White paper:

- “1) New transactions are broadcast to all nodes.
- 2) Each node collects new transactions into a block.
- 3) Each node works on finding a difficult proof-of-work for its block.
- 4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
- 5) Nodes accept the block only if all transactions in it are valid and not already spent.
- 6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.” (Nakamoto, 2008, p.3)

Como descrito na citação acima, é essencial que:

- A) cada transação nova que foi realizada será transmitida a todos nós (nodes);
- B) cada nó realizará o serviço de coletar e juntar as novas transações em blocos;
- C) Esse nó tem como objetivo encontrar uma difícil prova-de-trabalho para seu bloco, ou seja, a prova que a moeda não foi transferida anteriormente;
- D) Ao encontrar a prova de trabalho ele então a transmite para todos os nós da rede;

² Op.cit. 2008, p.2. disponível em: <https://bitcoin.org/bitcoin.pdf>

pela inovação dos grandes negócios. Mas todos que aceitam concordam que pode ser uma técnica que tem muito a oferecer e com potencial para se perpetuar por anos.

Um levantamento feito pelo site *coinmap.org* em seu mapa interativo mostra que até o dia 19 de agosto de 2020 havia no mundo 19.623⁵ estabelecimentos que aceitam pagamentos realizados com criptomoedas, desde café, redes de fast food, caixas eletrônicos e shoppings.

Tal levantamento nos evidencia que na realidade a criptomoeda tem um grande potencial para ficar, e que pode e - provavelmente - irá evoluir muito ainda para atender a demanda do comércio em geral.

2.5.2. BITCOIN PARA PAGAR IMPOSTOS

Como citado anteriormente, a bitcoin e as moedas digitais em geral, estão sendo usadas como forma de pagamento por muitos empresários, então faz com que seja levada a questão: a bitcoin poderia ser usada para pagar impostos?

Respondendo a pergunta acima, o estado de Ohio localizado no centro-oeste dos EUA - Estados Unidos da América - foi o pioneiro em utilizar as criptomoedas - especificamente - a Bitcoin, para o pagamento de impostos.

O mencionado Estado converte a moeda através de uma empresa denominada de Bitpay⁶, localizada em Atlanta. Isso não impede a companhia mencionada, de realizar serviços a outro estado, pois a legislação norte-americana permite que isso ocorra.

Há 23 impostos listados que possibilitam a realização do pagamento por meio de criptomoedas. Dentre estes estão às contas mais comuns de uso diário como, à luz elétrica e varia até as taxas de vendas. Entretanto, só é permitido aos donos de estabelecimentos comerciais ou pessoas jurídicas, receberem com moedas digitais, mas há o interesse de abranger as pessoas físicas em um futuro próximo. O pagamento se efetivará quando o

⁵COINMAP. MAP. Coinmap. Acessado dia 24 de agosto de 2020. Disponível em: <https://coinmap.org/view/#/world/-26.01976579/-66.02508545/8>.

⁶ÉPOCA NEGÓCIOS. Estado americano de Ohio começa a aceitar bitcoin para pagamento de impostos. ÉPOCA NEGÓCIOS. Acessado em 20 de agosto de 2020. Disponível em: <https://epocanegocios.globo.com/Mundo/noticia/2018/11/estado-americano-de-ohio-comeca-aceitar-bitcoin-para-pagamento-de-impostos.html#:~:text=Estabelecimentos%20comerciais%20e%20empresas%20poderão,usando%20a%20moeda%20virtual%20bitcoin&text=O%20estado%20norte-americano%20de,com%20o%20Wall%20Street%20Journal>.

indivíduo realizar o cadastro no site "OhioCrypto.com", e a partir daí serão processados pela empresa responsável pela conversão da moeda.

Josh Mandel, tesoureiro estadual de Ohio, afirma que tal movimento realizado pelo Estado visa oferecer mais formas de realizar pagamentos, em entrevista ao Cointelegraph⁷, Mandel afirma que tem como o principal objetivo facilitar o pagamento com a mais nova opção de pagamento e também: "projetar para o resto do país e do mundo que o estado de Ohio é líder em tecnologia blockchain. Acredito que, se quisermos expandir nossa economia de tecnologia aqui em Ohio, primeiro precisamos ser líderes em tecnologia."

No Canadá, a pequena cidade de Innisfil⁸, localizada no estado de Ontário, também começou a receber criptomoedas como pagamento de imposto. Para possibilitar o pagamento, a prefeitura da cidade fechou um acordo com a empresa Coinberry Pay que será responsável pelo processamento do pagamento. Esse pagamento será processado e então convertido em dinheiro, em seguida, será transferido para a cidade, que receberá em dinheiro moeda e não em criptomoeda.

Como observado o pagamento de imposto com bitcoin já é uma realidade, e a tendência é que mais cidades e estados venham a aderir essa nova tecnologia.

2.5.3. Restituição do imposto em Bitcoin

Nos EUA - Estados Unidos da América - há a opção de receber a restituição de impostos federais e estaduais em bitcoin, tal possibilidade se deu graças a um acordo firmado entre a Bitpay - empresa já mencionada acima - e a Refund, onde foi acordado que os clientes desta companhia tem a opção de receber - inteira ou em parte - sua restituição

⁷ JENKINSON, Gareth. **Cidade no Canadá vai permitir pagamento de impostos com bitcoin-definindo o padrão para o futuro?** Cointelegraph. Acessado em 20 de agosto de 2020. Disponível em: <https://cointelegraph.com.br/news/ohio-to-accept-tax-payments-in-crypto-setting-the-standard-for-future>

⁸RIGGS, Wagner. **Cidade no Canadá vai permitir pagamento de impostos com bitcoin.** Portal do Bitcoin. Acessado em 20 de agosto de 2020. Disponível em: <https://portaldobitcoin.uol.com.br/cidade-no-canada-vai-permitir-pagamento-de-impostos-com-bitcoin/#:~:text=Cidade%20no%20Canadá%20vai%20permitir%20pagamento%20de%20impostos%20com%20bitcoin,-por%20Wagner%20Riggs&text=O%20município%20de%20Innisfil%20será,bitcoin%20a%20partir%20de%200abril.>

em bitcoin. Isso ocorrerá através do aplicativo CoinRT⁹, e após criar uma conta o usuário receberá um número correspondente a agência que deverá ser incluído na declaração de imposto.

O CEO da Refund, Roger Chinchila (apud KAHTRI, 2019), afirmou que:

“Adding bitcoin was a natural fit for our customers who often do not have traditional checking accounts, pay high check cashing fees and regularly send money internationally. CoinRT enables them to get bitcoin quickly and easily for one flat fee.”

2.5.4. CAIXAS ELETRÔNICOS DE BITCOIN

Como já é de conhecimento de todos, a bitcoin não para de crescer, sinal disso é a quantidade de caixas eletrônicos voltada para transações dessa moeda que vem sendo instaladas no mundo todo, chegando a mais de 8.000 (oito mil)¹⁰ caixas eletrônicos instalados. Dessa quantidade 65% se encontra nos EUA¹¹.

A seguir demonstraremos um gráfico comparando os 10 países com mais caixas eletrônicos instalados no mundo, onde é possível observar a notável diferença entre os EUA e os outros países.

⁹ KAHTRI, Yogita. **Income tax payers in the U.S. now have the option to receive their federal and state refunds in bitcoin.** Coindesk. Acessado em 20 de agosto de 2020. Disponível em: <https://www.coindesk.com/us-income-tax-payers-can-now-get-refunds-in-bitcoin>

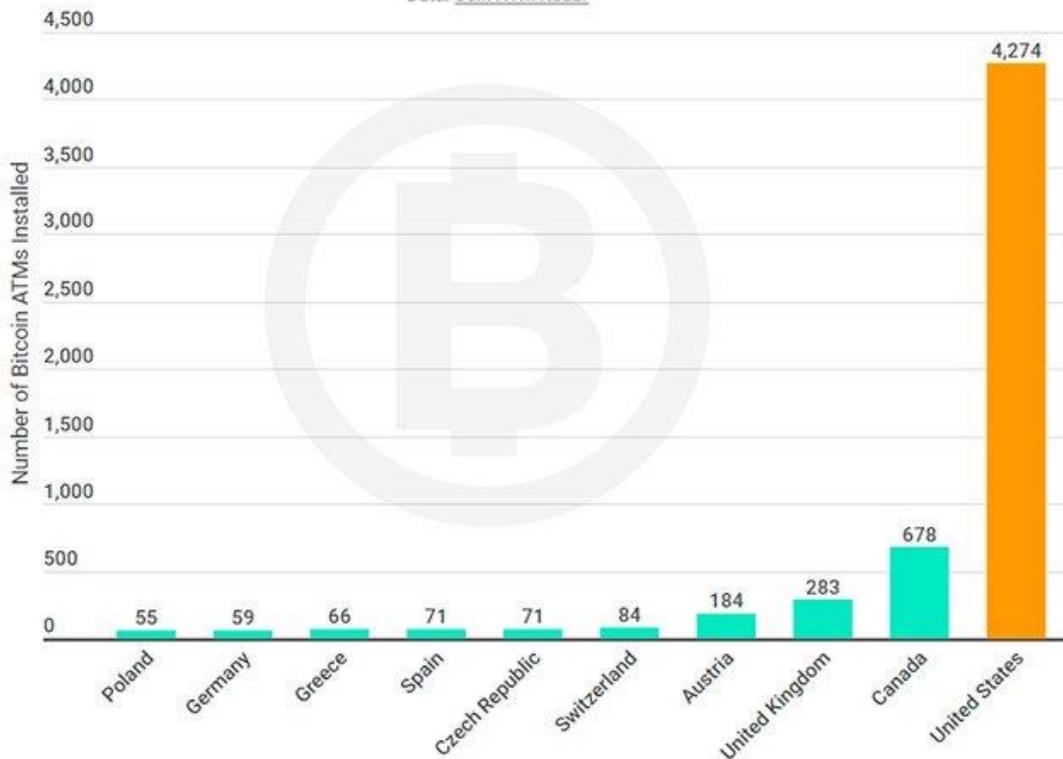
¹⁰ NASCIMENTO, Daniela Pereira. **Agora, existem mais de oito mil caixas eletrônicos de bitcoin em todo o mundo.** Money Times. Acessado em 22 de agosto de 2020. Disponível em: <https://www.moneytimes.com.br/agora-existem-mais-de-oito-mil-caixas-eletronicos-de-bitcoin-em-todo-o-mundo/>

¹¹ NOGUEIRA, João Gabriel. **Pesquisa diz que 66% dos caixas eletrônicos de Bitcoin estão nos EUA.** Mundo Conectado. Acessado em 20 de agosto de 2020. Disponível em: <https://mundoconectado.com.br/noticias/v/11979/pesquisa-diz-que-66-dos-caixas-eletronicos-de-bitcoin-estao-nos-eua>

Top 10 Countries Worldwide by Number of Bitcoin ATMs Installed

Details: as of January 9, 2020

Data: [Coin ATM Radar](#)



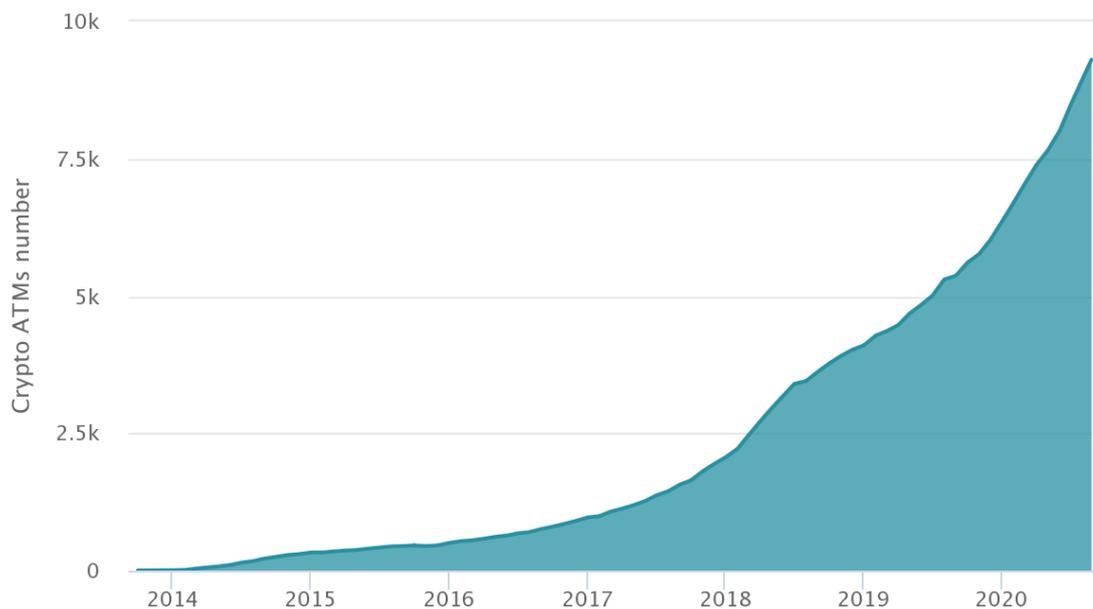
12

Como podemos observar no próximo gráfico, a instalação dessas caixas no mundo, já ultrapassou a marca dos oito mil, sendo que no ano de 2020 houve um expressivo aumento de instalação.

¹²COIN ATM RADAR. Estatísticas. Coin ATM Radar. Acessado em 20 de agosto de 2020. Disponível em: <https://coinatmradar.com/charts/growth/>

Crypto ATM Installations Growth

Source: coinatmradar.com



13

Esse crescimento exponencial de instalações de caixas atraiu os olhares dos reguladores, que visam diminuir a quantidade de crimes cometidos, como, por exemplo, a lavagem de dinheiro e a sonegação fiscal.

No ano de 2019 a Ciphertrace - empresa especializada em inteligência digital - por meio de um relatório, afirmou que 88% dos fundos que estavam nos caixas eletrônicos localizados nos EUA, foram transferidos para empresas no exterior. Tal número é preocupante visto que, essas companhias são Exchange internacionais de alto risco, o que facilita o cometimento do crime de lavagem de dinheiro e sonegação, por ser mais difícil conseguir informações. Além disso, a instalação dos caixas eletrônicos tornou mais fácil realizar transações, e proporcionou uma forma mais simples de se converter as moedas.

O Canadá com o objetivo de impedir a lavagem de dinheiro através desses caixas eletrônicos, aprovou uma lei em que as operadoras tem a obrigação de informar todas transações realizadas com valor acima de US\$ 10.000,00 (dez mil dólares).

