UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

FACULDADE DE CIÊNCIAS JURÍDICAS E SOCIAIS

DEPARTAMENTO DE CIÊNCIAS PENAIS

Filipe Gustavo Silva de Barba

LIMITES DA IMPUTAÇÃO PENAL DECORRENTE DA POSSE ILÍCITA INCIDENTAL DE ARQUIVOS DIGITAIS, ORIUNDOS DO PROCESSO DE MINERAÇÃO DE CRIPTOMOEDAS (ESTUDO DE CASO).

Porto Alegre

2018

FILIPE GUSTAVO SILVA DE BARBA

LIMITES DA IMPUTAÇÃO PENAL DECORRENTE DA POSSE ILÍCITA INCIDENTAL DE ARQUIVOS DIGITAIS, ORIUNDOS DO PROCESSO DE MINERAÇÃO DE CRIPTOMOEDAS (ESTUDO DE CASO).

Trabalho de Conclusão de curso apresentado como requisito parcial para obtenção do título de Bacharel em Direito, junto à Faculdade de Direito da Universidade Federal do Rio Grande do Sul

Orientador: Dr. Ângelo Roberto Ilha da Silva

Porto Alegre

2018

FILIPE GUSTAVO SILVA DE BARBA

LIMITES DA IMPUTAÇÃO PENAL DECORRENTE DA POSSE ILÍCITA INCIDENTAL DE ARQUIVOS DIGITAIS, ORIUNDOS DO PROCESSO DE MINERAÇÃO DE CRIPTOMOEDAS (ESTUDO DE CASO).

Aprovado em 03 de julho de 2018

BANCA EXAMINADORA

_____

Professor Dr. Ângelo Roberto Ilha da Silva

_____

Professor Dr. Odone Sanguiné

_____

Professor Dr. Pablo Rodrigo Alflen da Silva

Porto Alegre

2018

“Se você está propondo uma ideia porque ela é sua, então você estará orgulhoso dela, e desejará que ela seja bem sucedida. Mas se está fazendo isso procurando excluir idéias contrárias, isso não é exatamente científico. Isso é religioso (dogmático). Esse é o tipo de pensamento ao qual me oponho onde quer que apareça.”

- Alan Moore

AGRADECIMENTOS

Inicialmente, agradeço imensamente ao meu orientador, Prof. Dr. Ângelo Roberto Ilha da Silva por todo o auxílio, aconselhamento, amizade, paciência e respeito que recebi não apenas durante o processo de elaboração da presente monografia, mas ao longo da vivência acadêmica como, por exemplo, ao receber o privilégio de participar por dois anos e meio de seu grupo de pesquisa na universidade. Essa foi uma das melhores experiências acadêmicas que tive durante a graduação. Enfim, palavras não são suficientes para demonstrar a minha gratidão, professor! Agradeço também aos familiares e amigos por todo o apoio que obtive para a conclusão não apenas desta monografia, mas durante todo o processo da graduação. Por fim, desejo agradecer a minha querida Tícia, cujas intervenções sobre o meu estado de espírito, durante o processo da confecção desta monografia, foram essenciais para me retirar do desamparo criativo e esgotamento mental/emocional que inevitavelmente me assolaram de tempos em tempos; seu apoio fez toda a diferença para o resultado que está consolidado ao longo deste trabalho.

RESUMO

O presente trabalho concerne a uma análise jurídica necessária sobre as recentes descobertas descritas no artigo científico "*A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin",* estudo desenvolvido pela Universidade Técnica da Renânia do Norte-Vestfália em Aachen, Alemanha (RWTH Aachen University). Segundo os estudiosos, após apurarem, quantitativamente e qualitativamente, a presença de dados aleatórios e não financeiros na cadeia de blocos do *blockchain* do Bitcoin, encontraram diversos arquivos digitais cujos conteúdos poderiam ser considerados censuráveis ou até ilícitos de acordo com a jurisdição de cada país. Dentre as descobertas, foram recuperados diversos arquivos digitais que variam de livros, vazamento de informações pessoais até conteúdo pornográfico infantil na estrutura do *blockchain* do Bitcoin. Dentre os diversos aspectos técnicos, o mais alarmante deles é o fato de que todo o usuário minerador deve possuir uma cópia local do *blockchain* da criptomoeda para exercer suas atividades de mineração. Isso implica dizer, de acordo com os autores do estudo supracitado, que se tal estrutura for manejada inadequadamente, isso pode acarretar em riscos para cada participante da rede que replicar localmente o *blockchain* do Bitcoin, bem como colocar em risco todo o sistema se houver a inserção de conteúdo de natureza censurável ou ilícita. Após realizado o levantamento de premissas fáticas, técnicas e jurídicas, concluiu-se que a posse incidental dos arquivos digitais resultantes das práticas de mineração de moedas na rede Bitcoin, cujo conteúdo ou posse pode representar hipóteses de tipicidade formal na legislação penal brasileira, é atípica diante da ausência do preenchimento do elemento subjetivo do tipo (dolo) necessários em todos os tipos penais passíveis de aplicação no caso examinado, sendo, portanto, conduta insuscetível de criminalização e de imposição de qualquer forma de sanção penal. Ainda, cumpre salientar que a legislação pátria quanto à regulamentação do uso e comercialização de criptomoedas é incipiente, bem como também é ineficaz para sustentar uma política criminal adequada para coibir a ocorrência de circunstâncias semelhantes as que foram apresentadas pelo estudo da RWTH Aachen University. Diante desse panorama, a possibilidade de punir os usuários da rede Bitcoin, em virtude das circunstâncias fáticas acima expostas, representaria uma afronta direta aos princípios norteadores do Direito Penal brasileiro, haja vista que é dever do poder estatal ponderar o alcance de suas intervenções coercitivas, bem como reduzindo-as ao mínimo necessário, buscando assim formas alternativas para a composição de conflitos sociais.

Palavras-chave: moedas digitais, criptomoedas, crimes cibernéticos, posse incidental ilícita, pornografia infantil, *blockchain,* Bitcoin, *altcoin,* Direito Penal informático, finalismo penal, teoria do crime, Hans Welzel.

ABSTRACT

The present work concerns a necessary legal analysis of the recent discoveries described in the scientific article "*A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin"*, a study developed by the Technical University of North Rhine-Westphalia in Aachen, Germany (RWTH Aachen University). According to scholars, after quantitatively and qualitatively assessing the presence of random and non-financial data in the Bitcoin *blockchain*, they found several digital files whose contents could be considered objectionable or even illegal according to the jurisdiction of each country. Among the findings, a number of digital files ranging from books, *doxing* occurences to child pornographic content in Bitcoin *blockchain* structure were recovered. Among the various technical aspects, the most alarming of them is the fact that every Bitcoin miner user must have a local copy of the cryptocurrency's *blockchain* to carry out their mining activities. This implies, according to the authors of the aforementioned study, that if such a structure is handled improperly, this may entail risks for each network participant that locally replicates the Bitcoin *blockchain*, as well as endangering the entire system if there is content of an objectionable or unlawful nature. After the collection of factual, technical and legal premises, it was concluded that the incidental possession of the digital files resulting from the mining activities of the Bitcoin network, whose content or possession may represent hypotheses of formal typicity in Brazilian criminal law, is atypical (non-criminalizable) in view of the absence of the filling of the subjective element of the type (deceit) required in all criminal types that may be applied in the case under examination; being, therefore, impassible conduct of criminalization and of application of any type of penal sanction. Also, it should be noted that the national legislation on the regulation of the use and marketing of cryptocurrencies is incipient as well as ineffective to support a proper criminal policy to prevent similar occurrences from those presented by the RWTH Aachen University's study. In view of this scenario, the possibility of punishing the users of the Bitcoin network, due to the aforementioned factual circumstances, would represent a direct affront to the guiding principles of Brazilian Criminal Law, since it is the duty of the state power to consider the scope of its coercive interventions, as well as reducing them to the minimum necessary, thus seeking alternative forms for the composition of social conflicts.

Keywords: cryptocurrency, cybercrime, illegal incidental possession, child pornography, *blockchain*, Bitcoin, *altcoin*, Cybercrime Law, finalism theory, crime theory, Hans Welzel.

LISTA DE SIGLAS

CP – Código Penal

ECA – Estatuto da Criança e do Adolescente

STF – Supremo Tribunal Federal

TJRS – Tribunal de Justiça do Estado do Rio Grande do Sul

TRF1 – Tribunal Regional Federal da 1ª Região

TRF2 – Tribunal Regional Federal da 2ª Região

TRF3 – Tribunal Regional Federal da 3ª Região

TRF4 – Tribunal Regional Federal da 4ª Região

TRF5 – Tribunal Regional Federal da 5ª Região

LISTA DE TABELAS

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

O tema do presente trabalho concerne a uma análise jurídica necessária sobre as recentes descobertas descritas no artigo científico "*A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin",* estudo desenvolvido pela Universidade Técnica da Renânia do Norte-Vestfália em Aachen, Alemanha (RWTH Aachen University). Segundo os estudiosos, após apurarem, quantitativamente e qualitativamente, a presença de dados aleatórios e não financeiros na cadeia de blocos do *blockchain*[1] do Bitcoin, encontraram diversos arquivos digitais cujos conteúdos poderiam ser considerados censuráveis ou até ilícitos de acordo com a jurisdição de cada país. Dentre as descobertas, foram recuperados diversos arquivos digitais que variam de livros, vazamento de informações pessoais até conteúdo pornográfico infantil na estrutura do *blockchain* do Bitcoin.

De plano, pode-se afirmar que problemática pode ser maior do que se apresenta. Deve-se tal afirmativa quanto aos aspectos históricos e funcionais das criptomoedas[2], especialmente o Bitcoin. No aspecto histórico, tanto o Bitcoin quanto outras criptomoedas são empregadas até hoje como sistema de pagamentos para a realização de transações financeiras com finalidades ilícitas, tendo como um dos exemplos mais emblemáticos o caso do site *Silk Road*. Logo, as criptomoedas possuem certo estigma social por serem reconhecidas também como uma ferramenta para atividades criminosas.

No aspecto funcional, seja no Bitcoin, seja em qualquer *altcoin*[3], o sistema de criptomoedas é mantido pelos usuários conhecidos como "mineradores". Tais usuários são responsáveis por verificar e validar as transações financeiras ocorridas entre os demais usuários da rede da criptomoeda, bem como manter a integridade e credibilidade das informações contidas no *blockchain*.

Tais processos são automatizados, uma vez que a verificação e validação de blocos que irão integrar a estrutura do *blockchain* é meramente criptográfica, sem

---

[1] *O Blockchain* desempenha a função como um "livro-razão" que registra todas as transações financeiras realizadas com a criptomoeda. Os conceitos sobre essa estrutura serão aprofundados ao longo do presente trabalho.

[2] Definição inaugurada por Wei Dai ao sugerir que um novo modelo de moeda digital teria sua emissão e trocas consolidada através do emprego de algoritmos criptográficos. Disponível em: <https://bitcoin.org/en/faq#general>. Último acesso em: 05/06/2018

[3] *Altcoin* é uma denominação genérica destinada a todas as criptomoedas alternativas ao Bitcoin (SWAN, 2015, x).

qualquer análise qualitativa destes blocos de informação. A atividade de mineração pode ser vantajosa, tendo em vista que o usuário que conseguir validar um novo bloco de informação para integrar a estrutura do *blockchain* é premiado com uma determinada quantidade de moedas digitais, assim como ele também receberá os valores relativos às comissões das transações financeiras validadas do respectivo bloco de informação.

O aspecto mais alarmante e que, por sua vez, guarda grande relevância a análise jurídica do presente trabalho é o fato de que todo o usuário minerador deve possuir uma cópia local do *blockchain* da criptomoeda para exercer suas atividades de mineração. Isso implica dizer, de acordo com as justificativas dos autores do estudo supracitado, que se tal estrutura for manejada inadequadamente, isso pode acarretar em riscos para cada participante da rede que replicar localmente o *blockchain* do Bitcoin, bem como colocar em risco todo o sistema se houver a inserção de conteúdo de natureza censurável ou ilícita. Essa é, portanto, a problemática que justifica a elaboração do presente trabalho.

Sendo assim, o objetivo da presente monografia está subdividido nos seguintes pontos: a) analisar o mérito e a factibilidade técnica do estudo elaborado pela RWTH Aachen University (*A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin*); b) apresentar uma visão técnica mais didática acerca do mecanismo de funcionamento das criptomoedas, voltada para leitores que não possuem tanta familiaridade com tais conceitos tecnológicos; c) contextualizar as implicações fáticas oriundas das descobertas do estudo da RWTH Aachen University com os institutos jurídicos existentes na doutrina, na legislação e jurisprudência pátria; e d) proceder com a análise jurídica e estabelecer os limites da imputação penal cabíveis aos usuários mineradores de Bitcoin que detenham a posse incidental de conteúdos potencialmente ilícitos na legislação penal brasileira, presumindo-se que tais usuários nunca acessaram diretamente o conteúdo do *blockchain* da respectiva criptomoeda.