Outros governos veem a necessidade de regulá-la, entendendo que a instalação pode ser um potencial ou não para a sonegação de impostos e lavagem de dinheiro.

¹³ OP.CIT. <https://coinatmradar.com/charts/growth/>

No Brasil não há caixas eletrônicos de bitcoin instalados, entretanto, a cidade de São Paulo irá receber o seu primeiro caixa, que será inserido pela empresa Coinverse, e poderá ser encontrado no shopping Nações Unidas, localizado no World Trade Center. A empresa afirma que tem interesse em colocar também, na cidade do Rio de Janeiro e em todas as capitais brasileira.

2.6. COMO MINERAR BITCOIN

Nakamoto utiliza-se da expressão “minerar”, pois entende que o bitcoin é como um “ouro” digital, por permitir que todas as pessoas em qualquer lugar do mundo, que possua um computador ou equivalente, possa minerar e adquirir o bitcoin, necessitando apenas utilizar a rede dessa moeda, a qual está em toda a rede virtual. Também é necessário que o computador utilizado esteja conectado à internet e - conseqüentemente - a rede blockchain da bitcoin. “The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation” (Nakamoto,2008).

Atualmente, minerar bitcoin virou algo importante e lucrativo, tanto para quem minera, quanto para as indústrias que vendem o material utilizado para minerar, exemplo disso é o grande número de placas de vídeo sendo lançadas para uso da mineração, e conforme a busca por criptomoedas sobe, mais valorizados esses materiais se tornam, afinal a procura pelos mesmos é muito grande.



14

MINING-P106-6G

2.7. CONSEQUÊNCIAS COM O ÚLTIMO BITCOIN MINERADO

Fernando Ulrich, estima que o último bitcoin seja minerado em 2140, isso acontecerá se a potência de mineração se elevar a um nível muito maior do que o atual, visto que a cada bitcoin minerado a dificuldade para encontrar outra moeda – BTC -aumentará.

“Estima-se que os mineradores colherão o último “satoshi”, ou 0,00000001 de uma bitcoin, no ano de 2140. Se a potência de mineração total escalar a um nível bastante elevado, a dificuldade de minerar bitcoins aumentará tanto que encontrar o último “satoshi” será uma empreitada digital consideravelmente desafiadora.” (Ulrich, 2014, p.20)

Ainda assim resta as perguntas, o que acontece quando o último bitcoin for minerado? Qual será a recompensa dos mineradores por manter a rede ativa?

¹⁴ **ASUS.** Mining-P106-6G. Asus. Acessado dia 2 de agosto de 2020. Disponível em: <https://www.asus.com/Graphics-Cards/MINING-P106-6G/> .

Ulrich explica que quando o último bitcoin for minerado, os mineradores que mantêm seu processamento na verificação das transações serão recompensados com a taxa de serviço da transferência realizada.

“Uma vez que o último “satoshi” tenha sido minerado, os mineradores que direcionarem sua potência de processamento ao ato de verificação das transações serão recompensados com taxas de serviço, em vez de novos bitcoins minerados. Isso garante que os mineradores ainda tenham um incentivo de manter a rede operando após a extração do último bitcoin.” (Ulrich, 2014, “bitcoin a moeda na era digital”).

2.8. O QUE SÃO EXCHANGES

As denominadas “*Exchange*” ou também conhecidas “corretoras de criptoativos”, são plataformas onde é possível realizar transações de moedas digitais, que funcionam como facilitadora da compra, venda e troca de moedas virtuais. O serviço das Exchanges é basicamente o de conectar os vendedores com os compradores, e assim mantem as transações mais seguras.

Para utilizar a Exchange o usuário precisa realizar um cadastro, e com isso é aberta uma conta onde o utente pode transferir valores de instituições financeiras, desde que possua conta corrente.

O cadastro nas Exchanges varia de uma para outra, pois são regras de regulamentação. No Brasil, por exemplo, é exigido que seja enviado uma foto digitalizada de algum documento com foto, ou o nome completo e o número do CPF.

As Exchanges funcionam de forma semelhante ao mercado de ações, ou seja, há a variação da cotação das moedas de Exchange para Exchange, o que permite que usuário faça cadastro em várias delas e negocie na que achar mais vantajosa.

2.9. RASTREABILIDADE DA BITCOIN PARA RESPONSABILIZAÇÃO DE CRIME

O uso da bitcoin é tão atrativo - pelo fato da anonimidade - que traz consigo uma grande dificuldade quando é necessário rastrear o usuário que realiza qualquer tipo de

transgressões penais para responsabilização de eventuais crimes, como a lavagem de dinheiro, fraude, invasão cibernética etc.

É importante informar que a anonimidade que a bitcoin proporciona não é absoluta, visto que existem métodos de desanonimizar as transações ilegais realizadas por usuários. Veremos algumas delas a seguir:

2.9.1. ATAQUE DOS 51%

Trata-se de um ataque que visa atacar qualquer rede de blockchain, inclusive a bitcoin, essa ofensiva ocorre quando uma entidade/organização obtém a capacidade de controlar a maioria dos *hash rate*, com o objetivo único de explorar possíveis falhas no sistema.¹⁵

Esse ataque proporcionaria aos atacantes a aptidão necessária para retroceder transações que eles mesmos realizaram no momento da execução do ataque. O grande problema é que essa agressão traz consigo a possibilidade de causar o denominado duplo gasto (Double spending). Além disso, o agressor tem a possibilidade de barrar alguma ou - no pior dos casos - todas as transações (ataque de negação de serviço).

A possibilidade de um ataque desse escalão acontecer contra o bitcoin - que é um blockchain maior - tem sido muito discutida, visto que embora haja êxito contra alguns blockchain menores, nos maiores seria quase que inviável, pois necessitaria de um poder computacional de proporções enormes, que traga consigo um custo muito alto e ganhos baixos.

A chance de algum ataque funcionar contra a bitcoin, tem diminuído com o tempo, pois conforme a mineração do bitcoin acontece mais difícil é ataca-lo. Sendo assim o poder computacional necessário para ocorrência do ataque vai se tornando maior com o passar do tempo.

15 **BINANCE ACADEMY**. O que é um Ataque de 51%? Binance Academy. Acessado em 25 de agosto de 2020. Disponível em: <https://academy.binance.com/pt/security/what-is-a-51-percent-attack>

2.9.2. SELFISH MINING ATTACK

O selfish mining (mineração egoísta), consiste em um método de mineração em que se obtém uma cadeia maior que as dos demais mineradores. A cadeia maior sempre é considerada a mais correta, em razão da regra denominada da longest chain rule (regra da cadeia mais longa).

Ethan Heilman et al. (2015), define o selfish attack Como: “With selfish mining [14,29,37,60], the attacker strategically withholds blocks to win more than its fair share of mining rewards.”

Ittay Eyal e Emin Gun Sirer (2013), definiram essa tática como:

“Approximately speaking, the selfish mining pool keeps its mined blocks private, secretly bifurcating the blockchain and creating a private branch. Meanwhile, the honest miners continue mining on the shorter, public branch.”

Logo abaixo veremos exemplos que a binance academy apresentou para explicar de maneira mais didática essa forma de minerar:

“Suponha que a taxa total de hash seja dividida igualmente entre quatro mineradores: Alice, Bob, Carol e Dan (cada um com 25%). Alice, Bob e Carol seguem as regras, mas Dan está tentando enganar o sistema para benefício próprio.

Em circunstâncias normais, a expectativa é de que o minerador encontre um bloco e o adicione à cadeia imediatamente. E é isso que Alice, Bob e Carol fazem como participantes honestos. Mas se Dan encontra um bloco, ele o mantém em segredo (é uma solução válida, mas ainda não foi adicionada). Dan pode ter sorte e encontrar dois blocos seguidos antes dos outros.

Vamos supor que 100.000 blocos foram minerados. Então agora temos Alice, Bob e Carol tentando propor o bloco número 100.001. Dan o encontra, mas mantém em sigilo. Agora existem duas cadeias, a pública e a secreta de Dan (mais longa). Enquanto os outros ainda estão tentando encontrar o bloco 100.001, ele encontra o bloco 100.002.

A cadeia de Dan está agora dois blocos à frente. Desde que sua sorte não acabe e ele possa permanecer à frente da outra cadeia, ele continua. Quando os outros o alcançam e ficam a apenas um bloco de distância, ele então revela sua cadeia.

A cadeia de Dan, agora pública, é mais longa que a cadeia em que os outros participantes estavam trabalhando. De acordo com uma regra que chamamos de longest chain rule (regra da cadeia mais longa), a cadeia “correta” é a que acumulou mais Proof-of-Work - também chamado de chainwork -. Ou seja, se um node (nó) detecta uma cadeia com mais trabalho acumulado, ele irá selecionar esta cadeia, dedicando seu poder de mineração à cadeia mais longa.

Agora, Alice, Bob e Carol podem ver a cadeia de Dan – eles agora reconhecem essa como a cadeia a ser seguida. Quaisquer recompensas que eles teriam ganho na outra cadeia não existirão mais. E como Dan minerou os blocos da cadeia mais atual, ele mantém todas as recompensas¹⁶.”

O exposto no exemplo acima, nos mostra que o efeito prático desse ataque afeta os demais mineradores, visto que eles foram lesados, pois perderam as prováveis recompensas que iriam receber ou já haviam recebido para Dan.

Entretanto tal pratica sairia mais caro do que a mineração conforme as deveria ser, e também não seria atrativo para os mineradores em geral, em razão desse ato prejudicar a segurança da rede, o que ocasionaria em uma queda nos valores da bitcoin - em outras palavras - o minerador egoísta não iria obter o lucro desejado .

2.9.3. ECLIPSE ATTACK

O eclipse attack é uma forma de atingir onde o agente tem objetivo de atacar um usuário específico isolando o mesmo. Nesse acometimento o indivíduo após isolar a vítima obstrui a “visão” da atividade real que está a rede, e garante que os nós realizados sejam todos controlados por ele.

O ataque é realizado da seguinte forma:

- 1º: primeiramente o invasor irá colocar na rede da vítima o seu IP, no qual a vítima irá se conectar sem saber, no momento em que reiniciar o software

¹⁶ **BINANCE ACADEMY**. Guia sobre Selfish Mining. Binance academy. Acessado em 22 de agosto de 2020. Disponível em: <https://academy.binance.com/pt/blockchain/selfish-mining-explained>

- 2º: em sequência, a vítima se encontrará em uma situação de controle pelo invasor, e com vários nós maliciosos colocados pelo agente, ou seja, a vítima está com a visão da rede obstruída.

Para que seja possível o ataque a vítima precisa estar em uma rede de IPs públicos.

Quando realizamos transferências eclipsadas, há a possibilidade de ocorrer alguns problemas, sendo eles:

- Gasto duplo com 0 (zero) confirmações: Esse gasto ocorre quando o indivíduo aceita a transação sem que haja confirmação, ou seja, a transmissão foi passada adiante. Entretanto até sua chegada no blockchain, quem enviou pode realizar uma nova transação com os mesmo valores só que aloca-las em outro lugar, e quando essa transação secundária tiver a taxa mais alta, ela será incluída na blockchain antes da anterior, o que invalidaria a primeira transação e a segunda passaria a ser a “correta”, mas vale lembrar que apenas será um risco para quem receber a transação se o mesmo realizar a 0 confirmação, ou seja, não confirmar se foi de fato realizada. Ethan Heilman et al. (2015), afirma que “In a 0-confirmation transaction, a customer pays a transaction to a merchant who releases goods to the customer before seeing a block confirmation, i.e., seeing the transaction in the blockchain.”

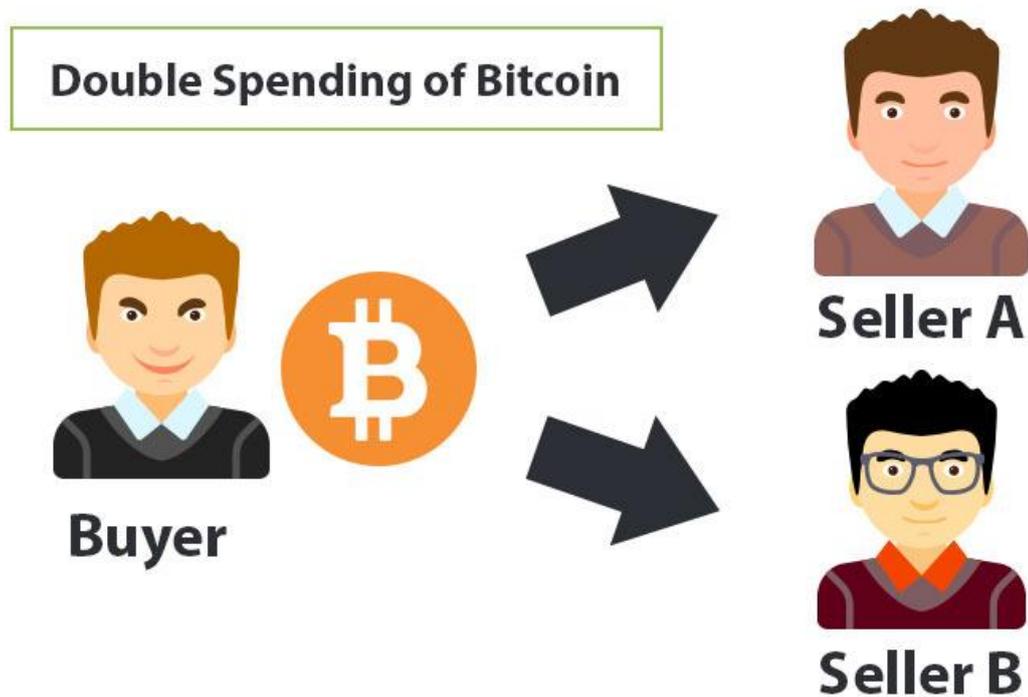
- Gasto duplo com N confirmações: Esse tipo de problema acontece quando algumas empresas tem a política de esperar uma quantidade especifica de confirmações antes de considerar o pagamento como realizado, muito semelhante ao problema supracitado do gasto duplo com 0 confirmações, só que a dificuldade de realiza-lo é maior, visto que o invasor teria que eclipsar tanto os mineradores quanto os comerciantes. Esse tipo de ataque acontece da seguinte maneira: o invasor transmite a transação para o minerador e então a inclui na blockchain. Entretanto não seria a correta e sim uma falsa, então seria transmitido esse blockchain ao comerciante, que erroneamente liberaria a mercadoria acreditando se tratar de uma blockchain válida, mas quando esse blockchain for inserido novamente a verdadeira rede será rejeitada por ela.

Assim explica Ethan Heilman et al. (2015):

“The attacker sends its transaction to the eclipsed miners, who incorporate it into their (obsolete) view of the blockchain. The attacker then shows this view of blockchain to the

eclipsed merchant, receives the goods, and sends both the merchant and eclipsed miners the (non-obsolete) view of blockchain from the non-eclipsed miners.”

Como podemos ver, esse ataque tem grande potencial lesivo, que pode causar muitos danos a economia, ou então usar como forma de dificultar o trabalho da concorrência. Entretanto a chance de tal ataque acontecer e obter sucesso contra a bitcoin são baixas, mas se tratando de altcoins essa possibilidade se torna muito maior.



17

3. REGULAÇÃO DO BITCOIN

3.1. ETIMOLOGIA DA PALAVRA REGULAÇÃO

Para entender a regulação da bitcoin, é necessário que antes se entenda o que é a regulação no aspecto do direito.

¹⁷ **BITCOIN.NET.** Double Spend. Bitcoin.net. acessado em 30 de agosto de 2020. Disponível em: <http://bitcoins.net/guides/double-spend.asp>.

Regulação no dicionário Michaelis é definido como “*ato ou efeito de regular(-se)*”, porém no sentido jurídico, pode ser entendida como uma intervenção indireta do Estado, sendo ela uma atividade pertencente apenas a ele.

“A regulação econômico-social consiste na atividade estatal de intervenção indireta sobre a conduta dos sujeitos públicos e privados, de modo permanente e sistemático, para implementar as políticas de governo e a realização dos direitos fundamentais” (FILHO, Marçal Justen, 2013 p. 677)”.

Portanto a regulação pode ser entendida como uma forma de demandar certas condutas a determinadas pessoas envolvidas, servindo como um norte para os indivíduos, quando os mesmos precisarem tomar alguma decisão.

3.2. NATUREZA JURÍDICA DA BITCOIN

Para ocorrer a regulação da bitcoin é necessário que seja identificado sua natureza jurídica, pois quando estiver identificada poderá então se utilizar do correto tratamento jurídico.

O Brasil possui vários órgãos regulamentadores, onde cada um dispõe de atribuições legais e expertises diferentes, sendo assim é necessário que ocorra a identificação da natureza jurídica das criptomoedas, para assim utilizar o tratamento jurídico adequado a estas.

3.3. BITCOIN COM NATUREZA JURÍDICA DE ATIVO

Como já demonstrado no presente trabalho, as criptomoedas possuem várias características próprias, o que dá margem para podermos considera-las um ativo financeiro.

Antes de adentrarmos na classificação da bitcoin em ativo, é necessário entender alguns tipos existentes de ativos: ativo de capital, ativo monetário, ativo financeiro e ativo tóxico.

Os Ativos denominados capital, são aqueles de propriedade, tal como carro, casas, terrenos ou até mesmo itens colecionáveis.

O segundo ativo a ser tratado é conhecido como monetário ou circulante, que diz respeito ao montante em que a empresa possui em caixa, bancos. O que é devido ou também aquilo que pode ser convertido em dinheiro como matérias primas de bens produzidos, e até mesmo a bitcoin.

O terceiro ativo é o financeiro, que é aquele que não é físico, e possui um valor oriundo de contratos, títulos e ações que podem ser negociados nos mercados financeiros.

O quarto ativo denominado tóxico, oferece um grande risco, que é tão elevado que quando comprado já está ou pode acontecer a queda.

Atualmente a Receita Federal Brasileira considera as criptomoedas como ativo financeiro em seu sentido *lato sensu*, ou seja, seu posicionamento tem um conceito amplo com objetivo regular todas as peculiaridades encontradas nas criptomoedas.

Embora a RFB venha a considerar as moedas digitais como ativo financeiro, essa definição não vem contemplada em nossa legislação, o que faz com que haja necessidade de procurar sua definição em outros meios. “Ativo financeiro: título emitido por instituições e empresas para manter a riqueza de quem o possui, sendo ainda um passivo para quem fez a emissão” (DINIZ, 2007. P.344).

Sendo assim, ativos financeiros podem ser créditos, contratos ou qualquer outro instrumento que representa algum tipo de dívida, portanto, em decorrência das criptomoedas não terem qualquer tipo de obrigação de pagamento com o seu uso, a definição descrita acima faz com que ele se enquadre perfeitamente.

Desta forma podemos concluir que as criptomoedas podem ser consideradas ativos financeiros desde que estejam presentes as informações necessárias, ou seja, quando é usada para basear dados em escriturações de títulos de créditos.

3.4. BITCOIN COM NATUREZA JURÍDICA DE COMMODITY

As commodities são artigos/bens de comércio que não estão sujeitos a processos de modificação. É “um artigo utilizado em troca ou comércio, sendo que este conceito somente abrange bens tangíveis tais como produtos e mercadorias, distinguindo-se de serviços.” (EIZIRICK, Nelson et al. 2011. P. 237).

Sendo assim, é possível entender que commodities são aqueles bens tangíveis que podem ser utilizados para trocas ou comércios.

A Bitcoin poderia ser classificada como *commodities*, embora seja um pouco forçado esse enquadramento, é possível observar que essas moedas digitais não poderiam ser consideradas como moedas pela legislação brasileira, em razão de não conseguir atender a relação de taxas.

A corrente de pensamento que defende que as criptomoedas deveriam ser consideradas como commodity, utilizam o argumento de que no geral essas moedas possuem valor econômico, e, portanto, contém o necessário para serem tratadas como bens. Além disso, elas se comportam - de maneira econômica - muito semelhante as commodities, sendo possível encontrar em tribunais estrangeiros decisões que alegam que as criptomoedas não possuem os requisitos para serem consideradas "DINHEIRO", assim deveriam ser chamadas de commodities.

3.5. BITCOIN COM NATUREZA DE MOBILIÁRIO

Valor mobiliário - também denominado título financeiro - é um título de propriedade ou de crédito, no qual pode vir a ser emitido por um ente público ou privado - sociedade anônima ou instituição financeira - que tem como órgão fiscalizador a CVM (comissão de valores mobiliários).

No Brasil, valor mobiliário pode ser encontrado na lei nº 6.385 de dezembro de 1976. Porém, a legislação trouxe a definição de forma indireta em seu art. 2º, sendo possível verificar o que pode ser considerado valor mobiliário.

“Art. 2º São valores mobiliários sujeitos ao regime desta Lei:

I - As ações, debêntures e bônus de subscrição;

II - Os cupons, direitos, recibos de subscrição e certificados de desdobramento relativos aos valores mobiliários referidos no inciso II;

III - os certificados de depósito de valores mobiliários;

IV - As cédulas de debêntures;

V - As cotas de fundos de investimento em valores mobiliários ou de clubes de investimento em quaisquer ativos;

VI - As notas comerciais;

VII - os contratos futuros, de opções e outros derivativos, cujos ativos subjacentes sejam valores mobiliários;

VIII - outros contratos derivativos, independentemente dos ativos subjacentes; e

IX - Quando ofertados publicamente, quaisquer outros títulos ou contratos de investimento coletivo, que gerem direito de participação, de parceria ou de remuneração, inclusive resultante de prestação de serviços, cujos rendimentos advêm do esforço do empreendedor ou de terceiros.”

Fabio Ulhôa, nos expõe em seu livro de direito comercial que:

“A definição legal de valor mobiliário é larga o suficiente para alcançar as mais variadas operações de oferta pública de investimentos coletivos, tendo atendido de modo satisfatório aos problemas surgidos com o sistema de listagem anteriormente empregado no Brasil. Não se pode deixar de notar, contudo, que sua amplitude é um tanto exagerada”(VERÇOSA 1997, apud Coelho)

Sendo assim, valor mobiliário são todos aqueles listados no art. 2º da lei 6.385/76 ou qualquer outro que venha a ser criado por regulamentação/lei específica.

Em razão da tecnologia Blockchain nos prestar informações a respeito da origem e todo o caminho que o título percorreu até o momento em que se realiza a pesquisa que trata da eventual ação, podemos considerar que as moedas digitais pode ser uma ação escritural, obtendo assim a natureza de valor mobiliário.

Entretanto, pelo fato da bitcoin não se originar de uma pessoa jurídica, não advém de um negócio realizado por terceiro, e sim através de um código aberto, que pode ser achado disponível na internet, tornando-se acessível por qualquer pessoa em qualquer lugar do mundo, ao contrário de valores mobiliários que se encontram apenas vinculados a pessoas jurídicas e estão sujeitos a supervisão do Estado, enquanto que a bitcoin é supervisionado por todos.

3.6. A FALTA DE REGULAÇÃO DO BITCOIN

Como já comentado no presente trabalho, as moedas digitais carecem de legislação específicas para trata-las, o que resulta a ocorrência de lacunas. “As leis e regulações atuais não preveem uma tecnologia como a Bitcoin, o que resulta em algumas zonas legais cinzentas”. (Ulrich, 2014).

Essa falta de legislação ocorre pelo fato de a bitcoin e as moedas digitais em geral, serem muito recentes, gerando uma falta de definições legislativas - já existentes - no ordenamento jurídico em que ela possa ser encaixada, pois quando se trata a respeito de moedas ou até mesmo de qualquer meio financeiro ou instituições, é preciso que se utilize analogia quando há necessidade de tratar sobre o assunto, porém essa analogia ocorre de maneira complexa, pois é difícil saber qual lei poderia ser aplicada ao caso e como aplicá-la. “O Bitcoin não se encaixa em definições regulamentares existentes de moeda ou outros instrumentos financeiros ou instituições, tornando complexo saber quais leis se aplicam a ele e de que forma. (Ulrich, 2014).

A falta de legislação em relação as moedas digitais tem impacto também em sua tributação, pois há uma grande dificuldade de identificar a quem pertence a competência tributária quando se trata de negócios ou de situações jurídicas em que se utiliza as criptomoedas.

3.7. INSTRUÇÃO DA RECEITA FEDERAL

A Receita Federal nos instrui que nos casos em que houver movimentação acima de R\$ 30.000,00 (trinta mil reais) ao mês em moedas digitais, deverá ser declarado no imposto de renda e também, recolher 15% em tributo.

Portanto, entende-se que embora as criptomoedas não sejam consideradas moedas e não há regulamentação, elas devem ser equiparadas a ativos financeiros, sendo assim, deve ser declarada pelo valor de aquisição em seu imposto de renda, conforme instrução normativa da receita federal em anexo.

3.8. REGULAÇÃO NO BRASIL

No Brasil a regulação das criptomoedas está em sua fase inicial, pois existe uma evidente série de desafios existente para os órgãos reguladores. Grande parte deles são em relação a sua emissão e a seu funcionamento, afinal um dos motivos de sucesso dessas moedas, diz respeito a sua independência que quase impossibilita a atuação estatal. Todavia, há um grupo com entendimento de que as criptomoedas, por se tratar de uma tecnologia - no qual é distribuída e descentralizada - o Estado não deveria intervir, porém é necessário que haja regulação por parte do mesmo nem que seja mínima, pois a falta da

regulação adequada pode gerar consequências ruins que certamente atingirão a sociedade.

A autorregulação acabou se tornando uma saída pela falta da devida regulação, pois embora ela tenha um status de contrato, quando se choca com a legislação, acaba gerando efeitos apenas entre os usuários que a aceitaram, diferentemente da regulação tradicional em que o Estado impõe e assim somos obrigados a seguir. Em contrapartida, a autorregulação é praticamente – inteiramente - composta pela característica de ser voluntária.

Atualmente no Brasil, há alguns projetos de leis tramitando na câmara dos Deputados, que visam regulamentar as criptomoedas. Dentre eles podemos citar o projeto de lei nº 2.303/15 e nº 2.060/19.

3.9. PROJETO DE LEI Nº2.303/15

O projeto de lei nº 2.303/15 de autoria do Sr. Áureo que tramita na câmara dos deputados, se encontra em fase de audiência. Esse projeto tem como objetivo enquadrar as moedas digitais e o programa de milhagens aéreas na definição de “arranjos de pagamento” no qual teria como supervisor o banco central.

É possível observar a lei em seu inteiro teor em anexo no presente trabalho.

4. O BITCOIN NO COMETIMENTO DE CRIMES

4.1. LAVAGEM DE DINHEIRO UTILIZANDO BITCOIN

Antes de adentrarmos no tema do uso da Bitcoin para cometimento de crimes, é necessário entender o que é a lavagem de dinheiro.

Lavagem de dinheiro ou “branqueamento de capitais”, é oriunda da lei 9.613 de 1998 que foi posteriormente modificada pela lei 12.683 de 2012. Trata-se de um crime com a finalidade de ocultar ou dissimular a origem ilícita de ativos financeiros ou bens patrimoniais.

A seguir veremos a lei em seu inteiro teor:

“Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal.

Pena – reclusão, de 3 (três) a 10 (dez) anos, e multa.

§ 1º Incorre na mesma pena quem, para ocultar ou dissimular a utilização de bens, direitos ou valores provenientes de infração penal:

I – Os converte em ativos lícitos;

II – Os adquire, recebe, troca, negocia, dá ou recebe em garantia, guarda, tem em depósito, movimenta ou transfere;

III- Importa ou exporta bens com valores não correspondentes aos verdadeiros.

§ 2º Incorre, ainda, na mesma pena quem:

I – Utiliza, na atividade econômica ou financeira, bens, direitos ou valores provenientes de infração penal; II – Participa de grupo, associação ou escritório tendo conhecimento de que sua atividade principal ou secundária é dirigida à prática de crimes previsto nesta Lei.

§ 3º A tentativa é punida nos termos do parágrafo único do art. 14 do Código Penal.

§ 4º A pena será aumentada de um a dois terços, se os crimes definidos nesta Lei forem cometidos de forma reiterada ou por intermédio de organização criminosa.

§ 5º A pena poderá ser reduzida de um a dois terços e ser cumprida em regime aberto ou semiaberto, facultando-se ao juiz deixar de aplicá-la ou substituí-la, a qualquer tempo, por pena restritiva de direitos, se o autor, coautor ou partícipe colaborar espontaneamente com as autoridades, prestando esclarecimentos que conduzam à apuração das infrações penais, à identificação dos autores, coautores e partícipes, ou à localização dos bens, direitos ou valores objeto do crime.”

Após breve leitura do referido artigo, pode-se observar que a lei abrange a definição de lavagem de dinheiro para aquele indivíduo que utiliza - na atividade econômica ou financeira - aqueles bens que são frutos da infração penal.