Quanto à linha metodológica adotada, o trabalho foi dividido em três capítulos distintos. O primeiro capítulo apresentará o estudo que será objeto de análise desta monografia. Nesse capítulo será exposto o objeto, a justificativa, a metodologia do respectivo estudo científico, bem como suas conclusões e discussões conceituais. O segundo capítulo apresentará um aprofundamento da dimensão técnica abordada no primeiro capítulo acerca do mecanismo de funcionamento das criptomoedas. Cumpre

frisar que tal capítulo foi elaborado para facilitar a compreensão do conteúdo do primeiro capítulo. Portanto, recomenda-se aos leitores que não estiverem familiarizados com os conceitos da tecnologia supracitada que procedam inicialmente à leitura do segundo capítulo e, posteriormente, ao primeiro.

Por fim, o último capítulo descreverá conceitualmente os institutos jurídicos necessários para resolução do problema jurídico evidenciado com as descobertas do estudo da RWTH Aachen University, uma vez que há usuários mineradores de Bitcoin no país e que, portanto, de acordo com o referido estudo, tais usuários estariam em posse de conteúdos potencialmente ilícitos. Nesse capítulo, serão descritos os princípios mais relevantes do Direito Penal brasileiro, a dimensão doutrinária da teoria do crime que será aplicada no caso concreto acima descrito, a aplicabilidade dos tipos penais previstos na legislação penal, bem como a jurisprudência correlata ao caso. Na seção 4.2 do respectivo capítulo, proceder-se-á com análise jurídica propriamente dita do problema jurídico supracitado, realizando assim o silogismo entre as premissas maiores (jurídicas) e menores (fáticas e técnicas).

Face ao exposto, o presente trabalho busca apresentar uma solução adequada para a resolução do emergente problema jurídico acima exposto que poderá, eventualmente, prejudicar diversos usuários de criptomoedas brasileiros. Em que pese as circunstâncias negativas que permeiam a história das criptomoedas, dada a ausência de uma política criminal mais adequada, quanto ao combate de crimes cibernéticos, bem como a incipiente regulamentação do uso e comercialização de criptomoedas no país, prima-se apresentar no presente trabalho que criminalização dos usuários mineradores de criptomoedas, nas circunstâncias previamente expostas, pode representar um mal emprego do poder punitivo estatal.

2. UMA ANÁLISE QUANTITATIVA DO IMPACTO DOS DADOS ALEATÓRIOS CONTIDOS NO BLOCKCHAIN DO BITCOIN *(A QUANTITATIVE ANALYSIS OF THE IMPACT OF ARBITRARY BLOCKCHAIN CONTENT ON BITCOIN*[4]**): ESTUDO DESENVOLVIDO PELA UNIVERSIDADE TÉCNICA DA RENÂNIA DO NORTE-VESTFÁLIA EM AACHEN, ALEMANHA (RWTH AACHEN UNIVERSITY).**

O presente capítulo tem como propósito apresentar o estudo científico que embasará as premissas fáticas que serão analisadas sob o espectro jurídico no capítulo 4 deste trabalho de conclusão de curso. Sendo assim, nos tópicos seguintes será realizada a exposição do objeto, a justificativa científica para elaboração e suas respectivas conclusões e discussões do estudo científico que fundamentará o escopo fático que será analisado juridicamente no presente trabalho.

2.1 O OBJETO E A JUSTIFICATIVA CIENTÍFICA DA PESQUISA

Conforme asseverado pelos autores do estudo científico desenvolvido na Universidade Técnica da Renânia do Norte-Vestfália em Aachen, doravante RWTH Aachen University, o objeto da respectiva pesquisa teve como propósito analisar quantitativamente a presença de dados aleatórios e não financeiros[5] na cadeia de blocos do *blockchain* do Bitcoin, estrutura responsável por manter um registro público credível de todas as transações já realizadas com a referida criptomoeda (MATZUTT *et al.*, 2018, p.1).

Por sua vez, a justificativa científica para a realização do estudo da RWTH Aachen University se baseia na premissa de que a tecnologia do *blockchain* do Bitcoin pode gravar na sua estrutura, irrevogavelmente, dados aleatórios que variam desde mensagens curtas até fotos. A inserção de dados não financeiros não é uma prática incomum, visto que tal tipo de dado pode fomentar serviços notariais digitais, liberações seguras de compromissos criptográficos ou esquemas de não equívocos (MATZUTT *et al.*, 2018, p.2).

---

[4] Disponível em: < https://publications.rwth-aachen.de/record/721552>. Acesso em: 20/05/2018.

[5] Conforme exposto pelos autores do estudo científico em análise (MATZUTT *et al.*, 2018, p.3), convencionou-se como um dado digital não financeiro todo conteúdo com estrutura independente como, por exemplo, um arquivo ou texto legível ou qualquer outro tipo de dado digital inserido fragmentadamente por meio de um método de inserção de baixo nível.

Portanto, em tese, se tal estrutura for manejada inadequadamente, isso pode acarretar em riscos para cada participante da rede que replicar localmente o *blockchain* do Bitcoin, bem como colocar em risco todo o sistema se houver a inserção de conteúdo de natureza censurável ou ilícita. As premissas técnicas que justificam a elaboração do estudo da RWTH Aachen University serão analisadas com maior profundidade no terceiro capítulo do presente trabalho.

2.2 A METODOLOGIA DE PESQUISA APLICADA

No tocante às metodologias aplicadas no estudo da RWTH Aachen University, a referida pesquisa abordou os seguintes escopos: 1) exposição das possibilidades de métodos de inserção de dados arbitrários e serviços de inserção de conteúdos na cadeia do *blockchain*; 2) avaliação dos riscos e benefícios na inserção de dados não financeiros no *blockchain* e; 3) a análise sistêmica do conteúdo não financeiro encontrado no *blockchain* do Bitcoin e a discussão de suas respectivas repercussões. Ressalvado o disposto no item nº1, os demais pontos serão analisadas na seção a seguir do presente capítulo.

No que concerne ao item nº1, o estudo da RWTH Aachen University descreveu brevemente as características de funcionamento das transações financeiras do Bitcoin. Como descrito pelos autores do estudo supracitado (MATZUTT *et al.*, 2018, p.2), cada transação da criptomoeda possui vários scripts de entrada que desbloqueiam valores de transações anteriores e de vários outros scripts de saída que, por sua vez, especificam quem deverá receber tais valores. Para que haja o desbloqueamento de valores, os scripts de entrada necessitam que exista a assinatura criptográfica (chave privada) do proprietário dos valores. Igualmente, com a finalidade de evitar que scripts mal intencionados causem excesso de processamento na verificação das transações realizadas, o Bitcoin utiliza modelos padronizados de script de transação, sendo esperado como conduta em relação aos usuários da rede que descartem scripts não compatíveis ou impróprios.

FIGURA E TABELA 1 – Fluxograma de métodos de inserção de dados e serviços de inserção de conteúdo utilizados no Bitcoin e tabela descritiva da carga útil, custos e eficiência respectiva a cada método descrito na figura 1.

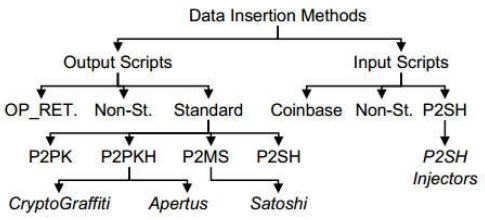


Fig. 1: Bitcoin data insertion methods (italics show content insertion services)

Method	Payload	Costs/B	Eff.
OP_RET.	80 B	3.18–173.55 ct	poor
Coinbase	96 B	—	poor
Non-St. Out.	99 044 B	1.03–198.05 ct	poor
Non-St. In.			med.
P2PK	85 345 B	1.24–207.79 ct	high
P2PKH	58 720 B	1.87–197.58 ct	high
P2MS	92 625 B	1.11–234.33 ct	high
P2SH Out.	62 400 B	1.77–195.54 ct	high
P2SH In.	99 018 B	1.03–225.61 ct	high

Table 1: Payload, costs, and efficiency of low-level data insertion methods

Fonte: A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin, 2018, p.3.

Como exposto na tabela 1, o estudo da RWTH Aachen University descreveu a metodologia de comparação entre os métodos de inserção de baixo nível, aptos para alocar dados não financeiros em transações financeiras do Bitcoin, de acordo com a eficiência, à carga útil inserível e aos custos por transação (MATZUTT *et al.*, 2018, p.3).

Nesse sentido, consignou-se a carga útil por transação (payload per transaction – PpT) de acordo com o número de bytes de conteúdo não financeiro que podem ser adicionados a uma única transação padronizada, com tamanho igual ou inferior à 100.000 bytes, ao passo de que os custos foram avaliados de acordo com a quantidade mínima e máxima por byte (costs per byte – CpB), relacionado assim o valor unitário para inserção de cada byte até o maior volume de dados que uma transação pode conter. Por fim, o critério da eficiência está embasado na capacidade de cada método de inserção em alocar grandes quantidades de dados arbitrários com facilidade e com custos relativamente baixos.

A seguir, de acordo com o exposto na figura 1, os pesquisadores elencaram quatro grupos de classificação de métodos de inserção de dados: a) OP_RETURN; b) Coinbase; c) Transações não padronizadas; e d) Transações financeiras padronizadas (MATZUTT *et al.*, 2018, p.4-5).

Em relação ao primeiro grupo, OP_RETURN trata-se de um modelo de transação especial que possibilita armazenar pequenos fragmentos de dados a uma transação financeira, sendo tal recurso uma forma de oferecer meio controlado para anotar transações sem quaisquer efeitos colaterais negativos. Todavia, tal método de inserção de dados possui uma limitação de 80 bytes por transação.

Por sua vez, o Coinbase consiste numa transação específica utilizada pelos mineradores de *bitcoins*[6] como forma de incentivo para que esses usuários ofereçam seu poder computacional para manter o *blockchain* do Bitcoin (MATZUTT *et al.*, 2018, p.3-4). Através dessa modalidade de transação, o minerador que vencer a competição do processo de mineração deve reivindicar o prêmio por ter construído o bloco mais recente que integrará a cadeia do *blockchain*. Nesse método de inserção de dados, como apontado pelos pesquisadores, apesar de existir a possibilidade da inserção de dados arbitrários no *blockchain*, tal método carece de eficiência, uma vez que somente mineradores ativos podem inserir pequenas frações de dados, além de possuir limitações semelhantes ao método OP_RETURN.

Acerca sobre as particularidades do terceiro grupo (MATZUTT *et al.*, 2018, p.4), embora seja desencorajado entre os usuários da rede Bitcoin, as transações financeiras podem ser consolidadas por scripts de entrada e scripts de saída modificados por qualquer usuário da rede Bitcoin[7] e, em tese, tais mecanismos poderiam ser utilizados para transportar blocos de dados arbitrários. Conforme exposto pelos autores do estudo, embora haja potenciais para transmissão de dados arbitrários com custos relativamente baixos, através da inobservância dos modelos padronizados de inserção de dados do Bitcoin, tal metodologia tende a ser ineficaz, haja vista que a elevada probabilidade de blocos de dados criados nesses moldes serem ignorados pelos demais mineradores da rede Bitcoin.

Embora pareça ser um fato improvável, as transações financeiras padronizadas têm o potencial de serem utilizadas inadequadamente como método de inserção de dados aleatórios não financeiros (MATZUTT *et al.*, 2018, p.4). Nesse sentido, os autores do estudo científico em análise citam a possibilidade de substituir chaves públicas e valores do *hash* do script por dados arbitrários, respectivamente, através dos métodos P2PK, P2MS para a primeira hipótese e PSPKH, P2SH na hipótese seguinte, visto que os demais usuários da rede Bitcoin não podem verificar sua exatidão antes que esses sejam referenciados por um script de entrada subsequente. Ademais, há o potencial da inserção eficiente de dados em scripts de entrada através do método de

[6] São usuários de rede Bitcoin que dedicam o poder computacional de suas máquinas para validar e verificar blocos de informações que integrarão o *blockchain* desta criptomoeda, bem como são responsáveis por manter a congruência do conteúdo desta estrutura (ANTONOPOULOS, 2014, p.174).

[7] O Bitcoin é um open source, portanto, qualquer usuário possui a liberdade de realizar modificações no algoritmo da criptomoeda. Disponível em: <https://bitcoin.org/en/faq#general>. Último acesso em: 05/06/2018.

inserção P2SH, tendo em vista que tais scripts são publicados com um script de resgate próprio. Por fim, os pesquisadores concluíram ainda que transações financeiras padronizadas sejam capazes de armazenar grandes quantidades de conteúdo, cujo fato também implica em custos significativos na transação.