Há uma corrente de pensamentos que acredita que essa lei tem o objetivo de proteger um bem jurídico que já foi lesado em um crime antecedente, gerando como consequência uma necessidade de se identificar qual foi o crime praticado anteriormente a lavagem de dinheiro. Entretanto, tal posicionamento caracterizaria *bis in idem*, uma vez que o autor do crime antecedente pode ser o mesmo que cometerá o crime de lavagem de dinheiro, e no Direito Penal Brasileiro é vedado a dupla punição do agente, quando se trata de violação do mesmo bem jurídico.

“Ainda que se exija uma relação entre os crimes, os bens tutelados são materialmente distintos, o que confere autonomia ao crime de lavagem, legítima sua punição

em concurso material com o crime antecedente, no caso de identidade de autoria, e justifica a fixação da mesma pena para todos os casos de lavagem, seja qual for o delito original.”(BADARÓ e BOTTINI, 2019)

É importante destacar que embora a lavagem de dinheiro seja um processo único, possui uma metodologia dividida em 3 (três) fases caracterizadoras do crime, todas distintas entre si, são elas:

- 1ª fase: É a colocação dos recursos oriundos de uma atividade ilegal em qualquer tipo de aparato que dissimule a origem do dinheiro, por exemplo, enviar uma quantidade de moedas para o exterior utilizando-se meios não oficiais como doleiros, convertendo em ativos não financeiros etc. O importante é destacar que será utilizado qualquer meio que aparentemente são lícitos.
- 2ª fase: Esta tem o objetivo de afastar o recurso de sua origem ilícita, para que assim dificulte o seu rastreamento, e conseqüentemente a descoberta do crime. Pode ser citado como exemplo a realização de exportações superfaturadas ou até mesmo fictícias.
- 3ª fase: esta etapa tem o objetivo de criar uma falsa origem lícita para o produto fruto de atividades ilícitas, para que assim possa se utilizar o dinheiro para proveito pessoal. Pode ser citado como exemplo a utilização de ativos como obras de arte ou pedras preciosas, pois o dinheiro proveniente dessa venda não teria a necessidade de ser levado, uma vez que, será supostamente lícita sua origem, e o que realmente foi lavado foi o ativo original.

Após feitas as considerações a respeito do crime de lavagem de dinheiro e suas principais características, podemos relacionar o crime tratado utilizando-se as bitcoins.

Como já citado no presente trabalho, as criptomoedas em geral carecem de normas ou mesmo de tratados internacionais ratificado pelo Estado. Também falamos sobre sua facilidade para realizar transferências - e mais importante - sem registro bancário. Além disso, podemos observar que as Exchange carecem de qualquer tipo de fiscalização que possa impedir a lavagem de dinheiro, o que resulta em um aumento exponencial desse crime por utiliza-la como instrumento para sua execução.

Recentemente foi descoberto pelas autoridades uma nova maneira de lavar dinheiro, onde os criminosos misturam a bitcoin e depois as trocam por novas transações

legais. Esse procedimento ocorre de diversas maneiras, há formas simples como, por exemplo, a troca por moeda estrangeira desse ativo para outro ativo em espécie e, logo em seguida a realização da transferência para a bitcoin.

É de suma importância salientar que apenas obter a bitcoin com dinheiro ilícito, não configura o crime de lavagem de dinheiro, em razão de não ter havido a reinserção na economia formal. Sendo assim, para caracterizar o crime é necessário que se utilize a bitcoin para aquisição de bens ou vende-la, e assim fazer com que o dinheiro retorne a economia formal.

Como já tratado no presente trabalho, o crescimento da bitcoin fez com que o lançamento de caixas eletrônicos para realização de transações fosse tido como um grande passo. Porém, tal medida contribuiu também para lavar dinheiro, visto que facilitou a realização de transações, o que chamou a atenção de autoridades do mundo inteiro que buscam medidas para impedir a ocorrência desse crime. Contudo, até agora apenas o Canadá tomou medidas, estipulando uma lei na qual os caixas eletrônicos devem fornecer informação quando houver transação com valor acima de US\$10.000,00 (dez mil dólares), sendo assim, a tendência é ocorrer a regulação.

4.2. FRAUDE USANDO BITCOIN

Antes de adentrarmos no assunto da fraude utilizando a bitcoin há a necessidade de entender o que é fraude.

Fraude é descrito no **dicionário Michaelis** como:

“1 -Ato de má-fé que tem por objetivo fraudar ou ludibriar alguém; cantiga, engano, sofisticação; 2- Mentira ardilosa; sicofantia; 3- Entrada ilegal de produtos estrangeiros, sem o pagamento dos tributos alfandegários; 4- Ato de falsificar documentos, marcas e produtos.”

Sendo assim, fraude consiste em enganar outrem com propósito de prejudica-lo e tem o objetivo principal de obter alguma vantagem pessoal.

Há diversos tipos de fraude e maneiras de se cometer, uma das mais conhecidas e mais comum no dia a dia é o estelionato, que vem descrito no art. 171, do código penal, que consiste em: “obter para si ou outrem, vantagem ilícita, em prejuízo alheio, induzindo

ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: pena- reclusão, de um a cinco anos, e multa”

Tal crime ocorre quando o sujeito se utiliza de qualquer meio fraudulento, que resulte na indução da vítima ao erro ou então a mantém nessa situação, e com isso obtém uma vantagem indevida para si ou para outrem, e como consequência causa dano patrimonial a alguém.

Há alguns pensadores que entendem que ela pode ser dividida em fraude Penal e fraude Civil, embora não haja distinção em sua natureza ontológica.

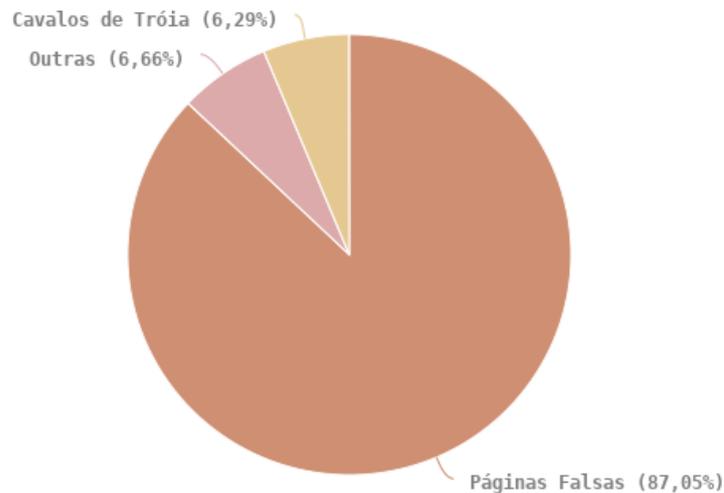
Mirabete em seu Manual de Direito Penal (2016), nos ensina que:

“Não há fraude penal e fraude civil; a fraude é uma só. Pretendida distinção sobre o assunto é supérflua, arbitrária e fonte de danosíssimas confusões. O que importa verificar, pois, é se, em determinado fato, se configuram todos os requisitos do estelionato, caso em que é sempre punível, sejam quais forem as relações, a modalidade e a contingência do mesmo” (MIRABETE E FABBRINI, 2016. p.288)

No Brasil as fraudes podem ser encontradas e tipificadas no art.171 e seguintes do Código Penal brasileiro, e as demais fraudes se encontram em códigos legais específicos como, por exemplo, a fraude eleitoral, fiscal entre outras.

O instituto CERT.BR nos traz um gráfico de incidentes de tentativa de fraude dividido em formas de cometimento:

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2019
Tentativas de fraudes



© CERT.br – by Highcharts.com 18

- **Cavalos de Tróia:** Tentativas de fraude com objetivos financeiros envolvendo o uso de cavalos de Tróia.
- **Páginas Falsas:** Tentativas de fraude com objetivos financeiros envolvendo o uso de páginas falsas.
- **Outras:** Outras tentativas de fraude.

É notável que as fraudes cibernéticas acontecem com maior frequência com o uso de páginas falsas, que muitas vezes são utilizadas para enganar investidores de moedas digitais.

A falta de regulação da bitcoin - já demonstrado acima - traz consigo várias possibilidades de os usuários sofrerem fraudes.

A fraude com bitcoin tem sido uma infração penal muito comum em razão da sua facilidade de cometimento, como por exemplo, quando as vítimas entregam bitcoin pra Exchanges e eles por sua vez, somem com o montante da vítima.

¹⁸**CERT.BR.** Estatísticas. Cert.Br. acessado dia 25 de julho de 2020. Disponível em: <https://www.cert.br/stats/incidentes/2019-jan-dec/fraude.html>.

No Brasil grande parte das fraudes, ocorreram com os infratores prometendo as vítimas um grande retorno em dinheiro em pouco tempo, desde que a vítima depositasse um valor inicial e, então o criminoso sumia com a quantia depositada.

Há também situações semelhantes envolvendo pessoas jurídicas, onde estas solicitavam que as vítimas deixassem um montante de dinheiro sobre sua custódia prometendo aplica-la de maneira eficiente, porém o dono fugia ou gastava essa quantia.

Como observado, a falta de regulação das criptomoedas no Brasil facilita o cometimento deste crime, que - consequentemente - acaba sujando o nome dos criptoativos.

4.3. PIRÂMIDES FINANCEIRAS E A BITCOIN

A Pirâmide Financeira com bitcoin tem sido um crime muito frequente, porém para entendermos melhor como este delito ocorre com a utilização da criptomoeda, é necessário entendermos melhor no que ele consiste.

O crime tratado no presente tópico, trata-se de uma pratica de negócios fraudulentos, que consiste na captação rotineira de pessoas, que normalmente pagam uma taxa pra adentra-la com a promessa de receber lucro ou qualquer tipo de vantagem indevida em um curto espaço de tempo, ou seja, é obviamente um negócio que não tem como dar certo, afinal quando param de entrar aplicadores no esquema, ele se torna insustentável em um nível que não há como ter retorno algum de investimento.

A CVM (comissão de valores mobiliários) tem notado que houve um aumento expressivo no número de denúncias envolvendo esse tipo de fraude no ano de 2019. José Alexandre Vasco (apud BOMBANA), superintendente de proteção e orientação aos investidores da CVM, afirmou que: “Estamos lidando com um aumento sem precedentes no número de denúncias¹⁹”. Tal afirmação respalda-se no fato de ter havido um recorde nas

¹⁹ BOMBANA, Lucas. **CVM intensifica fiscalização sobre pirâmides financeiras, em especial as que envolvem criptomoedas**. IstoÉ Dinheiro. acessado em 30 de julho de 2020. Disponível em: <https://www.istoedinheiro.com.br/sempre-alerta/>

denúncias desse crime chegando no total de 250 denúncias no ano de 2019, ou seja, um aumento de 140% em relação ao ano anterior.

INVESTIDORES ILUDIDOS

Em cinco anos, total de reclamações na CVM cresceu quase dez vezes. Cada denúncia pode envolver até milhares de pessoas lesadas



(a) Inclui denúncias contra pessoas físicas e empresas não registradas na autarquia

(b) Estimativa; até 27 de maio foram abertos 104 processos

Fonte: CVM

20

O crime em questão tem sido tão frequente que foi atribuído ao mesmo algumas fases, são elas:

- 1 fase: Euforia, momento em que o número de investidores está crescendo exponencialmente, permitindo assim que os mais antigos consigam sacar.
- 2 fases: Nessa fase o crescimento de investidores paralisa, e desta forma a empresa começa a atrasar pagamentos e saques.

²⁰ Op.cit. IstoÉ. Disponível em: <https://www.istoedinheiro.com.br/sempre-alerta/>.

- 3 fases: Acontece no momento em que a empresa não consegue pagar os saques²¹.

Após a explicação do que se trata a pirâmide financeira, podemos relacioná-la as moedas digitais. As conhecidas “aplicações de moedas digitais” têm recebido uma atenção especial da fiscalização, em razão de seu grande aumento de investidores que recebem a promessa de enormes ganhos.

Atualmente, esse tipo de pirâmide envolvendo as moedas digitais se encontram em um modelo de negócio denominado “marketing multinível”, que prometem ao investidor um ganho de 10% em sua primeira indicação, e conforme aumenta o número de indicações a porcentagem cai pra 4% e depois para 1%, ou seja, nada mais é do que a tradicional pirâmide financeira, pois as empresas com más intenções que não utilizam de produtos que são economicamente sustentáveis, tendem a quebrar, afinal não há mais sustentação.

No Brasil atualmente, o crime de pirâmide financeira se encontra no art. 2º, inciso IX da lei nº 1.521/51 que dispõe a respeito dos crimes contra a economia popular.

O MPF (Ministério Público Federal) em razão do alto crescimento do crime, disponibilizou aos cidadãos brasileiros um guia prático com o objetivo de conscientizar as pessoas a identificarem as diferenças entre um investimento financeiro e um golpe²².

4.4. BITCOIN E A SONEGAÇÃO FISCAL

Antes de entrarmos no assunto do tópico é necessário entender o que é o imposto de renda e base legal utilizada para sua tributação.

O Brasil possui uma legislação tributária que presa a utilização do Princípio da Capacidade Contributiva. Tal princípio remete a ideia de que deve haver mais igualdade em relação a cobrança, pois dessa forma aqueles que tem muito pagam mais do que aqueles que possuem pouco.

²¹ **EXAME**, Pirâmides de Bitcoin: perda pode acabar com economias. Saiba evitar. Exame. Acessado dia 02 de agosto de 2020. Disponível em: <https://exame.com/seu-dinheiro/piramides-de-bitcoin-perda-pode-acabar-com-economias-saiba-evitar/>

²² **O MPF de olho nas pirâmides financeiras: saiba como distinguir um investimento financeiro de um golpe.** – Brasília: MPF/2ªCCR, 2016. Acessado em 02 de agosto de 2020. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/cartilhas/guia-pratico-piramides-financeiras>

“Na realidade, a expressão capacidade contributiva em sua origem foi genericamente considerada como sinônimo de riqueza ou de patrimônio, indicando as forças econômicas individuais que propiciavam o pagamento diferenciado dos tributos. A carga tributária seria então proporcional à riqueza ou ao patrimônio acumulado”. (MEIRELLES, José Ricardo, 1997, p.334).

A Constituição Federal de 1988 em seu art. 145, §1, dispõe a respeito da capacidade contributiva:

“ART. 145. - A União, os Estados, o Distrito Federal e os Municípios poderão instituir os seguintes tributos:

§1-Sempre que possível, os impostos terão caráter pessoal e serão graduados segundo a capacidade econômica do contribuinte, facultando à administração tributária, especialmente para conferir efetividade a esses objetivos, identificar, respeitados os direitos individuais e nos termos da lei, o patrimônio, os rendimentos e as atividades econômicas do contribuinte.”

Essa mesma constituição federal, em seu art. 153, inciso III, explica quais são os impostos que competem a união:

“ART. 153 -Compete à União instituir impostos sobre:

- I - Importação de produtos estrangeiros;
- II - Exportação, para o exterior, de produtos nacionais ou nacionalizados;
- III - renda e proventos de qualquer natureza;
- IV - Produtos industrializados;
- V - Operações de crédito, câmbio e seguro, ou relativas a títulos ou valores mobiliários;
- VI - Propriedade territorial rural;
- VII - grandes fortunas, nos termos de lei complementar.”

Após breve leitura do exposto artigo, especificamente em seu inciso III, é possível observar que a competência do imposto de renda pertence à União, e a mesma o faz através do órgão denominado Receita Federal.

Resta ainda a dúvida a respeito de como é calculado o valor que será cobrado pelos bens, entretanto por ser um assunto muito extenso e que não é interessante para o presente trabalho, falaremos apenas do cálculo com a bitcoin.

Atualmente a Receita Federal faz uma tributação progressiva em relação a Bitcoin, ou seja, a cobrança varia em relação ao lucro obtido. Abaixo é possível observar na tabela

quais

as

porcentagens:

Alíquota de IR	Ganho de capital
15%	Até R\$ 5 milhões de lucro
17,5%	Acima de R\$ 5 milhões até R\$ 10 milhões
20%	Acima de R\$ 10 milhões até R\$ 30 milhões
22,5%	Acima de R\$ 30 milhões

23

Entretendo cada caso possui regras específicas²⁴, são elas:

- Pessoas físicas que negociam sem intermediário entre si: quando há esse tipo de negociação haverá a necessidade de prestar contas quando realizar uma movimentação acima de R\$ 30.000,00 (trinta mil reais), tal prestação será realizada através da DARF (Documento de Arrecadação da Receita Federal).
- Pessoas físicas que negociam utilizando corretoras brasileiras: Nesse caso o indivíduo que utiliza o CPF (cadastro de pessoa física) terá que declarar no imposto de renda anualmente.
- Quando diz respeito as Corretoras: As corretoras terão obrigação de informar ao Fisco todas as transações que realizarem para seus clientes, independentemente do valor, e ainda nos casos de atraso da entrega de tal informação, a corretora receberá multa de 500 reais quando for pessoa jurídica que está iniciando a sua atividade ou que se encontra imune/isenta pelo simples. Caso a empresa não se enquadre no que foi dito acima, essa

²³ **SEU DINHEIRO.** Como declarar bitcoin e outras criptomoedas no imposto de renda. Seu Dinheiro. acessado em 30 de julho de 2020. Disponível em: <https://www.seudinheiro.com/2020/imposto-de-renda/como-declarar-bitcoin-e-outras-criptomoedas-no-imposto-de-renda/>

²⁴ ZOGBI, Paula. **Novas regras do Imposto de Renda: como declarar bitcoin e outras criptomoedas.** InfoMoney. Acessado em 30 de julho de 2020. Disponível em: <https://www.infomoney.com.br/minhas-financas/novas-regras-do-imposto-de-renda-como-declarar-bitcoin-e-outras-criptomoedas/>

multa sobe para R\$ 1.500,00 (um mil e quinhentos reais) por mês, e se a corretora omitir, passar dado incorreto ou incompleto, a multa será de 3%.

- Pessoas físicas que utilizam corretoras estrangeiras: Quando se utiliza esse tipo de corretora, é necessário declarar todo mês quando o valor das operações ultrapassar os R\$ 30.000,00 (trinta mil reais).

É importante destacar que quando se tratar de declaração envolvendo bitcoin, só será necessário declarar desde que a negociação ultrapasse o piso de R\$ 35.000,00 (trinta e cinco mil reais), ou seja, se o sujeito comprar bitcoin em um valor de R\$ 20.000,00 (vinte mil reais) e o vendeu por 10 mil, houve então prejuízo, em outras palavras ele não obteve ganho de capital, sendo assim não tem necessidade de recolher imposto. Entretanto, se nessa situação hipotética o sujeito tivesse vendido a bitcoin há R\$ 16.000,00 (dezesesseis mil reais) fazendo com que o valor da transação seja de R\$ 36.000,00 (trinta e seis mil reais), é necessário o pagamento do imposto de renda sobre a diferença.

Tal método exposto acima ajuda com que os investidores sejam mais organizados. O consultor da Exchange XDEX²⁵, Paulo Junqueira apud Gregorio, explica que:

“É como se fosse um registro contábil, entradas e saídas independentes, apurando o ganho em cada transação. Às vezes o contribuinte tem, entre aspas, ‘preguiça’, e escolhe declarar um valor médio de compras e vendas, mas isso não é aceito pela Receita”.

A Receita Federal afirma expressamente a necessidade de declaração das moedas digitais e como deve ser feito.

“445 — As moedas virtuais devem ser declaradas? Sim. As moedas virtuais (bitcoins, por exemplo), muito embora não sejam consideradas como moeda nos termos do marco regulatório atual, devem ser declaradas na Ficha Bens e Direitos como “outros bens”, uma vez que podem ser equiparadas a um ativo financeiro. Elas devem ser declaradas pelo valor de aquisição.

[...]

606 — Os ganhos obtidos com a alienação de moedas “virtuais” são tributados? Os ganhos obtidos com a alienação de moedas virtuais (bitcoins, por exemplo) cujo total alienado no mês seja superior a R\$ 35.000,00 são tributados, a título de ganho de

²⁵ GREGORIO, Rafael. **Como declarar bitcoins e outras criptomoedas no imposto de renda.** Valor Investe. Acessado em 30 de julho de 2020. Disponível em: <https://valorinveste.globo.com/mercados/cripto/noticia/2020/03/09/como-declarar-bitcoins-e-outras-criptomoedas-no-imposto-de-renda.ghtml>

capital, segundo alíquotas progressivas estabelecidas em função do lucro, e o recolhimento do imposto sobre a renda deve ser feito até o último dia útil do mês seguinte ao da transação. O contribuinte deverá guardar documentação que comprove a autenticidade das operações “²⁶”.

Há casos em que há a utilização da bitcoin para o pagamento de contas, nessas hipóteses é preciso observar se houve um gasto na negociação acima de R\$ 35.000,00 (trinta e cinco mil reais) o que torna o ganho tributável, sendo assim, se eu utilizo a criptomoeda para pagar uma conta de R\$ 60.000,00 (sessenta mil reais) terei que pagar imposto.

Após a explicação acima, podemos adentrar ao assunto do tópico em questão. O crime de Sonegação Fiscal que está previsto na lei nº 4.729/65, que traz em seus incisos do art.1º condutas que caracterizam sonegação:

“Art. 1º Constitui crime de sonegação fiscal:

I - Prestar declaração falsa ou omitir, total ou parcialmente, informação que deva ser produzida a agentes das pessoas jurídicas de direito público interno, com a intenção de eximir-se, total ou parcialmente, do pagamento de tributos, taxas e quaisquer adicionais devidos por lei;

II - Inserir elementos inexatos ou omitir, rendimentos ou operações de qualquer natureza em documentos ou livros exigidos pelas leis fiscais, com a intenção de exonerar-se do pagamento de tributos devidos à Fazenda Pública;

III - alterar faturas e quaisquer documentos relativos a operações mercantis com o propósito de fraudar a Fazenda Pública;

IV - Fornecer ou emitir documentos gratuitos ou alterar despesas, majorando-as, com o objetivo de obter dedução de tributos devidos à Fazenda Pública, sem prejuízo das sanções administrativas cabíveis.

V - Exigir, pagar ou receber, para si ou para o contribuinte beneficiário da paga, qualquer percentagem sobre a parcela dedutível ou deduzida do imposto sobre a renda como incentivo fiscal.

Pena: Detenção, de seis meses a dois anos, e multa de duas a cinco vezes o valor do tributo.”

É importante destacar que todos os crimes subscritos acima, são dolosos, sendo assim, há a necessidade de o indivíduo ter uma livre vontade e conhecimento de que está praticando-o.

²⁶ **PERGUNTAS E RESPOSTAS 2020**. Receita Federal. Acessado em 01 de agosto de 2020. Disponível em: http://receita.economia.gov.br/interface/cidadao/irpf/2020/perguntao/pr-irpf-2020-v-1-2-2020-04-13_publicacao.pdf

Entretanto, a lei acima não foi “forte” o suficiente para combater a infração tratada, o que gerou o surgimento da lei de nº 8.137/90, que dispõe em seu dispositivo legal a inteira matéria contida na lei anterior, só que de maneira mais eficiente, visto que transformou os crimes antes formais em materiais ou de resultado, e também elevou a pena.

A Bitcoin não possui uma legislação específica, e possui certa anonimidade mesmo quando se utiliza as Exchange, pois já vimos que ela não é muito criteriosa nas criações de contas. Considerando esses pontos, é possível observar que existe uma certa facilidade em sonegar os impostos quando se trata de criptomoedas, afinal, caso não esteja usando Exchanges, não será possível a Receita Federal ter conhecimento de que o sujeito movimentou as moedas digitais e nem a quantidade, e muito menos quem é o indivíduo, e consequentemente adquire através desse ato anonimidade.

Como já tratado na presente obra, a ascensão da Bitcoin trouxe consigo a criação de caixas eletrônicos para facilitar e incentivar o uso dessa criptomoeda. Esse meio alternativo de realizar transações contribuiu para a prática do crime de sonegação fiscal, visto que esses caixas eletrônicos não notificam os órgãos governamentais sobre as transações. As autoridades do mundo inteiro veem então, que há uma necessidade de regular a utilização desses caixas.

4.5. CRIMES CIBERNÉTICOS E A BITCOIN

A invasão cibernética conhecida também como crimes digitais, crimes eletrônicos, crimes virtuais entre outros nomes, se consuma com o uso de dispositivos informáticos, podendo ocorrer com conexão a rede mundial de computadores – internet - ou não. Portanto, essa infração nada mais é do que qualquer ato ilegal no qual teve como objeto para a execução qualquer acessório tecnológico ou então delitos contra computadores.

Os doutrinadores, utilizam-se de classificações normativas que visam facilitar o tratamento ao crime, dentre essas classificações podemos destacar algumas, denominadas de puros, mistos e comuns e outra de próprios e impróprios.

Os crimes classificados como puro é em relação a conduta e a vontade do agente, que visa atacar o sistema do computador e/ou seus componentes, ou seja, atacar o hardware ou software do computador. Dessa forma, o indivíduo tem a intenção única de lesionar os equipamentos físicos, sistema informático e o banco de dados.

“O crime cibernético puro está relacionado a comportamentos ilícitos que objetivam especificamente a atacar sistema computacional e seus componentes, seja o hardware ou o software, abarcando ainda os dados e os sistemas em si. Nessa modalidade, a investida do agente tem por objetivo atingir o equipamento físico, o sistema informático e as informações dos bancos de dados. Nessa modalidade, exemplificativamente, temos a invasão de servidores e sites.” (Matsuyama e Lima, 2016, p.3)

A infração classificada como misto depende da utilização da internet para seu cometimento. Nesta o agente não busca lesionar o sistema do computador ou seus componentes físicos, mas se utiliza dos mesmo para concretizar o crime. Podemos usar como exemplo, casos em que o infrator usa informações ou aplicativos do lesionado para sacar dinheiro de sua conta. “O agente não dirige sua conduta ao sistema computacional ou a seus componentes, mas o uso da tecnologia é ferramenta primordial para a concretude da ação delinvente” (Matsuyama e Lima, 2016, p.3)

Já os crimes denominados comuns, são aqueles que o infrator utiliza a rede mundial de computadores como instrumento para consumação do crime, que já é tipificado pelo Código Penal, como por exemplo, quando o agente faz uso das redes sociais para executar a conduta no crime de difamação.

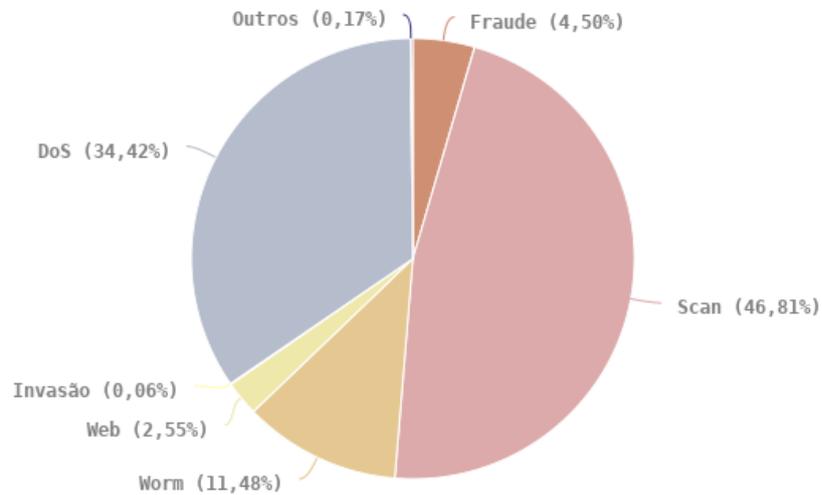
Podemos então agora tratar das classificações denominadas de próprios e impróprios, sendo que o primeiro se trata daqueles que o infrator se utiliza o sistema do lesionado para executar o crime. Tal categoria engloba todos os crimes de invasão de dados que o infrator não tenha autorização e também os crimes de interferência a dados informatizados, sendo assim, os crimes classificados como próprios dependem da utilização do computador.

Os impróprios são aqueles em que o agente utiliza-se de computadores para cometer crimes nos quais já estão tipificados no Código Penal, a diferença é que esses crimes podem ocorrer sem a utilização dos computadores, exemplo disso é o crime de pedofilia, que pode ser cometido com ou sem o uso de computadores.