De outra banda, conforme analisado no estudo da RWTH Aachen University, os serviços de inserção de conteúdo podem ser utilizados para alocar dados no *blockchain* do Bitcoin como documentos ou imagens (MATZUTT *et al.*, 2018, p.4-5). Quatro serviços foram identificados para fins de análise no referido estudo: a) CryptoGraffiti; b) Satoshi Uploader; c) Injetores P2SH; e d) Apertus. Cumpre frisar que todos os serviços de inserção dependem dos métodos de inserção de dados descritos na figura 1.

O primeiro serviço de inserção de conteúdo, CryptoGraffiti, trata-se de um serviço disponível na web que lê e grava mensagens e arquivos oriundos do *blockchain* do Bitcoin. Seu funcionamento ocorre através da utilização de múltiplos scripts de saída P2PKH dentro de uma única transação, sendo possível armazenar 60 KiB de conteúdo. Tal serviço pode recuperar conteúdos adicionados no *blockchain* se as transações que contiverem tais dados possuírem, pelo menos, 90% de caracteres imprimíveis ou se o respectivo conteúdo se trata de um arquivo de imagem.

Por sua vez, o Satoshi Uploader procede com inserção de conteúdo através de uma única transação com múltiplas saídas P2X[8]. Os dados inseridos por esse serviço são armazenados em conjunto para facilitar a decodificação e a verificação do conteúdo através da soma de verificação CRC32[9].

Por outro lado, há vários serviços[10] que oferecem a possibilidade inserção de conteúdo no *blockchain* do Bitcoin através de scripts de entrada P2SH que, por sua vez, são capazes de armazenar fragmentos de dados dentro de sua estrutura. Tais serviços são conhecidos como Injetores P2SH. Com a finalidade de garantir a integridade dos dados armazenados no *blockchain*, os scripts de resgate do P2SH contêm e verificam os valores de *hash* de cada parte inserida na respectiva estrutura de dados.

---

[8] Denominação adotada pelos autores do estudo para referenciar quaisquer métodos de inserção de dados que pertencem ao grupo de transações financeiras padronizadas, descrito na seção 2.1 do estudo em análise.

[9] 32 bit Cyclic Redundancy Check (verificação cíclica de redundância de 32 bits).
Disponível em:< https://www.w3schools.com/php/func_string_crc32.asp >. Acessado em 20/05/2018.

[10] Vide LE CALVEZ, Antoine, **Non-standard P2SH scripts**. Disponível em:< https://medium.com/@alcio/non-standard-p2sh-scripts-508fa6292df5>. Acessado em 20/05/2018.

Finalmente, o último serviço de inserção de dados, Apertus, é descrito como um recurso capaz de fragmentar conteúdo em diversas transações através da utilização arbitrária de scripts de saída P2PKH. Em seguida, tais fragmentos são referenciados em um arquivo armazenado no *blockchain* que, por sua vez, é utilizado na remontagem e recuperação dos fragmentos previamente inseridos, sendo possível, ainda, opcionalmente incrementar os dados já inseridos com comentários, renomear arquivos ou aplicar uma assinatura digital.

Estabelecida as diferenciações pertinentes entre método de inserção de dados e serviços de inserção de conteúdo, o estudo da RWTH Aachen University abordou sobre a metodologia de detecção aplicada para reconhecer dados não financeiros na cadeia de blocos do *blockchain* do Bitcoin (MATZUTT *et al.*, 2018, p.8).

Nessa esteira, algumas diretrizes básicas foram estabelecidas para evitar a maior incidência de falsos positivos, dentre as quais: a exclusão de qualquer saída de transação financeira padrão cujos valores já gastos no momento da análise do estudo e a desconsideração de qualquer arquivo recuperado do *blockchain* que seja ilegível. Como devidamente ponderado pelos autores do estudo científico em análise, embora a análise técnica empreendida tenha esgotado todas alternativas de inserção de dados aleatórios não financeiros no *blockchain*, ainda não poderia ser considerada possível a detecção efetiva e plena de todos os dados não financeiros presentes na cadeia do *blockchain*.

Em seguida, o estudo da RWTH Aachen University organizou as metodologias de detecção em três grupos: a) detectores de método de inserção de baixo nível; b) detectores de serviços e; c) detector de transações suspeitas (MATZUTT *et al.*, 2018, p.8-9).

Relativo aos critérios de detecção do primeiro grupo, estes foram designados para detectar quaisquer modalidades de transações financeiras manipuladas, assim como transações do tipo OP_RETURN, Coinbase e não padronizadas. Especificamente, o detector de texto utilizado pelos pesquisadores do estudo científico em análise procurou encontrar padrões de scripts de saída P2X com valores mutáveis e que estes, por sua vez, contenham quantidade de caracteres ASCII imprimíveis superiores ou iguais a 90% (noventa por cento). Sendo assim, se for preenchida a condição previamente referida, o detector retorna todos os scripts de saída com seus respectivos conteúdos textuais.

Finalmente, foram consideradas todas as transações realizadas nos moldes do método de inserção Coinbase, OP_RETURN, assim como os scripts de saída não padronizados.

No tocante às particularidades do segundo grupo, os detectores deste grupo são capazes de detectar e extrair arquivos com base nos protocolos de serviços previamente analisados (CryptoGraffiti, Satoshi Uploader, Injetores P2SH e Apertus). Tais detectores também permitem a identificação do método de inserção de dados utilizado nas transações e, consequentemente, verificar qual protocolo de serviço fora utilizado para alocar dados na cadeia do *blockchain*.

O detector de serviços CryptoGraffiti foi designado para combinar transações com um canal de saída que envia um "sinal" para um *hash* de chave pública controlado pelo provedor do respectivo serviço. Outrossim, todos os valores mutáveis de scripts de saída que custam menos de 10.000 satoshi[11] são concatenados e armazenados em um arquivo. Tal limite de valor de custeio foi utilizado para descartar eventuais scripts de saída não manipulados como, por exemplo, o provedor do respectivo serviço que está gastando seus ganhos.

Por outro lado, o detector do serviço Satoshi Uploader foi orientado para buscar quaisquer transações que tivessem valores mutáveis e cujo gasto de bitcoins fosse pequeno e uniforme. Caso os primeiros 8 (oito) bytes contiver uma combinação válida de tamanho e a soma de verificação CRC32 para a carga útil da transação, haverá a carga dos respectivos dados para um arquivo individual.

A seguir, o detector dos serviços de injetores P2SH foi direcionado para resgatar scripts que contiver mais de uma operação *hash*, uma vez que transações financeiras padronizadas utilizam no máximo uma operação. Em seguida, caso atendida a condição supracitada, procede-se então com a concatenação das segundas entradas de todos os scripts de resgate das transações para um arquivo individual.

Por sua vez, o detector do serviço Apertus examinará recursivamente o *blockchain* em busca de arquivos com extensões compatíveis com arquivos Apertus, ou seja, a existência de listas codificadas e identificadores de transações anteriores. Caso não haja uma carga útil do Apertus que não possa referenciar outro arquivo da mesma extensão, procedeu-se com a recuperação dos dados do respectivo arquivo, bem como,

[11] Unidade monetária do Bitcoin, equivalente a 10^{-8} *bitcoins* (ANTONOPOULOS, 2014, p.114).

se existente, o comentário opcional disponível aos arquivos do referido serviço de inserção de conteúdo.

Por último, o detector de transações suspeitas foi idealizado para apurar serviços de inserção menos difundidos, bem como para analisar transações padronizadas que possuem grande probabilidade de portar dados não financeiros. No escopo de análise desse detector, foram consideradas apenas transações que possuem pelo menos 50 saídas suspeitas ao passo de que tais transações deveriam ter a mesma quantia pequena (valor inferior a 10.000 satoshi) ou se valores desta transação não forem gastos.

Ante o exposto, encerrada a exposição acerca do escopo metodológico utilizado pelo estudo científico, objeto de estudo do presente trabalho de conclusão de curso, será apresentado na seção a seguir os resultados da metodologia acima exposta, bem como suas conclusões e possíveis discussões sobre os achados oriundos da pesquisa científica supracitada.

2.3 PONDERAÇÕES, CONCLUSÕES E DISCUSSÕES DO ESTUDO

Como aduzido na introdução da seção anterior, será abordado a seguir, respectivamente, a avaliação dos riscos e benefícios na inserção de dados não financeiros no *blockchain*, bem como a análise sistêmica do conteúdo não financeiro encontrado na respectiva estrutura do Bitcoin e a discussão de suas respectivas repercussões.

No tocante acerca do primeiro tema, como fora asseverado na seção 3.1 do estudo científico em análise, é imperioso ressaltar que a inserção de dados não financeiros pode ser uma prática benéfica para diversas finalidades como, por exemplo, a inserção de vouchers no *blockchain* como recurso para confirmar a existência de um documento digital em determinado instante no tempo – *timestamp* – (MATZUTT *et al.*, 2018, p. 5).

Através da utilização do método de inserção OP_RETURN, tal recurso é utilizado por diversos serviços de natureza notarial digital até o gerenciamento difuso de direitos digitais ou para gerar logs de não-equivocação. Além disso, relativo à utilização do método de inserção Coinbase como meio de alocar dados não financeiros no *blockchain*, tal método pode ser útil para os mineradores realizarem anúncios, enviar

mensagens curtas ou até adicionar bandeiras de voto identificáveis em transações cujos mineiros poderão votar adoção de recursos na rede do Bitcoin como, por exemplo, a adição do método de inserção P2SH (MATZUTT *et al.*, 2018, p.5-6).

Ademais, é pertinente ressaltar que a inserção de qualquer tipo de dado inserido na cadeia do *blockchain* terá a garantia de armazenamento não manipulável em longo prazo. Portanto, embora haja benefícios evidentes na garantia de segurança oferecida pelo *blockchain* do Bitcoin, uma vez que todo conteúdo inserido na referida estrutura será replicado compulsoriamente a todos os usuários que atuam na rede enquanto mantenedores da integridade do histórico de transações do Bitcoin.

Em contrapartida, apesar dos benefícios supracitados, a inserção de conteúdo censurável ou ilícito pode colocar em risco todos os usuários da rede Bitcoin, haja vista que, como previamente mencionado, qualquer conteúdo que ingressar na cadeia de blocos do *blockchain* se tornará imutável e será replicado localmente por cada usuário da rede que atua enquanto mantenedor dos registros de transações da criptomoeda. Nesse sentido, os pesquisadores do estudo em análise estabeleceram 5 (cinco) categorias de conteúdo de risco para usuários da rede Bitcoin (MATZUTT *et al.*, 2018, p. 6-8): a) Violações de Direitos Autorais; b) Malware; c) Violações de Privacidade; d) Conteúdo Politicamente Sensível; e e) Conteúdo Ilegal e Condenado.

Na primeira categoria, considerou-se como uma violação de direito autoral todo uso indevido de propriedade intelectual alheia como ocorre, por exemplo, uso de aplicações ou conteúdos digitais pirateados.

Por sua vez, como o título da segunda categoria sugere, entende-se como *malware* toda aplicação apta a causar danos patrimoniais tangíveis ou intangíveis como, por exemplo, a destruição de arquivos confidenciais, desmantelamento de dispositivos informáticos ou perdas financeiras propriamente ditas.

No que concerne à terceira categoria, consignou-se como uma violação de privacidade toda divulgação de dados sensíveis que possuem o potencial de causar a lesão ao patrimônio jurídico de determinada pessoa ou grupo de pessoas como, por exemplo, a prática de chantagem de vazar fotos ou vídeos íntimos em troca de benefício monetário.

A próxima categoria se trata sobre a divulgação de dados sensíveis pertencentes ao poder estatal, podendo ser a divulgação intencional ou a mera posse de tais conteúdos como crime, conforme o posicionamento da jurisdição de cada nação.

Finalmente, a última categoria engloba todas espécies de conteúdos que são amplamente condenadas e processadas em diversas jurisdições ao redor do mundo a citar, por exemplo, a pornografia infantil.

Como previamente exposto, há um espectro significativo de espécies de conteúdo censurável ou ilícito que pode causar danos diretos aos usuários, ainda que a posse de tal conteúdo tenha ocorrido inadvertidamente. Com efeito, conteúdos podem ser armazenados na cadeia do *blockchain* de forma anônima e irrevogável, ao passo de que tais conteúdos são constantemente validados e armazenados localmente pelos usuários que garantem a integridade e a credibilidade das informações constantes na referida estrutura do Bitcoin.