No Brasil há a possibilidade de encontrar dados percentuais sobre a quantidade, tipos de crime e comparação com demais países a respeito de crimes cibernéticos, no site da CERT.Br (centro de estudos, respostas e tratamento de incidentes de segurança no Brasil) como observado no gráfico abaixo:

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2019

Tipos de ataque



© CERT.br -- by Highcharts.com 27

- **worm:** notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- **Dos (DoS -- Denial of Service):** notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **Invasão:** um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- **Web:** um caso particular de ataque que visa - especificamente - o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- **Scan:** notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

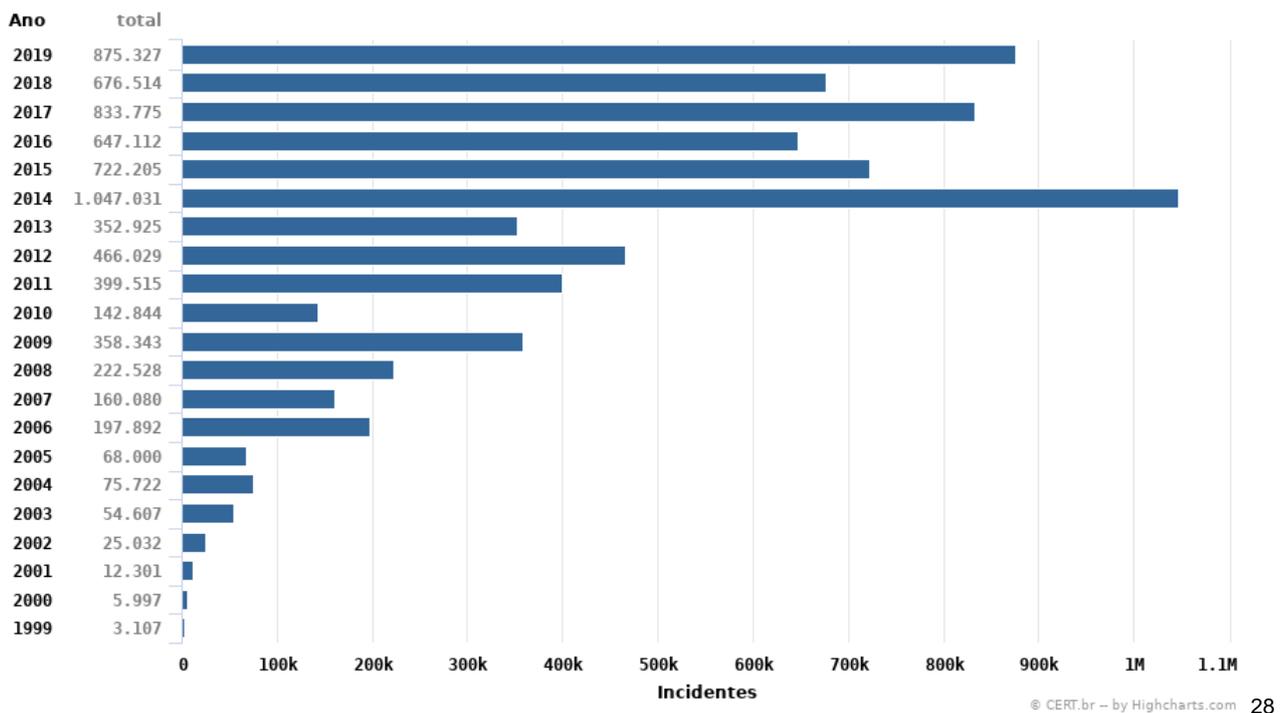
²⁷Op.Cit. Cert.Br. Disponível em: <https://www.cert.br/stats/incidentes/2019-jan-dec/tipos-ataque.png>. Acessado dia 5 de julho de 2020

- **Fraude:** segundo Houaiss, é "qualquer ato artiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
- **Outros:** notificações de incidentes que não se enquadram nas categorias anteriores.

O gráfico acima demonstra incidentes de crimes cibernéticos separados em tipos de ataques, sendo possível observar que as invasões cibernéticas possuem significativo percentual, visto que são mais difíceis de se cometer.

A seguir, será apresentado um gráfico com comparação de crimes cibernéticos do ano de 1999 ao de 2019:

Total de Incidentes Reportados ao CERT.br por Ano



Foi possível observar que os crimes cibernéticos tiveram um aumento expressivo nos últimos 3 anos, estando atrás apenas do ano de 2014, em razão desses crimes terem sido mais concentrados nos últimos 3 anos.

O Brasil teve como principal destaque nesses crimes, a criação da Lei de crimes cibernéticos, conhecida como lei Carolina Dieckmann (art. 154-A do Código Penal

²⁸ <https://www.cert.br/stats/incidentes/>

Brasileiro). Essa lei obteve grande destaque pelo episódio em que a atriz Carolina Dieckmann teve fotos íntimas vazadas. No âmbito jurídico teve grande importância, pois trouxe em seu dispositivo legal a tipificação dos atos de: invadir computadores, violar dados de usuários, divulgar informações privadas e “desconectar” sites. Tais condutas que são utilizadas rotineiramente nos crimes de *ransomware*, e com essa tipificação, houve facilidade em punir os responsáveis por esses delitos.

O MPF (Ministério Público Federal) nos apresentou uma coletânea de artigos que trataram do crime cibernético no ano de 2018, nessa coletânea há uma tabela, que consta informações a respeito de algumas formas de crimes cibernéticos comuns e seus respectivos artigos:

Tabela 1: Algumas tipificações de formas de crimes cibernéticos comuns

Crime	Tipificação
Estelionato e furto eletrônicos (fraudes bancárias)	arts. 155, §§ 3º e 4º, II, e 171 do CP
Invasão de dispositivo informático e furto de dados	art. 154-A do CP
Falsificação e supressão de dados	arts. 155, 297, 298, 299, 313-A, 313-B do CP
Armazenamento; produção; troca; publicação de vídeos e imagens contendo pornografia infantojuvenil	arts. 241 e 241-A, do ECA (Lei nº 8.069/1990)
Assédio e aliciamento de crianças	art. 241-D, do ECA (Lei nº 8.069/1990)
Ameaça	art. 147 do CP
<i>Cyberbullying</i> (veiculação de ofensas em blogs e comunidades virtuais)	arts. 138, 139, 140 do CP
Interrupção de serviço	art. 266, parágrafo 1º, do CP
Incitação e apologia de crime	arts. 286 e 287 do CP
Prática ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional	art. 20 da Lei nº 7.716/1989
Crimes contra a propriedade intelectual artística e de programa de computador	art. 184 do CP e Lei nº 9.609/1998
Venda ilegal de medicamentos	art. 273 CP

29

Tratando-se de crimes cibernéticos, há uma difícil tarefa que consiste em identificar para então punir os responsáveis. Quando falamos desse delito envolvendo a *bitcoin*, nos ocorre que essa criptomoeda utiliza uma rede *blockchain* de *peer-to-peer*, e acima de tudo é descentralizada, o que nos passa uma sensação de segurança. Entretanto, estas

²⁹ CAIADO, Felipe B. e CAIADO, Marcelo. **COMBATE À PORNOGRAFIA INFANTOJUVENIL COM APERFEIÇOAMENTOS NA IDENTIFICAÇÃO DE SUSPEITOS E NA DETECÇÃO DE ARQUIVOS DE INTERESSE** in Coletânea de artigos. Brasília, 2018, Volume 3. p.17.

características não impedem invasões cibernéticas, apenas o dificulta, visto que os hackers podem invadir todos os computadores que estão conectados à rede e assim obter acesso a rede blockchain. Contudo, dificilmente ocorre esse crime, visto que é cômodo para os hackers possuírem uma maneira segura de receber pagamento por serviços realizados.

4.5.1. CASO WANNACRY

O wannacry foi um ataque, ocorrido no ano de 2017, que os infratores cobravam das vítimas pagamento em bitcoin para liberar o acesso delas aos seus próprios arquivos que estavam criptografados³⁰.

Esse vírus é um software malicioso que criptografa os arquivos de quem foi invadido e cobra para descriptografar. Pode ser transmitido através de worm, o que faz com que se multiplique entre os dispositivos automaticamente. Esse ataque resultou em um prejuízo de milhões, a quem acredite, em bilhões.

Os responsáveis pelo ataque cobravam U\$ 300,00 (trezentos dólares) em bitcoin para descriptografar os arquivos, caso não realizasse o pagamento no tempo indicado, o valor era dobrado. Ao todo esses hackers conseguiram 70 mil Bitcoins, mas esses BTC foram rastreados em razão de um **bot**, desenvolvido pela empresa Quarts Keith Collins, que em seu artigo informa que: “Para retirar esses valores, os criminosos utilizaram um “mixer bitcoin”, ou seja, um serviço de lavagem de bitcoins para tentar esconder rastros das transações.”

Esse ataque foi muito preocupante, pois atingia vários sistemas de saúde no mundo inteiro, incluindo várias organizações como:

“Empresas: FedEx, Honda, Hitachi, Telefônica, O2, Renault

Universidades: Universidade de Tecnologia Eletrônica de Guilin, Universidade de Tecnologia Aeroespacial de Guilin, Universidade Marítima de Dalian, Cambrian College, Universidade Aristóteles de Thessaloniki, Universidade de Montreal

Empresas de transporte: Deutsche Bahn, LATAM Airlines Group, Ferrovias russas

Agências governamentais: Polícia de Andhra Pradesh, Agência de segurança pública chinesa, Instituto Nacional de Salud (Colômbia), NHS - Serviço Nacional de Saúde

³⁰ LATTO, Nica. **O que é o WannaCry?** Avast. Acessado em 05 de julho de 2020. Disponível em:

<https://www.avast.com/pt-br/c-wannacry>

(Reino Unido), NHS da Escócia, Tribunal de Justiça de São Paulo, vários governos estaduais na Índia (Gujarat, Kerala, Maharashtra, Bengala Ocidental)”.(LATTO, 2020)

O ataque foi parado por um pesquisador chamado Marcus Hutchins, Nica Latto (2020) explica que:

“O pesquisador de segurança cibernética, Marcus Hutchins, descobriu que, depois que o WannaCry entrava em um sistema, ele tentava se conectar a um URL específico. Se o URL não fosse encontrado, o ransomware infectava o sistema e criptografava arquivos. Hutchins conseguiu registrar um nome de domínio para criar um DNS sinkhole que funcionava como um kill switch e desativou o WannaCry.”

4.5.2. CASO SILK ROAD

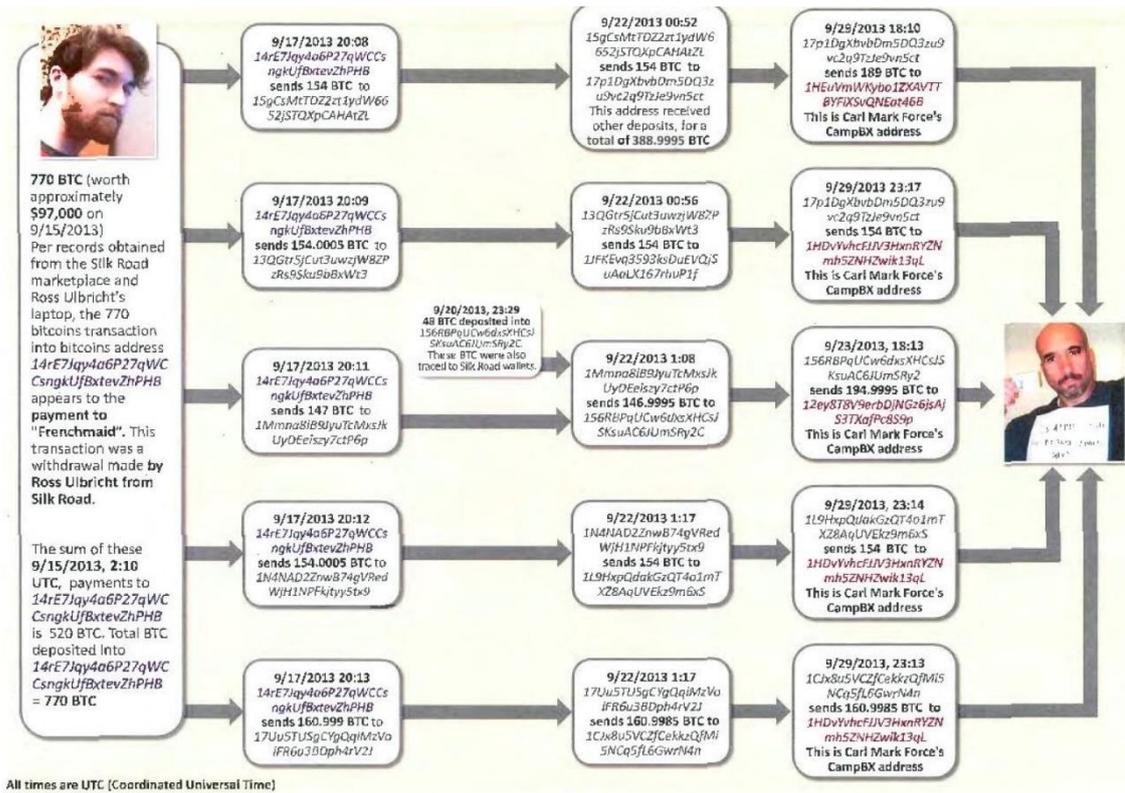
O caso Silk Road, trata-se de um mercado que funcionava na Darknet, que garantia aos compradores e vendedores de produtos ilegais, anonimato.

Esse site foi lançado no ano 2011 e oferecia aos compradores a criação de contas de maneira gratuita e, aos vendedores exigiam que comprassem contas em leilões. Os pagamentos ocorriam com o BTC. Em 2013 o FBI prendeu Ross Ulbricht, acusado de ser o criador e operador do site.

O que chama a atenção no caso Silk Road, é o envolvimento de Agentes Federais dos EUA, que estavam atuando na operação. Esses agentes utilizaram nomes fictícios para repassar informações ao acusado, que em contrapartida, realizava pagamento em bitcoins para os mesmos. A partir daí o Agente passou a cometer o crime de lavagem de dinheiro, transferindo a quantia para o Panamá e para uma empresa japonesa.

Entretanto, o agente cometeu uma série de erros que o levaram à prisão, como por exemplo, o fato dele ter enviado um e-mail para Silk Road, que constava seu próprio nome.

Na imagem abaixo é possível observar a enorme quantidade de pagamentos realizados pelo acusado aos Agentes Federais.



5. CONSIDERAÇÕES FINAIS

A princípio o presente trabalho buscou encontrar a origem, definição e funcionamento da Bitcoin, inclusive, a forma que ela é utilizada para o cometimento de crimes. Tal tarefa se mostrou ser complexa, pois exigiu muita cautela perante os autores que tratam desses temas. Também foi necessário afunilar com cuidado assunto por assunto.

O presente trabalho presou por explicar a origem dessa moeda através - principalmente - do White Paper de autoria de seu próprio criador, Satoshi Nakamoto, e mencionar de maneira rápida a crise financeira de 2008, importante acontecimento ocorrido no momento em que essa moeda surgiu, que foi um dos principais fatores para aceitação dessa criptomoeda.

31 Disponível em: <https://www.bitcoinforensics.it/2015/04/bitcoin-forensics-silk-road/> . acessado dia 10 de agosto de 2020

A partir da explicação supracitada, foi abordado então que a bitcoin é uma criptomoeda baseada na rede peer-to-peer (ponto-a-ponto), o que possibilita a transferência de dados sem a utilização de um intermediário, tornando-a descentralizada. Essa transferência fica armazenada na rede de blocos chamada blockchain, que funciona como um livro de razão publica, onde qualquer pessoa em qualquer lugar do mundo consegue ter acesso. Tal rede é teoricamente imutável e inviolável impedindo assim o gasto duplo.

Abordamos também, a questão de a Bitcoin ser usada para pagamento de contas, em razão da maioria ser paga em forma de boleto e de sua aceitação no comércio em geral. Por eufemismo de uns empresários com a nova forma de investir e por pura inovação quando se trata de grandes empresas, foi levantado o debate sobre a utilização da bitcoin para pagar impostos, utilizando empresas especialista em criptomoedas para intermediar o pagamento, fato que já aconteceu em cidades dos EUA e Canadá, que realizaram tal ato com o objetivo de oferecer mais opções para pagamento de impostos, gerando assim, mais facilidade. Também há casos em que foi utilizada como opção para a restituição de impostos.

Continuando nesse contexto do advento da bitcoin, foi ressaltado o grande número de caixas eletrônicos para transação de criptomoedas instaladas no mundo inteiro, destacando por meio de gráficos que grande parte se concentra nos EUA e que, embora tal iniciativa tenha sido boa, gerou facilidade para ocorrência dos crimes de lavagem de dinheiro e sonegação fiscal. Além disso, discorreremos sobre como e quando o Brasil receberá o primeiro caixa eletrônico desse tipo em um futuro breve.

Fora apresentado que as moedas digitais podem ser obtidas através de compra ou mineração, tornando-se lucrativo para industrias que fornecem material necessário para minerar e para os mineradores e que, após o processo, o usuário poderá realizar transações e armazenar o que for minerado nas Exchanges, que são plataformas que facilitam a venda e compra dessas moedas, funcionando de maneira similar ao mercado de ações, o que gera necessidade do usuário utilizar varias Exchanges afim de obter as melhores ofertas.

Posto que o blockchain torna essa forma de negociar segura, foi tratado o tema sobre possíveis ataques as criptomoedas, como o ataque dos 51%, selfish mining e o eclipse ataque, que visam explorar possíveis problemas nos blockchain. Mas como mencionado,

embora sejam passíveis de obter sucesso contra altcoins, são difíceis de ocorrerem contra a rede de bitcoin, observado que necessitaria de muito poder computacional, o que geraria um gasto muito grande.

Encerrado essa contextualização sobre a bitcoin, o segundo capítulo tratou a respeito das implicações jurídicas em torno dela.

Inicialmente foi estudado qual a sua possível natureza jurídica, e o que implicaria reconhecimento dessas naturezas. Demonstramos que poderia vir a ser considerada como um ativo desde que usada para basear dados em escriturações de títulos de créditos e que estejam presentes as informações necessárias.

Em segundo as criptomoedas poderiam ter a natureza jurídica de commodity. A corrente que defende essa ideia argumenta que por ela possuir valor econômico, tem o necessário para ser considerada como um bem.

Em sequência foi apresentada a possível natureza de mobiliário em razão de fornecer através do blockchain, a informação sobre a origem e o caminho que a moeda percorreu até o momento em que foi feita a pesquisa. Além disso, poderia ser considerada uma ação escritural, o que gera a possibilidade de ter natureza de valor mobiliário.

No mais, foi evidenciado que a falta de leis específicas e regulação adequada gerou como consequência a dúvida sobre de que maneira ela deveria ser tributada, embora a Receita Federal tenha resolvido – provisoriamente - o problema, através de uma instrução normativa. Entretanto, a falta de regulação faz com que as moedas digitais se autorregulem.

Após o estudo das implicações jurídicas a respeito da natureza mais adequada, abordamos os possíveis crimes no qual as moedas poderiam ser utilizadas.

A princípio foi tratado o crime de lavagem de dinheiro no qual houve utilização da bitcoin. Foi mencionado o entendimento da doutrina a respeito desse delito, as suas 3 fases caracterizadoras, e logo após, demonstramos que esse crime acontece com a utilização das moedas digitais, em razão da facilidade de realizar transferência na rede, principalmente por sua anonimidade, pois, como mencionado, não há nenhum registro bancário a respeito do que foi transferido. Como as Exchanges carecem de fiscalização, mesmo utilizando-as ainda é difícil identificar infrações.

Também apresentamos o estudo a respeito do crime de fraude com a Bitcoin, desde a sua definição contida no dicionário até a doutrinária. Analisamos gráficos apontando quais

as fraudes cibernéticas mais frequentes, destacando dentre os vários tipos de fraude, a Pirâmide Financeira que é um esquema que consiste na captação frequente de pessoas que prometem lucros exorbitantes de forma rápida, mas que ao passar do tempo se torna insustentável pela diminuição da captação de pessoas. Crime tão frequente que chamou a atenção da CVM pelo grande número de denúncias.

No mesmo capítulo foi trabalhado o crime de sonegação fiscal no geral e como ele pode envolver as moedas digitais. Apontamos nesse tópico a sua funcionalidade e como é calculado o imposto de renda quando há necessidade de declaração das criptomoedas, utilizando como base a instrução normativa da Receita Federal.

E para encerrar estudamos os crimes cibernéticos, principalmente o de invasão cibernética, que pode envolver ou não a bitcoin. Apresentando através de gráficos as formas mais frequentes em que ocorre esse crime e uma tabela contendo as tipificações a luz do Código Penal Brasileiro.

Sendo assim, é possível chegar à conclusão de apesar de haver quem use as criptomoedas para cometimento de crimes, a bitcoin foi uma tecnologia inovadora que tem um grande potencial para permanecer. Além disso, há uma extrema necessidade de regulá-la para que haja o devido tratamento jurídico e eventual responsabilização quando necessário.

6. GLOSSÁRIO

7. ANEXOS

7.1. ANEXO A- INSTRUÇÃO NORMATIVA RECEITA FEDERAL.

INSTRUÇÃO NORMATIVA Nº 1.899, DE 10 DE JULHO DE 2019

Altera a Instrução Normativa RFB nº 1.888, de 3 de maio de 2019, que institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB).

O SECRETÁRIO ESPECIAL DA RECEITA FEDERAL DO BRASIL, no uso da atribuição que lhe confere o inciso III do art. 327 do Regimento Interno da Secretaria Especial da Receita Federal do Brasil, aprovado pela Portaria MF nº 430, de 9 de outubro de 2017, e tendo em vista o disposto no art. 113 da Lei nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional e no art. 16 da Lei nº 9.779, de 19 de janeiro de 1999, resolve:

Art. 1º A Instrução Normativa RFB nº 1.888, de 3 de maio de 2019, passa a vigorar com seguintes alterações:

"Art. 3º O conjunto de informações enviado de forma eletrônica deverá ser assinado digitalmente mediante o uso de certificado digital válido, emitido por entidade credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), sempre que for exigido no portal e-CAC da RFB." (NR)

"Art. 7º

.....

§ 1º Em relação aos titulares da operação, devem constar das informações a que se refere este artigo:

I - o nome da pessoa física ou jurídica;

II - o endereço;

III - o domicílio fiscal;

IV - o número de inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ), conforme o caso, ou o Número de Identificação Fiscal (NIF) no exterior, quando houver, no caso de residentes ou domiciliados no exterior; e

V - as demais informações cadastrais.

§ 2º Caso os titulares das operações sejam residentes ou domiciliados no Brasil, a prestação da informação relativa ao número de inscrição no CPF ou no CNPJ, conforme o caso, é obrigatória a partir da data da entrega do primeiro conjunto de informações, prevista no § 1º do art. 8º.

§ 3º Caso os titulares das operações sejam residentes ou domiciliados no exterior, a prestação das informações relativas ao país do domicílio fiscal, endereço e NIF no exterior é obrigatória a partir da entrega de informações a ser efetuada em janeiro de 2020, referentes às operações realizadas em dezembro de 2019.

§ 4º A entrega das informações relativas ao endereço da wallet de remessa e de recebimento, se houver, é obrigatória apenas na hipótese de recebimento de intimação efetuada no curso de procedimento fiscal." (NR)

Art. 2º Ficam revogadas a alínea "h" do inciso I e a alínea "h" do inciso II do art. 7º da Instrução Normativa RFB nº 1.888, de 3 de maio de 2019.

Art. 3º Esta Instrução Normativa entra em vigor na data de sua publicação no Diário Oficial da União.

MARCOS CINTRA CAVALCANTI DE ALBUQUERQUE

7.2. ANEXO B- PROJETO DE LEI Nº 2.303/15

PROJETO DE LEI Nº 2.303 DE 2015

(Do Sr. Aureo)

Dispõe sobre a inclusão das moedas virtuais e programas de milhagem aéreas na definição de “arranjos de pagamento” sob a supervisão do Banco Central

O Congresso Nacional decreta:

Art. 1º Modifique-se o inciso I do art. 9º da Lei 12.865, de 09 de outubro de 2013:

“Art. 9º.....

I - disciplinar os arranjos de pagamento; incluindo aqueles baseados em moedas virtuais e programas de milhagens aéreas;”

Art. 2º Acrescente-se o seguinte § 4º ao art.11 da Lei 9.613, de 03 de março de 1998:

“Art. 11

§ 4º As operações mencionadas no inciso I incluem aquelas que envolvem moedas virtuais e programas de milhagens aéreas”

Art. 3º “Aplicam-se às operações conduzidas no mercado virtual de moedas, no que couber, as disposições da Lei nº 8.078, de 11 de setembro de 1990, e suas alterações.

Art. 4º Esta Lei entra em vigor na data de sua publicação.

JUSTIFICAÇÃO

As chamadas “moedas virtuais” ganham cada vez mais destaque nas operações financeiras atuais.

Apesar de não haver ainda uma regulamentação nem nacional e nem internacional sobre a matéria, há uma preocupação crescente com os efeitos das transações realizadas por meios destes instrumentos.

O assunto mereceu um relatório especial do Banco Central Europeu (BCE) em outubro de 2012³², que foi atualizado em fevereiro de 2015³³. Apesar de concluir pela desnecessidade da introdução imediata de uma regulação mais ativa sobre as moedas virtuais, tal relatório aponta um conjunto de riscos que devem ser devidamente monitorados. Colocaremos a seguir um quadro com cada uma das principais conclusões do relatório e um comentário.

Quadro I

Riscos Apontados pelo Relatório sobre Moedas Virtuais do BCE	Comentário
“Não impõe um risco sobre a estabilidade de preços, conquanto a criação de moeda permaneça em um nível baixo” (tradução livre) ³⁴ ;	Como bem ressaltado o efeito das moedas virtuais sobre a estabilidade de preços ainda não traz preocupações enquanto estes mecanismos não crescerem em relação à economia. Assumindo ser inevitável que eles realmente continuem crescendo junto ao incremento do uso da internet, cabe monitorar a partir de que ponto esta premissa deixará de ser verdadeira.
“tendem a ser inerentemente instáveis, mas não têm o condão de comprometer a estabilidade financeira do país dada a sua conexão limitada com a economia real, seu baixo volume	Mais uma vez o Relatório do BCE faz a devida ressalva de que a desnecessidade de regulação imediata depende da (ainda) baixa amplitude de adoção dessas moedas virtuais. Com o crescimento da internet impulsionando as moedas virtuais haverá

³² Virtual currency Schemes. European Central Bank. October, 2012
<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

³³ Virtual Currency Schemes – a further analysis. February, 2015.

<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>

³⁴ “do not pose a risk to price stability, provided that money creation continues to stay at a low level”

<p>negociado e a falta de aceitação tão ampla entre os usuários” (tradução livre)³⁵</p>	<p>um natural incremento de pontos de conexão com a economia real, podendo passar a ameaçar a estabilidade financeira. De qualquer forma, o Relatório indica que tais esquemas são inerentemente instáveis, com elevada volatilidade da sua relação de troca com a moeda local.</p>
<p>“não é regulado no presente momento e não é supervisionado ou fiscalizado de perto por qualquer autoridade pública ainda que a participação nesses esquemas exponha os usuários a riscos de crédito, liquidez, operacionais e legais” (tradução livre)⁵</p>	<p>Aqui a preocupação é menos sistêmica e mais de direito do consumidor. Os usuários desses mecanismos estão inadvertidamente expostos a riscos financeiros significativos e sem proteção legal alguma.</p>
<p>“podem representar um desafio às autoridades públicas, dada a incerteza legal por trás destes esquemas que podem ser utilizados por criminosos, fraudadores e pessoas que lavam dinheiro para realizar suas operações ilegais” (tradução livre) 36</p>	<p>As moedas virtuais facilitam atividades criminosas, especialmente lavagem de dinheiro.</p>

³⁵ “tend to be inherently unstable, but cannot jeopardise financial stability owing to their limited connection with the real economy, their low volume traded and a lack of wide user acceptance”. ⁵ “are currently not regulated and are not closely supervised or overseen by any public authority, even though participation in these schemes exposes users to credit, liquidity, operational and legal risks”;

³⁶ “could represent a challenge for public authorities, given the legal uncertainty surrounding these schemes, as they can be used by criminals, fraudsters and money launderers to perform their illegal activities”;

<p>“podem ter um efeito negativo sobre a reputação dos Bancos Centrais, assumindo que o uso de tais sistemas cresce consideravelmente e que no caso de um incidente atrair a cobertura da imprensa, o público pode perceber o incidente como sendo causado, em parte, pelo fato de o Banco Central não estar fazendo seu trabalho direito” (tradução livre)³⁷.</p>	<p>Um esquema que pode ser entendido como uma “pirâmide” que acaba desmoronando pode ser interpretado como uma “barbearagem” do Banco Central, minando a sua credibilidade.</p>
<p>“recaem sob a responsabilidade dos Bancos Centrais na medida que o seu funcionamento tem características compartilhadas com os sistemas de pagamento, o que implica a necessidade de exame de pelo menos alguns dos seus desenvolvimentos e a provisão de uma avaliação inicial” (tradução livre)⁸</p>	<p>Constitui um reconhecimento de que as moedas virtuais constituem sistemas de pagamento e como tal devem ser monitorados de perto.</p>

Sobressai-se nesta análise das moedas virtuais o que é

considerado o maior caso de “sucesso” que é o Bitcoin. Conforme o relatório do ECB de 2012:

“Desenhado e implementado pelo programador japonês Satoshi Nakamoto em 2009, o esquema é baseado em uma rede peer-to peer similar ao Bit Torrent, o famoso protocolo de compartilhamento de arquivos como filmes, jogos e música na internet. O Bitcoin opera globalmente e pode ser usado como moeda para todos os tipos de transação (para ambos bens, e serviços virtuais e reais), competindo portanto com as moedas oficiais como o euro e o dólar.... embora o

³⁷ “could have a negative impact on the reputation of central banks, assuming the use of such systems grows considerably and in the event that an incident attracts press coverage, since the

Bitcoin seja um esquema de moeda virtual, possui algumas inovações que a tornam mais similar à moeda convencional” (tradução livre)⁹.