Ante o exposto, em tese, usuários de uma rede baseada na tecnologia *Blockchain* poderiam estar cometendo ilegalidades sem sequer ter ciência de tais circunstâncias, uma vez que os dados inseridos na estrutura do *blockchain* recebem apenas validação criptográfica pelos usuários mineradores, não sendo o conteúdo das transações inspecionado pelos respectivos usuários. Finalmente, as premissas acima expostas encontram síntese na seguinte afirmação realizada pelos autores do estudo da RWTH Aachen University (MATZUTT *et al.*, 2018, p.7-8), *in verbis:*

> Como afirmamos na Seção 2, é facilmente possível localizar e remontar tal conteúdo no blockchain. Portanto, embora a conversibilidade geralmente cubra a criação de uma representação visual, por exemplo, decodificando um arquivo de imagem, esperamos que o termo possa ser interpretado para incluir dados de blockchain no futuro[...].É crítico aqui que a lei alemã perceba que o disco rígido contém o blockchain como um documento[...] e que os usuários podem facilmente remontar qualquer conteúdo ilegal dentro do blockchain.(Tradução do autor)

De outra banda, no que concerne ao segundo tema a ser tratado nesta seção, serão expostos a seguir os resultados da análise sistêmica do conteúdo não financeiro encontrado no *blockchain* do Bitcoin, bem como a discussão de suas respectivas repercussões.

No sentido quantitativo da pesquisa, cumpre salientar que as medições realizadas no estudo da RWTH Aachen University são baseadas na versão completa do *blockchain*

do Bitcoin, datada de 31 de agosto de 2017, composta por 482.870 blocos e 250.845.217 transações, com dimensão total de 122,64 GiB (MATZUTT *et al.*, 2018, p.10). A partir de tal amostra, foram detectadas 3.535.855 transações com conteúdo não financeiro cuja carga útil total equivale a 118,53 MiB, representando assim cerca de 1,4% das transações no *blockchain* do Bitcoin.

Dentre os métodos utilizados para inserção de dados não financeiros no *blockchain* do Bitcoin, 95,90 MiB das detecções de transações com conteúdo não financeiro são oriundas de transações OP_RETURN (86,8%) e Coinbase (13,13%), sendo tal montante de transações equivalente a 80,91% dos dados não financeiros extraídos do *blockchain* do Bitcoin.

Nessa parcela da amostra colhida, 96,15% dos blocos possuem transações de custeio com conteúdo, sendo que 0,26% contêm quantidade igual ou superior a 90% de texto imprimível, 33,49% contêm quantidade igual ou superior de caracteres ASCII imprimíveis consecutivos. Outrossim, dentre as mensagens curtas encontradas nos respectivos blocos, 14,39% contêm bandeiras de votação de mineradores para implementação de novos recursos na rede do Bitcoin, bem como também há uma parcela de anúncios de mineradores ou mensagens curtas contendo versículos de oração (MATZUTT *et al.*, 2018, p.10).

Por sua vez, embora as transações do tipo P2X representam apenas 1,6% das detecções positivas do estudo da RWTH Aachen University, tal relação é inversamente proporcional ao conteúdo não financeiro identificado no *blockchain* do Bitcoin, constituído o montante de 9,08% (10,76 MiB) dos dados não financeiros identificados no estudo em análise (MATZUTT *et al.*, 2018, p.11).

Por fim, o grupo metodológico composto pelas transações não padronizadas e scripts P2SH não padronizados detectou 888 transações com conteúdo não financeiro, com carga útil total de 8,37 MiB. Dentre as detecções positivas, 7,07% dos dados financeiros encontrados são oriundos de transações realizadas através de injetores P2SH (MATZUTT *et al.*, 2018, p.11).

Em contrapartida, no que se refere às detecções de serviços de conteúdo, foram recuperadas 16,12 MiB de dados de natureza não financeira do *blockchain* do Bitcoin (MATZUTT *et al.*, 2018, p.11), sendo a metade deste valor composta por transações

realizadas através de injetores P2SH. O montante de dados restante é composto detecções positivas com os seguintes serviços de inserção de conteúdo: Apertus (21,70%), Satoshi Uploader (21,24%) e CriptoGraffiti (5,10%).

Finalmente, a tabela a seguir demonstra os resultados da pesquisa de acordo com a quantidade de dados não financeiros recuperados do *blockchain* do Bitcoin, bem como suas respectivas extensões e percentuais em relação à totalidade da amostra colhida:

TABELA 2 – Relação da quantidade, tipos de arquivos e percentuais de dados não financeiros encontrados no blockchain do Bitcoin.

File Type	Via Service? yes	no	Overall Portion	File Type	Via Service? yes	no	Overall Portion
Text	1353	54	87.07 %	Archive	4	0	0.25 %
Images	144	2	9.03 %	Audio	2	0	0.12 %
HTML	45	0	2.78 %	PDF	2	0	0.12 %
Source Code	7	3	0.62 %	**Total**	1557	59	100.0 %

Table 2: Distribution of blockchain file types according to our content-insertion-service and suspicious-transactions detectors.

Fonte: A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin, 2017, p.12.

Ante o exposto, como aduzido pelos autores do estudo da RWTH Aachen University (MATZUTT *et al.*, 2018, p.12), a maioria dos dados não financeiros recuperados do *blockchain* do Bitcoin são arquivos e imagens baseadas em texto (99,34%), ao passo que 1.616 arquivos revelaram possuir conteúdo significativo ao propósito do estudo científico supracitado.

Quanto à análise qualitativa dos arquivos de interesse encontrados no estudo da RWTH Aachen University, os pesquisadores abordaram a questão correlacionando o conteúdo de cada arquivo com as categorias de risco descritas na seção 3.2 do estudo em análise.

Relativo à primeira categoria, Violações de Direitos Autorais, foram encontrados 7 (sete) arquivos: software de codificação para quebra de proteção contra cópia de DVD's (*prime*) , o texto de um livro, uma cópia original do *paper "A Peer-to-Peer Electronic Cash System*" de Satoshi Nakamoto, dois artigos independentes, bem como duas chaves criptográficas vazadas, sendo uma chave privada RSA e uma chave secreta de firmware. Em contrapartida, nenhum arquivo encontrado na pesquisa se enquadrou na categoria de Malware (MATZUTT *et al.*, 2018, p.12-13).

Por sua vez, a terceira categoria, Violações de Privacidade, teve duas ocorrências de *doxing*[12]. Os dados vazados incluíam informações como números de telefones, endereços, contas bancárias, senhas e diversas identidades online. No tocante às ocorrências na quarta categoria, Conteúdo Politicamente Sensível, foram encontrados arquivos de backup do *WikiLeaks Cablegate*, bem como um artigo de notícias online sobre manifestações pró-democracia em Hong Kong (MATZUTT *et al.*, 2018, p.13).

Finalmente, a categoria "Conteúdo Ilegal e Condenável" obteve oito correspondências. Segundo os pesquisadores do estudo científico em análise (MATZUTT *et al.*, 2018, p.13), cinco desses arquivos ofertam conteúdo pornográfico moderado, sem especificar maiores critérios sobre o que seria considerado conceitualmente como "moderado". Dentre os três arquivos restantes, dois deles continham listas de links para sites que hospedavam pornografia infantil, contendo 274 links desse tipo de sites, sendo que 142 links são endereços tipicamente utilizados no navegador anônimo Tor (extensão *onion*). O arquivo restante se trata de uma imagem de "nudez branda" de um jovem. Novamente, os autores do estudo não especificaram o que seria "nudez branda" ou a idade aproximada de uma pessoa jovem. Outrossim, cumpre frisar que duas as imagens de conteúdo pornográfico explícito foram encontradas através do detector de transações suspeitas, portanto, tais conteúdos não foram inseridos através de serviços conhecidos.

Em suma, embora a tecnologia do *blockchain* possa ser bastante benéfica aos seus usuários, com suas possibilidades de utilização em serviços notariais digitais, gerenciamento de direitos ou sistemas de não equívocos; em contrapartida, a inserção de dados não financeiros têm o potencial de comprometer totalmente uma criptomoeda se tais dados representarem conteúdo censurável ou ilícito, implicando assim em ameaças imediatas aos usuários dessas ferramentas de troca. Como restou consolidado através das premissas e resultados apresentados ao longo do estudo da RWTH Aachen University, a inserção de conteúdos censuráveis ou ilícitos não só é tecnicamente possível, mas também se trata de prática consolidada na estrutura do *blockchain* do Bitcoin.

---

[12] De acordo com o dicionário Oxford, o verbo *dox* é o "ato de pesquisar e publicar informação privada ou associar tais tipos de informações a determinada pessoa na internet, com intenções tipicamente maliciosas" (tradução do autor). Disponível em: <https://en.oxforddictionaries.com/definition/dox>. Acesso em: 06/06/2018.

3. O BLOCKCHAIN E AS CRIPTOMOEDAS

O presente capítulo tem como propósito contextualizar da tecnologia das criptomoedas tanto no âmbito técnico quanto no âmbito socioeconômico. Inicialmente, será abordada a origem e evolução histórica das criptomoedas, bem como sua relevância socioeconômica na atualidade. Em seguida, será apresentado o sistema de funcionamento da tecnologia das criptomoedas. Por fim, haverá a síntese das premissas supracitadas e o cotejamento de suas implicações técnicas e fáticas.

3.1 BREVE PANORAMA HISTÓRICO

No ano de 1998, um dos integrantes do grupo autointitulado *Cypherpunks*, Wei Dai, manifestou-se perante o referido grupo sobre a existência da possibilidade tecnológica de criação de um novo modelo de sistema eletrônico de pagamentos integralmente online e completamente independente de intermediários financeiros imediatos, inclusive bancos. Nessa ocasião, houve a primeira abordagem conceitual do que se conhece atualmente como moeda digital ou criptomoeda[13] (KAPLANOV, 2012).

Wei Dai afirmara que tal sistema eletrônico de pagamento tinha o potencial de oferecer total anonimato aos seus usuários, através de pseudônimos não rastreáveis, ainda oferecer a publicidade plena de todas as transações ocorridas no respectivo sistema de pagamentos. Além disso, tal tecnologia funcionaria a partir de uma rede descentralizada, protegida por modelos específicos de criptografia de dados, cujos usuários seriam responsáveis e incentivados para cooperar entre si para manter a rede em funcionamento (KAPLANOV, 2012). Tal sistema de pagamentos foi chamado de "*b-money*"(GRINGBERG, 2011).

O conceito de sistema de pagamentos de Wei Dai adquiriu forma efetiva em 31 de outubro de 2008 através dos esforços intelectuais Satoshi Nakamoto[14]. Embora Wei Dai tenha preconizado a viabilidade tecnológica do conceito funcional de criptomoedas, foi Satoshi Nakamoto quem sintetizou o conceito de Wei Dai em uma aplicação prática.

[13] Definição inaugurada por Wei Dai ao sugerir que um novo modelo de moeda digital teria sua emissão e trocas consolidada através do emprego de algoritmos criptográficos. Disponível em: <https://bitcoin.org/en/faq#general>. Último acesso em: 05/06/2018.

[14] A real identidade de Satoshi Nakamoto permanece desconhecida até o presente momento. Muitos acreditam que esse nome seria apenas um pseudônimo de um indivíduo de gênero indefinido, embora haja quem acredita que tal nome também possa representar um grupo de pessoas (KAPLANOV, 2012, p.115).

Na data supracitada, em um fórum online cujas discussões técnicas eram voltadas à criptografia, Nakamoto criou a postagem intitulada "*Bitcoin P2P e-cash paper*". A referida postagem continha o artigo "*Bitcoin: A Peer-to-Peer Electronic Cash System*" cujo conteúdo descrevia o sistema de funcionamento necessário para a criação de um sistema de pagamento descentralizado, anônimo e independente de intermediários financeiros (SCHUERMANN, 2016).

O fórum online supracitado tinha diversos participantes como programadores independentes, matemáticos ligados à academia, profissionais de empresas de tecnologia da informação e organizações não governamentais. Diversos especialistas em programação e criptografia de diversos locais do mundo se uniram para implementar o conceito de sistema de pagamento de Nakamoto, dentre eles[15]: Hal Finney, Nick Szabo, Gavin Andresen, Martti Malmi, Jeef Garzik, Pieter Wuille, Matt Corallo, Mike Hearn, Gregory Maxwell e outros (CHOHAN, 2017).

Por outro lado, o sistema de pagamentos apresentado por Nakamoto revelou uma nova dimensão prática no conceito de liberdade monetária: a exclusão integral da necessidade de intermediários financeiros imediatos para assegurar o bom andamento de transações financeiras, papel tradicional exercido pelas instituições financeiras. Além disso, em contraste às concepções de Silvio Gesekk e Abul A'la Maududi que, por sua vez, também propuseram a criação de uma moeda livre de sistemas bancários como forma de fortalecer economias localmente, através de bancos comunitários e da adoção de um referencial monetário local para regiões pobres (BERGSTRA; LEEUW, 2013). Todavia, embora o Bitcoin tenha o potencial de resolver o problema supracitado, seu uso foi idealizado para transcender fronteiras nacionais.

Ademais, pode-se verificar que a resiliência e evolução do Bitcoin, enquanto um sistema *open source*[16] e operado com uma rede *peer-to-peer*[17], é devido ao sucesso a competitividade que este oferece a estruturas financeiras tradicionais, uma vez que o

[15] Disponível em: <https://en.bitcoin.it/wiki/Developers>. Último acesso em: 03/06/2018.
[16] Dentro dos limites da respectiva licença de uso, em linhas gerais, qualquer usuário possui a liberdade de realizar modificações no algoritmo da criptomoeda. Disponível em: <https://bitcoin.org/en/faq#general>. Último acesso em: 05/06/2018.
[17] Numa tradução livre, a rede *peer-to-peer é* "um tipo de rede de computadores onde cada estação possui capacidades e responsabilidades equivalentes. Isto difere da arquitetura cliente/servidor, no qual alguns computadores são dedicados a servirem dados a outros". Disponível em: <https://www.webopedia.com/DidYouKnow/Internet/peer_to_peer.asp>. Último acesso em: 05/06/2018

sistema de trocas do Bitcoin permite uma alternativa competitiva para realização de trocas, armazenamentos e mensuração de valores através do consenso descentralizado, tendo a validação da credibilidade de suas transações pelo uso da criptografia (BERGSTRA; LEEUW, 2013).

No ano de 2010, houve a primeira transação de *bitcoins* cujo objeto de troca se tratava de um bem tangível. Laszlo Hanycez, um programador que residia no estado da Flórida, realizou uma oferta de dez mil *bitcoins* para adquirir uma pizza. Embora tal transação tenha se consolidado de forma indireta, haja vista que o comerciante não aceitou a oferta, a respectiva oferta foi aceita por um indivíduo não identificado em Londres que, por sua vez, efetuou o pedido de duas pizzas em uma pizzaria localizada na Flórida chamada Papa Jones. Com a entrega das pizzas no endereço de Laszlo, a transferência ao credor anônimo foi realizada com sucesso (CHOHAN, 2017).

Em um futuro não muito distante do evento supracitado, a criptomoeda Bitcoin começou a ser negociada por uma corretora chamada Mt. Gox, sediada em Tóquio, Japão. O Bitcoin não apenas era negociado por essa corretora, mas também era realizada cotação desta criptomoedas em relação ao valor de moedas tradicionais. Com o sucesso resultante do nicho de mercado adotado pela Mt. Gox, outras corretoras seguiram o exemplo desta corretora e passaram a negociar *bitcoins*, bem como a realizar operações de câmbio com a respectiva criptomoeda. Assim, consignaram-se os primeiros movimentos especulativos perante as criptomoedas (KAPLANOV, 2012).

Posteriormente, com a proliferação progressiva de mercado de *bitcoins*, houve a intensificação do uso desta criptomoeda para as mais diversas finalidades. Nesse sentido, *bitcoins* foram utilizados para fomentar o site *Wikileaks* com doações, após o referido portal vazar informações sigilosas sobre o exército norte-americano em 2011, ao passo que *bitcoins* também foram empregados largamente na compra de artigos ou substâncias ilícitas em sites hospedados na *deep web* como, por exemplo, o mercado *Silk Road*, desmantelado em 2013 pelo FBI[18]. Consequentemente, na opinião pública,

[18]Disponível em: <https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts>. Acesso em: 03/06/2018.

criptomoedas foram associadas como ferramentas voltadas à prática de condutas criminosas (DION, 2013).

Apesar de tais percalços, bem como profundas variações no valor da cotação do Bitcoin durante o ano de 2011, em junho de 2012, houve a valorização e o aumento progressivo do valor de mercado da criptomoeda ao longo dos meses consecutivos, cujo fato culminou no início efetivo do uso das criptomoedas como forma de pagamentos de serviços por empresas na internet (DION, 2013).

Atualmente, há 1654 criptomoedas ou moedas digitais[19] disponíveis para ser transacionadas no mercado de valores, sendo há 154 empresas que oferecem ambientes para a comercialização de *bitcoins* e *altcoins*[20], espalhadas por 47 países ao longo do globo. O Brasil conta com 12 (doze) empresas corretoras de criptomoedas operantes no momento[21].

No último semestre de 2017, as criptomoedas começaram a receber uma atenção ainda maior pela comunidade internacional quando houve valorização vertiginosa do Bitcoin, a partir do segundo semestre de 2017. Em questão de seis meses, a unidade da referida criptomoeda valorizou-se mais de 900%, partindo do valor de $2.056,43 (01/06/2017) até o valor de $19.470,20 (18/12/2017)[22]. Infelizmente, nos meses consecutivos a essas cotações, sobreveio a concretização de um dos riscos inerentes ao uso de criptomoedas: a flutuação acentuada e sinuosa do valor das criptomoedas no mercado de valores. Todavia, o interesse pelo uso e investimento nas criptomoedas pela comunidade econômica mundial não regrediu com tais acontecimentos, mantendo-se cada vez mais relevante socialmente o fenômeno das moedas digitais (CHOHAN, 2017).

Ante o exposto, apesar de todos altos e baixos que as criptomoedas sofreram durante sua história, tal tecnologia disruptiva possui inquestionável importância social e econômica, representando uma nova forma em potencial que modificará definitivamente

---

[19] Disponível em: <https://coinmarketcap.com/all/views/all/>. Acesso em:07/06/2018.
[20] *Altcoins* é uma denominação genérica destinada a todas as criptomoedas alternativas ao Bitcoin (SWAN, 2015, x).
[21] Disponível em <https://exchangewar.info/>. Acesso em: 07/06/2018.
[22] Disponível em < https://coinmarketcap.com/currencies/bitcoin/>. Acesso em: 07/06/2018.

a concepção tradicional de trocas econômicas como, por exemplo, o desuso da figura de um intermediário obrigatório ou necessário para consolidação de qualquer transação financeira.

3.2 ESTRUTURA DE FUNCIONAMENTO DAS CRIPTOMOEDAS

Em linhas gerais, pode-se aferir que qualquer criptomoeda se sustenta funcionalmente através das seguintes estruturas: a) um sistema público de registro, com funcionalidade semelhante a um livro-razão contábil, que registra todas as transações realizadas entre os usuários da rede; b) uso de criptografia para garantir a segurança, bem como a validação das transações financeiras entre os usuários, assim como para garantir o anonimato dos mesmos; c) a descentralização do sistema de consenso, validação e verificação das transações financeiras realizadas entre os usuários da rede, de forma que a credibilidade das transações ocorridas na rede são garantidas por outros usuários da rede que não participam como intermediários diretos nas referidas transações (SWAN, 2015, ix-xi).

3.2.1 Panorama Geral de Funcionamento

Inicialmente, é imperioso salientar que toda a criptomoeda existente na atualidade é baseada no mecanismo de funcionamento inaugurado por Satoshi Nakamoto. Ao longo deste capítulo, o Bitcoin será utilizado em diversos momentos como exemplo para descrever o funcionamento de criptomoedas, todavia, tal particularização não é prejudicial para a fundamentação do presente capítulo, uma vez que, conforme mencionado, tal moeda inaugurou o conceito tecnológico. Em suma, em que pese a existência de particularidades inerente a cada *altcoin* existente, tais peculiaridades são inexpressivas em relação ao conceito tecnológico inaugurado e implementado no Bitcoin.

Dito isso, em geral, no que concerne à interação do usuário que deseja utilizar criptomoedas, há dois recursos distintos: a utilização de um aplicativo do tipo *client*, instalado na máquina local, ou através de serviços online oferecidos por corretoras de criptomoedas. As operações podem ocorrer em qualquer dispositivo informático (laptops, tablets, celulares, etc.) desde que os protocolos de funcionamento tenham sido

adaptados para respectiva arquitetura computacional. Nesse sentido, o Bitcoin oferece a aplicação *bitcoin client*, uma forma mais ampla e tradicional para a realização de todas as atividades do usuário da rede da respectiva criptomoeda. Outrossim, quanto ao Bitcoin, há corretoras que oferecem serviço na web para realização de operações financeiras sem a necessidade de utilização do *bitcoin client*. Portanto, há diversas formas de gerir recursos consubstanciados em criptomoedas (GRINGBERG, 2012).

Além disso, em qualquer das hipóteses supracitadas, todo indivíduo que utilizar criptomoedas terá para si uma carteira (*wallet*). Tal recurso é essencial para que o usuário não só possa realizar transferências de criptomoeda para outros usuários da rede assim como também possui grande utilidade como método de comunicação dentro da rede de um criptomoeda. Ademais, a carteira da criptomoeda armazena as chaves criptográficas do usuário da rede, indispensáveis para realização de transações no respectivo sistema de pagamentos. Logo, evidencia-se que a carteira (*wallet*) se trata de um recurso essencial e indispensável ao usuário de criptomoedas (GRINGBERG, 2012).

Cumpre frisar que, em regra, conforme consolidado no sistema Bitcoin, um usuário pode ter inúmeras carteiras, sendo apenas necessária a designação de um único endereço eletrônico por carteira. Toda a carteira é criada por uma aplicação *client* que, por sua vez, pode ser instanciada localmente ou remotamente (web). Em virtude disso, os usuários da rede são referenciados pelos seus pseudônimos, não existindo, portanto, qualquer vinculação direta com um determinado pseudônimo e uma carteira (DION, 2013).

De outra banda, todas as transações financeiras realizadas na rede de uma criptomoeda, após devidamente validadas e verificadas pelos demais usuários responsáveis pela integridade e credibilidade da respectiva rede, são inseridas em uma estrutura denominada *Blockchain*. Tal estrutura mantém um registro público do histórico de todas as transações ocorridas entre os usuários da criptomoeda. Os usuários mantenedores dessa estrutura são chamados de “mineradores”, todos eles se conectam a rede da criptomoeda por uma aplicação local do tipo *client* (KAPLANOV, 2012).

Quanto à regulação da velocidade de emissão de criptomoedas, em regra, trata-se de um processo automatizado pelo próprio algoritmo que é executado em todos integrantes da rede da respectiva criptomoeda. Nesse sentido, a tecnologia inaugurada pelo Bitcoin criou um sistema de pagamentos neutro, livre e disponível a qualquer usuário, uma vez que as transações ocorridas no respectivo não estariam sujeitas ao crivo de autoridades estatais ou financeiras (SWAN, 2015).

O procedimento para emissão de novas moedas dentro de um sistema de criptomoeda é realizado pelos próprios usuários mineradores. Especificamente, a emissão de novas moedas ocorre quando um novo bloco de informações é inserido na extremidade da cadeia do *blockchain*. As novas moedas são concedidas como um prêmio resultante de um processo de competição entre outros usuários mineradores da rede, resultante de um processo chamado "*proof-of-work*", cujo funcionamento será explicado oportunamente ao longo deste capítulo. Portanto, o sistema de uma criptomoeda só gera mais moedas se houver transações suficientes e usuários para verificar e validar as mesmas (SWAN, 2015).

De acordo com o algoritmo do Bitcoin, há um limite máximo de unidades de bitcoins a serem gerados pelos usuários, um recurso adotado para emular a escassez necessária da criptomoeda. Tal valor limite equivale a 21 milhões de bitcoins. Estima-se que os últimos bitcoins serão minerados no ano de 2.140 ou quando o bloco 13.230.000 for minerado, o fato que vier a ocorrer primeiro (ANTONOPOULOS, 2014). Hoje já existem pouco mais de 17 milhões de bitcoins em circulação[23].

Por meio do processo de mineração nos sistemas de criptomoedas, a criação de um novo bloco na cadeia do *blockchain* deverá ocorrer a cada 10 minutos. O usuário que vencer a competição para validar tal bloco de informação receberá 12,5 *bitcoins*. Cabe salientar que tal prêmio poderá ser obtido por grupos de usuários que se agrupam em *mining pools* para realizar a atividade de mineração no sistema de uma criptomoeda. O termo "mineração" é uma alegoria acerca da escassez programada na emissão de criptomoedas, tanto no que se refere à finitude do próprio recurso quanto à dificuldade

[23] Disponível em < https://blockchain.info/pt/charts/total-bitcoins>. Acesso em: 09/06/2018.

progressiva no processo de obtenção deste recurso com crescimento da competição pela obtenção do mesmo (ANTONOPOULOS, 2014).

Quanto ao nível de dificuldade de mineração, o algoritmo do sistema Bitcoin resolveu o problema localmente. Nesse aspecto, cada usuário minerador calibrará a dificuldade dos problemas gerados pela função *hash*, elemento integrante do processo de validação "*proof-of-work*", pelo número dos usuários da rede tentando resolvê-los. Portanto, quanto maior o número de mineradores, maior será a dificuldade da prova criptográfica necessária para validação dos novos blocos a serem integrados ao *blockchain*, ao passo de que o mesmo algoritmo facilitará ou dificultará o processo de "*proof-of-work*" de forma que cada novo bloco de informações seja criado a cada 10 minutos (ANTONOPOULOS, 2014).