O mais importante para nós, no entanto, são os riscos

potenciais apontados no relatório para o Bitcoin:

“De tempos em tempos, o Bitcoin é cercado por controvérsias. Algumas vezes ressalta-se o seu potencial para se tornar uma alternativa monetária ao tráfico de drogas e lavagem de dinheiro, como resultado do elevado grau de anonimato. Em outras ocasiões, os usuários têm

public may perceive the incident as being caused, in part, by a central bank not doing its job properly;”

⁸ “do indeed fall within central banks’ responsibility as a result of characteristics shared with payment systems, which give rise to the need for at least an examination of developments and the provision of an initial assessment.”

⁹ “Designed and implemented by the Japanese programmer Satoshi Nakamoto in 2009,¹ the scheme is based on a peer-to-peer network similar to BitTorrent, the famous protocol for sharing files, such as films, games and music, over the internet. It operates at a global level and can be used as a currency for all kinds of transactions (for both virtual and real goods and services), thereby competing with official currencies like the euro or US dollar.....Although Bitcoin is a virtual currency scheme, it has certain innovations that make its use more similar to conventional money”.

reclamado ter sofrido um roubo substancial de Bitcoins através de um “cavalo de troia” que ganhou acesso ao seu computador. A Fundação Fronteira Eletrônica, que é uma organização que busca defender a liberdade no mundo digital, decidiu não mais aceitar doações em Bitcoins. Entre as razões dadas, eles consideraram “que a Bitcoin gera preocupações legais ainda não testadas relacionadas às lei de ativos financeiros, com o “Stamp Payment Act” (legislação que proíbe qualquer pagamento abaixo em moeda, nota ou cheque abaixo de \$1), de evasão de tributos, de proteção do consumidor e lavagem de dinheiro, entre outros” (tradução livre)³⁸

O Relatório do BCE também possui um box específico (box 1) para os programas de milhagem. O efeito de tais programas, enquanto uma “moeda paralela”, não pode ser subestimado. O Relatório cita matéria do “The Economist” de 2005 que mostra que tais programas, já naquela época, atingiam valores significativos, inclusive

³⁸ “. From time to time, Bitcoin is surrounded by controversy. Sometimes it is linked to its potential for becoming a suitable monetary alternative for drug dealing and money laundering, as a result of the high degree of anonymity.⁹ On other occasions, users have claimed to have suffered a substantial theft of Bitcoins through a Trojan that gained access to their computer.¹⁰ The Electronic Frontier Foundation, which is an organisation that seeks to defend freedom in the digital world, decided not to accept donations in Bitcoins anymore. Among the reasons given, they considered that “Bitcoin raises untested legal concerns related to securities law, the Stamp Payment Act, tax evasion, consumer protection and money laundering, among others”

ultrapassando a quantidade de dólares em circulação. O Relatório inclui os programas de milhagem como um tipo específico de “moeda virtual”.

Em certa medida acreditamos que tanto o Banco Central como o Conselho de Controle de Atividades Financeiras (Coaf) e os órgãos do consumidor já tem competência para fiscalizar e regular moedas virtuais. No entanto, entendemos que as legislações que conferem tais atribuições podem ser mais transparentes em relação a tais atribuições, o que evita desnecessários questionamentos judiciais.

Sendo assim, endereçamos no projeto de lei proposto três questões relacionadas às moedas virtuais, uma em cada artigo: i) regulação prudencial pelo Banco Central, ii) lavagem de dinheiro e outras atividades ilegais e iii) defesa do consumidor. Deixamos claro no art. 1º que os “arranjos de pagamento” citados no inciso I do art. 9º da Lei 12.865, de 09 de outubro de 2013 inclui “*aqueles baseados em moedas virtuais e programas de milhagens aéreas*”. Ademais, deixamos claro no art. 2º que as operações que envolvem moedas virtuais estão incluídas na fiscalização do COAF: Por fim, não deixamos margem a dúvida de que a legislação de defesa do consumidor se aplica ao mundo das moedas virtuais no art. 3º.

Contamos com o apoio dos nobres pares para a aprovação desta importante medida para reduzir os riscos das moedas virtuais contra a estabilidade financeira da economia, diminuir a possibilidade delas financiarem atividades ilegais além de proteger o consumidor contra eventuais abusos.

Sala das Sessões, em de 2015.

Deputado AUREO

8. REFERENCIAS

ASUS. Mining-P106-6G. Asus. Acessado dia 2 de agosto de 2020. Disponível em: <https://www.asus.com/Graphics-Cards/MINING-P106-6G/> .

BADARÓ, Gustavo Henrique. BOTTINI, Pierpaolo Cruz. **Lavagem de dinheiro: aspectos penais e processuais penais: comentários à Lei 9.613/1998, com alterações da Lei 12.683/2012.** Volume 3. Ed. São Paulo. Thomson Reuters Brasil, 2019

BEAL, Vangie. **All About Peer-To-Peer (P2P) Networks.** Webopedia. Disponível em: https://www.webopedia.com/DidYouKnow/Internet/peer_to_peer.asp

BINANCE ACADEMY. Guia sobre Selfish Mining. Binance academy. Disponível em: <https://academy.binance.com/pt/blockchain/selfish-mining-explained>

BINANCE ACADEMY. O que é um Ataque de 51%? Binance Academy. Disponível em: <https://academy.binance.com/pt/security/what-is-a-51-percent-attack>

BITCOIN.NET. Double Spend. Bitcoin.net. Disponível em: <http://bitcoins.net/guides/double-spend.asp>.

BOMBANA, Lucas. **CVM intensifica fiscalização sobre pirâmides financeiras, em especial as que envolvem criptomoedas.** IstoÉ Dinheiro. Disponível em: <https://www.istoedinheiro.com.br/sempre-alerta/>

BRASIL. Constituição Federal. Brasília: Senado Federal, 1988

BRASIL. Lei nº 12.683. Brasília: Senado Federal, 2012

BRASIL. Lei nº 2.848. Brasília: Senado Federal, 1940.

BRASIL. Lei nº 6.385. Brasília: Senado Federal, 1976

BRASIL. Lei nº 9.613. Brasília: Senado Federal, 1998

BRASIL. Lei. Nº 4.729. Brasília: Senado Federal, 1965

BRASIL. Lei. Nº 8.137. Brasília: Senado Federal, 1990

CAIADO, Felipe B. CAIADO, Marcelo. **COMBATE À PORNOGRAFIA INFANTOJUVENIL COM APERFEIÇOAMENTOS NA IDENTIFICAÇÃO DE SUSPEITOS E NA DETECÇÃO DE ARQUIVOS DE INTERESSE** in Coletânea de artigos. Brasília, 2018, Volume 3. pp.8-24

CERT.BR. Estatísticas. Cert.Br. Disponível em: <https://www.cert.br/stats/incidentes/2019-jan-dec/fraude.html>

CHECO, Paolo. **Bitcoin forensics nell'indagine Silk Road.** Bitcoin forensics. Acessado dia 10 de agosto de 2020. Disponível em: <https://www.bitcoinforensics.it/2015/04/bitcoin-forensics-silk-road/>

COELHO, Fabio Ulhôa. **CURSO DE DIREITO COMERCIAL.** Volume 2. Ed. São Paulo: Revista dos Tribunais, 2018

COIN ATM RADAR. Estatísticas. Coin ATM Radar. Acessado em 20 de agosto de 2020. Disponível em: <https://coinatmradar.com/charts/growth/>

COINMAP. MAP. Coinmap. Acessado dia 24 de agosto de 2020. Disponível em: <https://coinmap.org/view/#/world/-26.01976579/-66.02508545/8>

EIZIRICK, Nelson et al. **Mercado de Capitais: regime jurídico.** 3. Ed. Rio de Janeiro: Renovar, 2011.

ÉPOCA NEGÓCIOS. Estado americano de Ohio começa a aceitar bitcoin para pagamento de impostos. ÉPOCA NEGÓCIOS. Disponível em: <https://epocanegocios.globo.com/Mundo/noticia/2018/11/estado-americano-de-ohio-comeca-aceitar-bitcoin-para-pagamento-de-impostos.html#:~:text=Estabelecimentos%20comerciais%20e%20empresas%20poderão,usando%20a%20moeda%20virtual%20bitcoin&text=O%20estado%20norte-americano%20de,com%20o%20Wall%20Street%20Journal>

EXAME, Pirâmides de Bitcoin: perda pode acabar com economias. Saiba evitar. Exame. Disponível em: <https://exame.com/seu-dinheiro/piramides-de-bitcoin-perda-pode-acabar-com-economias-saiba-evitar/>

FILHO, Marçal Justen. **Curso de Direito Administrativo.** São Paulo: Revista dos Tribunais, 2013

FRAUDE. In: DICIO, Dicionário Online de Português. Michaelis, 2020. Disponível em: <https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/fraude#:~:text=Dicionário%20Brasileiro%20da%20Língua%20Portuguesa&text=1%20Ato%20de%20má-fé,o%20pagamento%20dos%20tributos%20alfandegários>

GREGORIO, Rafael. **Como declarar bitcoins e outras criptomoedas no imposto de renda.** Valor Investe. Disponível em: <https://valorinveste.globo.com/mercados/cripto/noticia/2020/03/09/como-declarar-bitcoins-e-outras-criptomoedas-no-imposto-de-renda.ghtml>

HEILMAN, Ethan. KENDLER, Alison. ZOHAR, Aviv. GOLDBERG, Sharon. **Eclipse Attacks on Bitcoin's Peer-to-Peer Network**. USENIX Association. Washington, D.C., 2015. pp. 129-144

JENKINSON, Gareth. **Cidade no Canadá vai permitir pagamento de impostos com bitcoin- definindo o padrão para o futuro?** Cointelegraph. Disponível em: <https://cointelegraph.com.br/news/ohio-to-accept-tax-payments-in-crypto-setting-the-standard-for-future>

KAHTRI, Yogita. **Income tax payers in the U.S. now have the option to receive their federal and state refunds in bitcoin.** Coindesk. Disponível em: <https://www.coindesk.com/us-income-tax-payers-can-now-get-refunds-in-bitcoin>

LATTO, Nica. **O que é o WannaCry?** Avast. Disponível em: <https://www.avast.com/pt-br/c-wannacry>

MANZONI, Leandro. **8 estabelecimentos brasileiros que aceitam bitcoin.** FORBES. DISPONÍVEL EM: <https://forbes.com.br/negocios/2018/01/8-estabelecimentos-brasileiros-que-aceitam-bitcoin/#foto1>

MATSUYAMA, Keniche Guimarães. LIMA, João Ademar de Andrade. **CRIMES CIBERNÉTICOS: ATIPICIDADE DOS DELITOS**. III Congresso Brasileiro sobre Polícia Judiciária - 3º CBPJ. Campina Grande/PB., 2016. Pp 1-10.

MEIRELLES, José Ricardo. **O princípio da capacidade contributiva.** Brasília: Revista de informação legislativa, v. 34, n. 136, p. 333-339, 1997

Mirabete, Julio Fabbrini. FABBRINI, Renato N. **Manual do Direito Penal, volume 2: parte especial, arts. 121 a 234-V do CP.**- 2. Ed. rev., atual. e ampl. - São Paulo: Atlas, 2016.

NASCIMENTO, Daniela Pereira. **Agora, existem mais de oito mil caixas eletrônicos de bitcoin em todo o mundo.** Money Times. Disponível em: <https://www.moneytimes.com.br/agora-existem-mais-de-oito-mil-caixas-eletronicos-de-bitcoin-em-todo-o-mundo/>

NOGUEIRA, João Gabriel. **Pesquisa diz que 66% dos caixas eletrônicos de Bitcoin estão nos EUA.** Mundo Conectado. Disponível em: <https://mundoconectado.com.br/noticias/v/11979/pesquisa-diz-que-66-dos-caixas-eletronicos-de-bitcoin-estao-nos-eua>

O MPF de olho nas pirâmides financeiras: saiba como distinguir um investimento financeiro de um golpe. – Brasília: MPF/2ªCCR, 2016. Acessado em 02 de agosto de 2020. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/cartilhas/guia-pratico-piramides-financeiras>

PERGUNTAS E RESPOSTAS 2020. Receita Federal. Disponível em: http://receita.economia.gov.br/interface/cidadao/irpf/2020/perguntao/pr-irpf-2020-v-1-2-2020-04-13_publicacao.pdf

Portal eletrônico. NAKAMOTO, Satoshi. **Bitcoin: A peer-to-peer eletrônica cash system.** Disponível em: <https://bitcoin.org/bitcoin.pdf>

Portal eletrônico. **PORTAL DO BITCOIN.** Transações não confirmadas do Bitcoin batem recorde e chegam a 155mil. Portal do Bitcoin. Disponível em: <https://portaldobitcoin.uol.com.br/transacoes-nao-confirmadas-bitcoin-batem-recorde-e-chegam-155mil/>.

RIGGS, Wagner. **Cidade no Canadá vai permitir pagamento de impostos com bitcoin.** Portal do Bitcoin. Disponível em: <https://portaldobitcoin.uol.com.br/cidade-no-canada-vai-permitir-pagamento-de-impostos-com-bitcoin/#:~:text=Cidade%20no%20Canadá%20vai%20permitir%20pagamento%20de%20impostos%20com%20bitcoin,-por%20Wagner%20Riggs&text=O%20município%20de%20Innisfil%20será,bitcoin%20a%20partir%20de%20abril>

SEU DINHEIRO. Como declarar bitcoin e outras criptomoedas no imposto de renda. Seu Dinheiro. Disponível em: <https://www.seudinheiro.com/2020/imposto-de-renda/como-declarar-bitcoin-e-outras-criptomoedas-no-imposto-de-renda/>

SHIMABUKURO, Adriana. **AS INVESTIGAÇÕES NA ERA DAS MOEDAS DIGITAIS** in Coletânea de artigos. Brasília, 2018, Volume 3. pp.52-72.

Ulrich, Fernando, **Bitcoin- A moeda na era digital.** São Paulo: Instituto Ludwig Von Mises Brasil, 2014

ZOGBI, Paula. **Novas regras do Imposto de Renda: como declarar bitcoin e outras criptomoedas.** InfoMoney. Disponível em: <https://www.infomoney.com.br/minhas-financas/novas-regras-do-imposto-de-renda-como-declarar-bitcoin-e-outras-criptomoedas/>