Por fim, assevera-se que o sistema de criptomoedas, introduzido pelo Bitcoin, preconizou um sistema de pagamento que garanta os seguintes aspectos: a) segurança de transações e dos usuários em uma rede descentralizada; b) transações financeiras eficientes e credíveis; e c) eliminação integral da necessidade de intermediários para o devido andamento das transações financeiras (SCHEUERMANN; TSCHORSCH, 2016). Nos tópicos a seguir, serão tratarão com maior profundidade os aspectos técnicos sobre estrutura de funcionamento de criptomoedas.

3.2.2 *Blockchain*, o "livro-razão" das criptomoedas

Como previamente asseverado, um dos pilares da credibilidade de uma criptomoeda está embasado na estrutura do *Blockchain*, uma vez que tal estrutura não só apenas mantêm a publicidade de todas as transações realizadas entre os usuários[24], mas também fornece a segurança e a inviolabilidade do conteúdo das mesmas. Outrossim, tal estrutura é incrementada a cada 10 minutos pelos usuários mineradores da rede que, por sua vez, verificam e validam as transações realizadas pelos demais usuários da rede. Através do processo de mineração, a estrutura de blocos do *blockchain* será incrementada constantemente (SWAN, 2015).

[24] As operações financeiras podem ser visualizadas no seguinte endereço: <https://blockchain.info/pt/blocks>. Acesso em: 09/06/2018.

Imperioso destacar a imutabilidade do conteúdo inserido na estrutura do *blockchain* só é possível graças o uso de criptografia, especificamente, pelo emprego da função *hash*. Nesse sentido, o algoritmo estipula que todo bloco-filho deve referenciar ao respectivo bloco-pai e assim sucessivamente[25]. Todo bloco de informações que integra a estrutura do *blockchain* possui uma espécie de assinatura criptográfica única, gerada a partir da função criptográfica *hash* que, por sua vez, atribui uma sequência de caracteres alfanuméricos única a cada bloco integrante do *blockchain* (ANTONOPOULOS, 2014).

Em razão disso, qualquer modificação no conteúdo de qualquer bloco que integra o *blockchain* modificará o *hash* do respectivo bloco e, consequentemente, gerará uma invalidação em cadeia de todos os blocos consecutivos ao bloco modificado. Isso é uma medida importante para implementar o consenso descentralizado, uma vez que os próprios usuários são responsáveis pela integridade do próprio sistema da criptomoeda. Logo, verifica-se que o uso da função criptográfica *hash* é essencial para detectar quaisquer violações nas informações do *blockchain*.

Somado ao uso de criptografia como uma ferramenta de verificação de inviolabilidade de dados constantes na estrutura do *blockchain*, o algoritmo do Bitcoin também se utiliza um sistema de redundância no consenso acerca do conteúdo constante na referida estrutura. Nesse sentido, em regra, todos os usuários que exercem a função de mineradores possuem uma cópia local do *blockchain* do Bitcoin.

Por sua vez, tais usuários estão em constante espelhamento de sua versão do *blockchain* em relação à versão dos outros usuários da rede, seja para verificar a congruência das informações constantes no *blockchain* dos demais usuários, seja para sincronizar a atualização de um novo bloco de informação validado por outro usuário da rede (ANTONOPOULOS, 2014). Em geral, as dimensões de um bloco de informação inserido no *blockchain* possuem a dimensão aproximada de 1 Mb[26].

---

[25] Recomenda-se a consulta do anexo B deste trabalho para uma melhor compreensão da estrutura em comento.

[26] Gráfico da média da dimensão computacional dos blocos de informação inseridos no *blockchain* do Bitcoin. Disponível em: <https://blockchain.info/pt/charts/avg-block-size>. Acesso em: 18/06/2018.

Portanto, o *Blockchain* é um recurso essencial e indispensável para consolidar a congruência, a credibilidade e publicidade das transações financeiras realizadas em uma rede descentralizada, anônima e destituída da necessidade de possuir qualquer autoridade ou intermediário financeiro para regular ou garantir a credibilidade de tais transações.

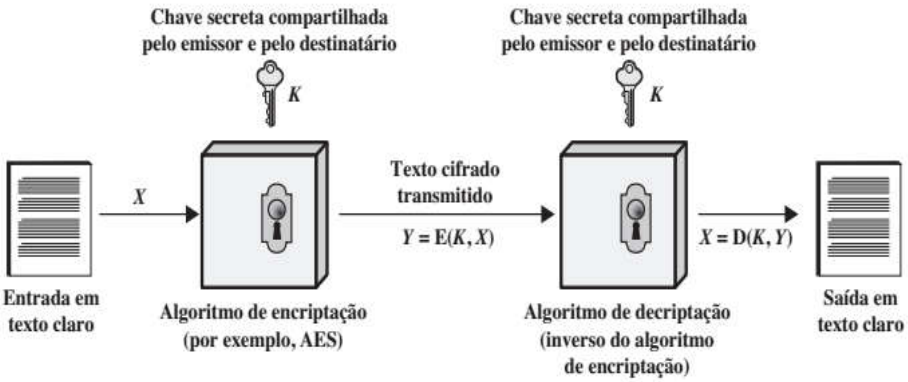
3.2.3 A Importância do Emprego da Criptografia nas Criptomoedas

Como previamente evidenciado, a criptografia constitui como um pilar essencial para a viabilização do sistema de criptomoedas que conhecemos atualmente. Com efeito, quando o sistema Bitcoin inaugurou o conceito de moeda digital, este se valeu dos conceitos de criptografia assimétrica como método de fornecer segurança nas transações financeiras e anonimato aos usuários da rede desta criptomoeda.

Conceitualmente, em termos computacionais, criptografia trata-se de uma técnica utilizada para garantir a confidencialidade e integridade das informações transmitida de um emissor a um ou mais interlocutores. Isso implica dizer que o ato de criptografar determinada informação consiste na sua cifragem para que apenas aqueles que detenham a chave para a reestruturação da respectiva informação possam fazê-lo (STALLINGS, 2015).

Nesse sentido, pode-se se classificar as modalidades de criptografia em dois grupos: simétrica e assimétrica. No primeiro grupo, a chave que codifica a informação é a mesma que a decodifica. Consequentemente, isso resulta no fato que tanto o emissor quanto o destinatário da informação devem compartilhar a mesma chave criptográfica. Caso contrário, o destinatário jamais saberá o real conteúdo da informação recebida (STALLINGS, 2015).

FIGURA 2 – Modelo simplificado de encriptação simétrica.



Fonte: Criptografia e Segurança de Redes: princípios e práticas, 2015, p.21.

Em que pese à existência de ameaças à segurança da informação, com métodos de tentativa e erro (*brute force*), tal esforço por si só não é capaz de colocar em vulnerabilidade a informação protegida por criptografia. A tabela a seguir demonstra o tempo necessário para quebra de uma chave criptográfica simétrica realizada por um PC[27] e um supercomputador, quarta e quinta coluna respectivamente (STALLINGS, 2015).

TABELA 3 – Tempo médio exigido para quebra de criptografia por tentativa e erro (*brute force*).

Tamanho de chave (bits)	Cifra	Número de chaves alternativas	Tempo exigido a 10^9 decriptações/s	Tempo exigido a 10^{13} decriptações/s
56	DES	$2^{56} \approx 7{,}2 \times 10^{16}$	2^{55} ns = 1,125 ano	1 hora
128	AES	$2^{128} \approx 3{,}4 \times 10^{38}$	2^{127} ns = $5{,}3 \times 10^{21}$ anos	$5{,}3 \times 10^{17}$ anos
168	Triple DES	$2^{168} \approx 3{,}7 \times 10^{50}$	2^{167} ns = $5{,}8 \times 10^{33}$ anos	$5{,}8 \times 10^{29}$ anos
192	AES	$2^{192} \approx 6{,}3 \times 10^{57}$	2^{191} ns = $9{,}8 \times 10^{40}$ anos	$9{,}8 \times 10^{36}$ anos
256	AES	$2^{256} \approx 1{,}2 \times 10^{77}$	2^{255} ns = $1{,}8 \times 10^{60}$ anos	$1{,}8 \times 10^{56}$ ano
26 caracteres (permutação)	Monoalfabético	$2! = 4 \times 10^{26}$	2×10^{26} ns = $6{,}3 \times 10^{9}$ anos	$6{,}3 \times 10^{6}$ anos

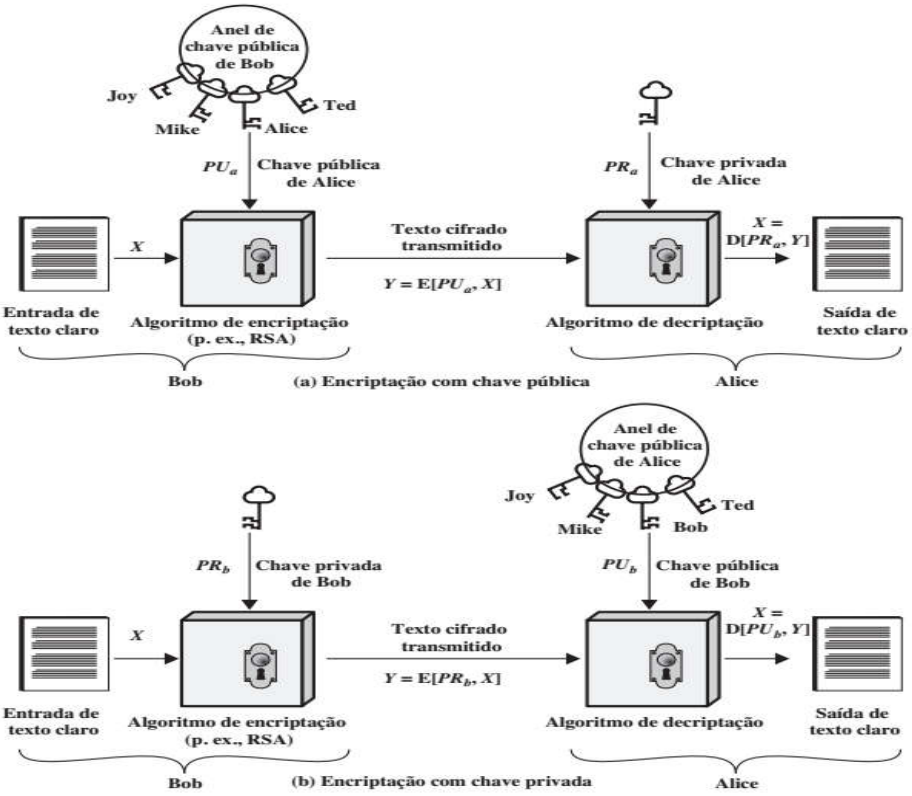
Fonte: Criptografia e Segurança de Redes: princípios e práticas, 2015, p.58.

Em contrapartida, no segundo grupo, diversamente da criptografia simétrica, a criptografia assimétrica utiliza-se de duas chaves para a codificação ou decodificação de

[27] *Personal Computer*, designação genérica para computadores de uso doméstico ou geral.

uma determinada informação, sendo uma delas denominada de chave pública e a outra de chave privada (STALLINGS, 2015).

FIGURA 3 – Modelo simplificado de encriptação assimétrica.



Fonte: Criptografia e Segurança de Redes: princípios e práticas, 2015, p.58.

No que concerne ao sistema criptográfico assimétrico, pode-se afirmar que a chave privada tem a funcionalidade de identificar a identidade de seu titular, ao passo de que a chave tem pública serve como parâmetro essencial para a troca de informações criptografadas entre o dono das chaves criptográficas e qualquer outro indivíduo. Assim, a chave privada sempre será utilizada para decifrar a codificação criada por uma chave pública pertencente ao mesmo usuário, assim como, da mesma forma, uma chave pública será necessária decifrar uma codificação feita por uma chave privada do mesmo usuário (STALLINGS, 2015).

Em linhas gerais, STALLING (2014) preleciona práticas pertinentes para garantia da inviolabilidade das informações através do uso das modalidades de criptografias descritas na tabela a seguir.

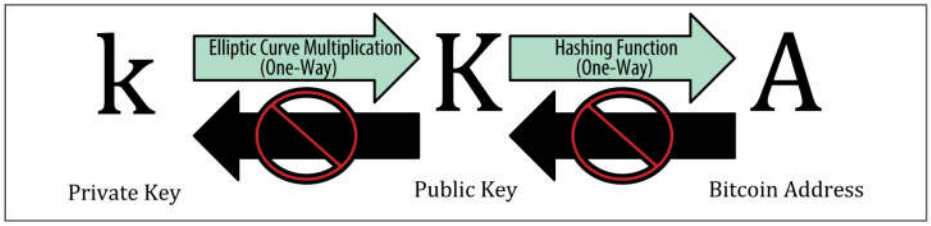
TABELA 4 – Diferenciais entre encriptação convencional (simétrica) e encriptação de chave pública (assimétrica).

ENCRIPTAÇÃO CONVENCIONAL	ENCRIPTAÇÃO DE CHAVE PÚBLICA
Necessário para funcionar:	*Necessário para funcionar:*
1. O mesmo algoritmo com a mesma chave é usado para encriptação e decriptação.	1. Um algoritmo é usado para encriptação, e um relacionado, para decriptação com um par de chaves, uma para encriptação e outra para decriptação.
2. O emissor e o receptor precisam compartilhar o algoritmo e a chave.	2. O emissor e o receptor precisam ter, cada um, uma chave do par (não a mesma).
Necessário para a segurança:	*Necessário para a segurança:*
1. A chave precisa permanecer secreta.	1. Uma das duas chaves precisa permanecer secreta.
2. Deverá ser impossível, ou pelo menos impraticável, decifrar uma mensagem se a chave for mantida secreta.	2. Deverá ser impossível, ou pelo menos impraticável, decifrar uma mensagem se uma das chaves for mantida secreta.
3. O conhecimento do algoritmo mais amostras do texto cifrado precisam ser insuficientes para determinar a chave.	3. O conhecimento do algoritmo mais uma das chaves mais amostras do texto cifrado precisam ser insuficientes para determinar a outra chave.

Fonte: Criptografia e Segurança de Redes: princípios e práticas, 2015, p. 203.

No tocante à utilização de criptografia nas criptomoedas, conforme implementado no Bitcoin, com a instalação local da aplicação *client*, um par de chaves criptográficas serão geradas automaticamente ao usuário nos seguintes termos.

FIGURA 4 – Fluxo de criação de chaves criptográficas no Bitcoin.



Fonte: Mastering Bitcoin, 2014, p.64

Nesse sentido, insta frisar que a tanto a chave pública quanto os endereços da carteira *(wallet)* são gerados pela chave privada criada pela aplicação *client.* Portanto, pode-se afirmar que o sistema de criptografia assimétrica é o recurso responsável por garantir o anonimato dos usuários da rede, bem como a segurança e a concretização das transações financeiras entre os mesmos.

De outra banda, como previamente mencionado, a função criptográfica *hash* é responsável por manter a integridade dos blocos de informação integrantes a cadeia do *blockchain*. Essa estrutura consiste num algoritmo computacional que gera uma sequência alfanumérica (*string)* única sobre o arquivo que foi sujeitado ao referido algoritmo (SWAN, 2015). Ademais, como fora supracitado, todo o bloco de informação

terá um *hash* único que o identifica pelo conteúdo que possui, ao passo de que o conceito central do *proof-of-work*, ou prova de validação criptográfica do bloco de informação, está fundada na função criptográfica *hash* (ANTONOPOULOS, 2014).

Em suma, o emprego da criptografia assimétrica é um recurso essencial para garantir o anonimato dos usuários, bem como a segurança e consolidação das transações financeiras dos usuários da rede criptomoeda, ao passo que o uso da função criptográfica *hash* se trata de um recurso indispensável para gerar o consenso descentralizado entre os usuários, assim como para garantir, quando combinado ao algoritmo do *blockchain,* a inviolabilidade das informações contidas na respectiva estrutura.

3.2.4 O Processo de Mineração e o *Proof-of-Work*

Conforme exposto rapidamente na seção 3.2.1, o processo de mineração em um sistema de criptomoedas é responsável pelo incremento da estrutura de dados do *blockchain,* bem como a emissão de novas moedas deste sistema. Por sua vez, os usuários da rede que viabilizam o processo de mineração são conhecidos como "mineradores". Esses usuários são responsáveis por validar e verificar transações financeiras, assim como os blocos de informação criados para ser inseridos na estrutura do *blockchain*. Todos os usuários mineradores possuem uma cópia local completa do *blockchain*[28] (ANTONOPOULOS, 2014).

Ademais, tais usuários competem entre si para inserir o bloco mais novo no topo da estrutura sequencial e remissiva do *blockchain*, uma vez que esse processo implica na premiação em criptomoedas ao usuário (ou grupo de usuários) que realizar tal feito, bem como o valor das comissões das transações financeiras[29] que integram tal bloco são destinadas ao vencedor do processo de mineração (ANTONOPOULOS, 2014).

---

[28] Recomenda-se a consulta do anexo C do presente para uma melhor compreensão do conceito referenciado.

[29] Como mencionado na tabela 1 do capítulo 2, toda a transação nas criptomoedas possui alguma comissão que, por sua vez, tem como propósito incentivar a participação de usuários de usuários da rede no processo de mineração.

De outra banda, o algoritmo do sistema Bitcoin implementa automaticamente um conceito de escassez de sua moeda, de forma que, com o tempo ou com a própria prática da mineração[30] de moedas, a emissão de moedas seja reduzida progressivamente. Nesse sentido, na atualidade, o processo de mineração remunera os mineradores vencedores da competição de validação de novos blocos com 12,5 *bitcoins*, sendo que o valor desta premiação se reduzirá pela metade (6,25 BTC) em 26 de maio de 2020 ou, se ocorrer primeiro, com a consolidação de 630.000 blocos minerados (ANTONOPOULOS, 2014).

Como previamente mencionado, o algoritmo do Bitcoin estabelece que novos blocos de informação devem ser inseridos na estrutura do *blockchain* a cada 10 minutos. O processo de validação de um bloco ocorre através da prova criptográfica *proof-of-work.* Tal procedimento de prova criptográfica, numa acepção simplificada, trata-se do ato dos mineradores calcularem, através de tentativa e erro, qual número decimal único (*nonce)* cujo valor seja igual ou inferior ao nível de dificuldade de um valor expresso em uma função *hash* gerada pelo próprio algoritmo do sistema do Bitcoin.

Tal nível de dificuldade é medido automaticamente pelo próprio algoritmo do Bitcoin que, por sua vez, utiliza como parâmetros a quantidade de mineradores ativos na rede e o tempo médio para resolução de provas criptográficas em blocos anteriores. Outrossim, o nível de dificuldade está embasado na expressão do próprio *hash* gerado nos blocos de informações, sendo que o nível de dificuldade está fundamentado na quantidade de zeros sucessivos que deverá existir na respectiva expressão[31]. Portanto, quanto maior a quantidade de zeros sucessivos no *hash* que estabelece o nível de dificuldade, mais trabalhosa será a tarefa de achar um número decimal equivalente ou com valor inferior que satisfaça a condição para a criação de um novo bloco para a estrutura do *blockchain.*

Encontrada a solução, esta será verificada pelos demais usuários da rede, ou seja, se o número decimal único (*nonce*) equivale ao *hash* atribuído ao bloco construído pelo

[30] O algoritmo do Bitcoin foi programado para realizar reduções sucessivas de emissão de moeda a cada 4(quatro) anos ou quando houver a mineração de 210.000 blocos de informação. A redução ocorrerá quando qualquer uma das hipóteses ocorrer primeiro (ANTONOPOULOS, 2014, p.174).
[31] Exemplo de um *hash* criptográfico, expresso em notação hexadecimal: 0000000000000002a7bb d25a417c0374cc55 261021e8a9ca74442b01 284f0569 (ANTONOPOULOS, 2014, p.197).

minerador e que, por sua vez, tal *hash* respeite os critérios de dificuldade para a atividade de mineração estabelecida entre os usuários da rede. Se a verificação do novo bloco gerar um resultado positivo, se o usuário que o verificou possuir uma versão do *blockchain* com uma quantidade de blocos menores, automaticamente o novo bloco validado será replicado para todos os usuários cujas versões do *blockchain* possuem uma quantidade menor de blocos. Caso contrário, o bloco minerado que for criado alheio aos padrões de validação de blocos do sistema Bitcoin será descartado pelos demais usuários da rede. (ANTONOPOULOS, 2014).

Em suma, o processo de mineração, bem como o *proof-of-work* são recursos essenciais à emissão de moeda e validação e verificação das transações financeiras respectivamente, ou seja, para que o propósito da criptomoeda de fato se suceda entre os usuários da rede do sistema. Em regra, todos os usuários que participam desses processos, os mineradores, possuem uma cópia local do *blockchain* nos seus dispositivos computacionais. Ademais, toda a validação de conteúdos dos blocos de informação ocorre no escopo estritamente criptográfico, ou seja, via de regra, nenhum minerador da rede verifica qualitativamente o conteúdo dos blocos validados por outros mineradores, apenas a congruência da prova criptográfica do respectivo bloco. Ambos os fatos possuem enorme relevância para as análises que serão realizadas longo do presente trabalho.

3.3 CONCLUSÕES PARCIAIS

3.3.1 Quanto à factibilidade técnica do estudo da RWTH Aachen University

Neste mérito, o estudo da RWTH Aachen University analisou o potencial da inserção de dados não financeiros na estrutura do *blockchain* do Bitcoin, mediante a aplicação de todos os métodos de inserção de dados tradicionais e não padronizados, bem como serviços de inserção de conteúdo disponíveis na *web.*

Com efeito, todas as transações financeiras padronizadas do Bitcoin, utilizadas no estudo supracitado, estão documentadas ao longo do capítulo 5 da obra de Andreas A. Antonopoulos. Conforme descrito por esse autor, toda transação financeira, assim como os blocos de informação construídos com as mesmas transações, precisam

respeitar estruturas básicas para que possam ser validadas e verificadas por outros usuários da rede. Se não houver a observância de tais premissas, nenhuma transação ou bloco de informação será produzido. Portanto, em tese, é possível reconhecer o tipo de método de inserção de dados empregado de acordo com a particularidade estrutural de cada método (OP_RETURN, *Coinbase*, P2PK, P2SH, etc.).

Em contrapartida, apesar da improbabilidade na maioria das ocasiões, transações não padronizadas podem ser validadas de forma inesperada por outros usuários, uma vez que não há nenhum tipo de tecnologia à prova de falhas. Portanto, haja vista que o sistema do Bitcoin é *open source*, assim como qualquer outra criptomoeda, em tese, não há óbice para qualquer usuário desenvolver seu próprio método de inserção de dados capaz de "burlar" as estruturas padronizadas e obrigatórias de uma criptomoeda.

Além disso, quanto ao fato das cópias locais do *blockchain* nos computadores dos usuários mineradores, conforme asseverado ao longo do capítulo 7 da obra de Andreas A. Antonopoulos, com efeito, todo usuário da rede que atua nesta atividade mantêm uma cópia integral do *blockchain* que, por sua vez, estará sujeita a constantes incrementos de conteúdo.

Somado ao fato que a validação de conteúdo dos blocos de informação é automatizada e meramente criptográfica, ou seja, embora haja garantia quanto à inviolabilidade do conteúdo do bloco, todavia, não há nenhuma forma de garantia quanto à verificação da natureza de conteúdo potencialmente censurável ou ilícito. Portanto, ainda que de forma incidental, isso pode implicar que usuários mineradores estejam em posse de dados não financeiros alheios ao seu consenso pessoal com conteúdo potencialmente censurável ou ilícito.

Ante as premissas apresentadas ao longo do presente capítulo, pode-se afirmar que o estudo da RWTH Aachen University possui factibilidade técnica e conceitual.

3.3.2 Quanto às implicações fáticas e jurídicas resultantes das descobertas do estudo da RWTH Aachen University

Como fora discorrido ao longo do presente trabalho, sedimentou-se que a participação em sistemas de pagamentos como o Bitcoin ou qualquer outra criptomoeda em geral oferece um novo conceito de liberdade monetária. Todavia, apesar das aparentes vantagens como, por exemplo, a garantia de segurança de transações

financeiras independente da intervenção direta de um terceiro na respectiva transação, o sistema de criptomoeda oferecem riscos ocultos significativos, especialmente no tocante ao processo de mineração de moedas.

As descobertas do estudo da RWTH Aachen University revelaram um espectro preocupante quanto à prática de mineração. Como asseverado na seção anterior, o consenso descentralizado em uma rede de criptomoedas ocorre de forma automática e impessoal. Logo, para fins de validação de um bloco de informação, a validação é meramente criptográfica, não ocorrendo qualquer avaliação acerca do conteúdo não financeiro inserido no bloco de informação que fará parte da estrutura do *blockchain.* Após a inserção do bloco de informação no *blockchain*, sua modificação ou retirada é irreversível conforme os procedimentos padrões do algoritmo da respectiva estrutura.

Portanto, ante as premissas fáticas e conceituais apresentadas ao longo do presente trabalho, pode-se aduzir que todo o usuário que exerce atividades de mineração da rede Bitcoin estaria em posse dos arquivos digitais censuráveis ou ilícitos, descritos na seção 4.3 no estudo da RWTH Aachen University e referenciados no segundo capítulo deste trabalho.

Provavelmente, na maioria dos casos, tais usuários sequer possuem consciência sobre a posse de tais arquivos. Contudo, tal fato enseja uma zona gris quanto aos limites da imputação penal cabíveis a estes indivíduos, uma vez que, em tese, embora possa haver tipicidade penal formal sobre a posse de determinados tipos de arquivos digitais; para justificar a punibilidade do agente, a aferição da presença do elemento subjetivo do tipo penal pode ser uma tarefa tortuosa ao operador do direito diante das premissas fáticas e conceituais apresentadas ao longo deste trabalho.

Sendo assim, tal problemática jurídica será analisada com maior profundidade no capítulo a seguir.

4. OS LIMITES DA IMPUTAÇÃO PENAL APLICÁVEIS AOS USUÁRIOS “MINERADORES” DA CRIPTOMOEDA BITCOIN

Neste capítulo serão analisadas as dimensões jurídicas concernentes as questões fáticas e técnicas expostas, respectivamente, no segundo e terceiro capítulos do presente

trabalho, bem como a discussão dos limites de sua aplicabilidade. Na seção 4.1, serão apresentadas as premissas jurídicas adotadas para fins de análise do caso concreto, descrito no capítulo 2 do presente trabalho, enquanto que a discussão acerca da aplicabilidade das respectivas premissas será abordada na seção 4.2 deste capítulo.

4.1 PREMISSAS DOUTRINÁRIAS ADOTADAS.

Inicialmente, cumpre esclarecer que o conteúdo que será apresentado a seguir fornecerá uma visão sistêmica sobre alguns institutos jurídicos que integram o Direito Penal brasileiro, essenciais à análise jurídica que será discorrida na seção 4.2.

Contudo, em prol da objetividade e precisão almejadas no presente trabalho, receberam maior destaque apenas os institutos jurídicos cuja pertinência para a referida análise jurídica seja indispensável. Sendo assim, os demais institutos jurídicos que não obtiverem tais qualidades para os fins supracitados, ao longo deste capítulo, serão mencionados, se necessário, de forma oportuna e pontual.

4.1.1 Premissas Principiológicas

Nesta perspectiva, adotaremos o conceito norteador como princípio de Direito do presente trabalho conforme descrito por Miguel Reale na sua obra "Lições Preliminares de Direito":

> [...] princípios gerais de direito são enunciações normativas de valor genérico, que condicionam e orientam a compreensão do ordenamento jurídico, quer para a sua aplicação e integração, quer para a elaboração de novas normas. Cobrem, desse modo, tanto o campo da pesquisa pura do Direito quanto o de sua atualização prática (REALE, 2002, p. 282).

A seguir, serão abordados os princípios de Direito Penal com maior relevância na doutrina jurídica e no ordenamento jurídico brasileiro.

4.1.1.1 Princípio da Legalidade e Princípio da Reserva Legal

De acordo com Bitencourt (2012), os princípios da legalidade e da reserva legal delimitam que a elaboração de normas incriminadoras se trata de uma função estrita à lei, implicando assim que nenhum fato poderá ser considerado criminoso, bem como se

considerará incabível qualquer forma de aplicação de pena ou sanção ao respectivo fato, se não houver lei previa que o defina como crime e que atribua-lhe sanção correspondente. Portanto, toda conduta que for considerada como criminosa deve ter sua definição precisa e inequívoca em texto legal.

De outra banda, Pacelli e Callegari (2016) corroboram os conceitos tradicionais supracitados e, ainda, aduzem que o princípio da legalidade, no âmbito da matéria penal, abrangeria o conceito do princípio de reserva legal, uma vez que a expressão *legalidade* é revestida de uma dimensão mais ampla, referindo-se a totalidade do ordenamento jurídico.

Consoante ao entendimento acima exposto, Nucci (2017) assevera que tais princípios penais possuem fulcro no disposto no art. 5.º, XXXIX, da *Carta Magna*[32], ao passo de que o termo *lei*, abrangido por ambos os princípios, é compreendido no sentido estrito da expressão, ou seja, a norma penal deverá ser emanada pelo Poder Legislativo, dentro da sua esfera de competência, cuja atribuição pertence ao Congresso Nacional como regra.

4.1.1.2 Princípio da Irretroatividade da Lei Penal

Nesta esteira, Pacelli e Callegari (2016) prelecionam o princípio da irretroatividade da lei penal como um consectário igualmente lógico e evidente do princípio da legalidade, assim como o mesmo fato ocorre entre este princípio e o princípio da reserva legal:

> Toda lei que pretender a sua aplicação a uma hipótese passada terá sua validade condicionada à natureza de seu conteúdo: se for benéfica, poderá ser aplicada; se não o for, ou seja, se contiver nova definição de crime, ou o aumento de pena, ou, ainda, qualquer outro prejuízo ao agente, não poderá ser aplicada (PACELLI; CALEGARI, 2016, p. 93).

Por sua vez, Nucci (2017) aborda o conceito do princípio em análise pela sua denominação complementar: princípio da retroatividade da lei penal benéfica. Como explanado pelo autor em questão, leis penais benéficas podem voltar no tempo para

[32] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
(...) XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal; (BRASIL,1988)

favorecer o agente que cometera um crime, ainda que o fato tenha decisão condenatória transitada em julgado, conforme positivado no inciso art. 5, XL, da *Carta Magna*[33].

Por fim, Bitencourt (2012, p.46) assevera que leis temporárias ou excepcionais são espécies de fontes normativas que constituem exceções ao princípio da irretroatividade penal, uma vez que se tratam de normas penais ultrativas[34] previstas no Código Penal: "[...] mesmo esgotado seu período de vigência, terão aplicação aos fatos ocorridos durante a sua vigência. São leis de vida curta e cujos processos, de regra, estendem-se para além do período de sua vigência".

4.1.1.3 Princípio da Intervenção Mínima e Princípio da Fragmentariedade

Conforme preleciona Nucci (2017), o princípio da intervenção mínima parte do pressuposto de que a lei penal não deve ser vista como a primeira opção (*prima ratio*) do legislador como forma de solução para os conflitos existentes na sociedade, fato perene inerente no convívio em coletividades. Nesse sentido, o autor salienta que há outros ramos do Direito com maior aptidão para solucionar as desavenças ou lides que podem surgir entre os integrantes da comunidade. Logo, o princípio da intervenção mínima concebe o Direito Penal como o último recurso ou *ultima ratio* para composição de conflitos sociais.

Na concepção de Pacelli e Callegari, tal princípio possui contornos mais abrangentes no tocante à política criminal e no escopo da hermenêutica penal, *in verbis*:

> Para nós, a intervenção mínima surge como a alternativa efetivamente acolhida pela ordem jurídica nacional para a configuração de seu Direito Penal, e, mais especificamente, no âmbito da hermenêutica penal. Constitui, sim, matéria de observância necessária no âmbito da política criminal, mas, também, instrumental apto e suficiente a exercer controle do excesso incriminador no interior dos tipos penais, ocupando papel relevante no campo da prática do direito, quando nada para diminuir o alcance da respectiva incidência (dos tipos), quando desconectada com o sistema geral de reprovações e de condutas proibidas. Em um Estado de Direito, o máximo que se concede em matéria penal é a intervenção mínima. (PACELLI; CALEGARI, 2016, p. 84).

---

[33] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
(...) XL - a lei penal não retroagirá, salvo para beneficiar o réu; (BRASIL,1988)

[34] Art. 3º - A lei excepcional ou temporária, embora decorrido o período de sua duração ou cessadas as circunstâncias que a determinaram, aplica-se ao fato praticado durante sua vigência. (BRASIL,1940)

Em virtude das premissas acima expostas, conforme asseverado por Bitencourt (2012, p.45) e corroborado pelos demais autores supracitados, o princípio da fragmentariedade, corolário ao princípio da intervenção mínima, concebe que o Direito Penal "[...] não deve sancionar todas as condutas lesivas dos bens jurídicos, mas tão somente aquelas condutas mais graves e mais perigosas praticadas contra bens mais relevantes". Outrossim, o autor em comento ainda salienta que tal princípio repercute decisivamente na norma penal no que concerne tanto ao seu alcance de aplicabilidade quanto aos limites de seu conteúdo.

4.1.1.4 Princípio da Adequação Social e Princípio da Insignificância

De acordo com Nucci (2017), os princípios da adequação social e da insignificância são decorrentes do princípio da intervenção mínima. Segundo o autor em comento, o princípio da adequação social se baseia na premissa de que, quando uma prática ou conduta que se torna socialmente aceitável e assimilada pelos costumes de determinada coletividade, não há como caracterizá-las como lesivas ao bem jurídico. Ainda, Nucci (2017, p.146) preconiza que o princípio da insignificância caracteriza-se pela "[...] desnecessidade de se aplicar sanção penal a uma infração considerada insignificante em relação à proporcionalidade da lesão ao bem jurídico tutelado pela lei penal".

Por sua vez, Pacelli e Callegari (2016) mencionam que o princípio da adequação social fora elaborado por Hans Welzel. Segundo os autores, entende-se como "socialmente adequadas são todas as atividades que se movem dentro do marco das ordens ético-sociais da vida social, estabelecidas por intermédio da história" (WELZEL, 1956 *apud* PACELLI; CALEGARI, 2016, p.204). Em contrapartida, concebido por Claus Roxin, o princípio da insignificância deve ser compreendido como uma abordagem interpretativa sobre condutas típicas que ensejam *danos de pouca importância* (ASSIS TOLEDO, 1994). Nessa esteira, Assis Toledo ilustra a dimensão da aplicabilidade do referido instituto jurídico no ordenamento jurídico brasileiro, *in verbis*:

> [...] segundo o princípio da insignificância, que se revela por inteiro pela sua própria denominação, o direito penal, por sua natureza fragmentária, só vai até onde seja necessário para a proteção do bem jurídico. Não deve ocupar-se de bagatelas. Assim, no sistema penal brasileiro, por exemplo, o dano do art. 163 do Código Penal não deve ser qualquer lesão à coisa alheia, mas sim

> aquela que possa representar prejuízo de alguma significação para o proprietário da coisa [...] (ASSIS TOLEDO, 1994, p.133).

Finalmente, como ponderado por Bitencourt (2012), o princípio da adequação social, *per se,* não é suficiente para decidir a relevância típica do comportamento, uma vez que toda conduta enseja certo grau de perigo e, em abstrato, possua o potencial de gerar algum resultado típico; ao passo de que, no que se refere ao princípio da insignificância, a insignificância de determinada conduta só poderá ser valorada em contraste com a *consideração global* da ordem jurídica.

4.1.1.5 Princípio da Ofensividade ou Lesividade

Segundo as lições de Pacelli e Callegari (2016, p.87-88), o princípio da ofensividade ou lesividade se caracteriza quando determinada conduta "[...] implique um risco efetivo, e racionalmente justificado, ao bem jurídico protegido na norma penal incriminadora, quando não o dano concreto e consumado". Em contrapartida, tal concepção é combatida por Nucci e Bitencourt.

Nucci (2017) defende que o princípio da ofensividade ou lesividade decorre diretamente da observância do princípio da intervenção mínima. Em razão disso, Nucci sustenta que a ofensividade ou lesividade deve estar presente no contexto do tipo penal incriminador para que este, por sua vez, seja validado e legitimado; caso contrário, isso ensejaria o esgotamento do Direito Penal em situações com situações inócuas e sem propósito.

Por fim, Bitencourt (2012, p. 49-50) afirma que "[...] o legislador deve abster-se de tipificar como crime ações incapazes de lesar ou, no mínimo, colocar em perigo concreto o bem jurídico protegido pela norma penal". Segundo o autor em comento, a inobservância da referida premissa implicaria em um tipo penal de *perigo abstrato* que, por sua vez, tratar-se-ia de uma hipótese de inconstitucionalidade do respectivo tipo penal (BITENCOURT, 2012). Portanto, segundo Bitencourt, se o bem jurídico não for exposto a risco efetivo ou lesão concreta, não haveria de se falar em ofensividade ou lesividade e, consequentemente, na ocorrência de infração penal.

4.1.1.6 Princípio de Culpabilidade

Conforme preleciona Nucci (2017), o princípio da culpabilidade possui fundamento na máxima consubstanciada no tradicional brocardo jurídico *nullum crimen sinen culpa*; ou seja, a responsabilidade penal só ocorrerá na modalidade subjetiva, bem como apenas se houver a efetiva constatação de que o autor do crime tenha agido com dolo ou culpa. Tal premissa encontra-se positivada no parágrafo único do art. 18 do Código Penal[35].

Ademais, o princípio da Culpabilidade, na concepção de JESCHECK tem como finalidade por um lado "conferir a necessária proteção do indivíduo em face de eventual excesso repressivo do Estado, fazendo com que a pena, por outro, circunscreva-se às condutas merecedoras de um juízo de desvalor ético-social" (JESCHECK, 1981 *apud* NUCCI, 2017, p.171).

De outra banda, consoante as premissas previamente expostas, Bitencourt (2012) assevera que o conceito de culpabilidade possui três dimensões distintas no âmbito do Direito Penal: a) instituto jurídico que fundamenta a pena; b) elemento de determinação ou aferição da pena; e c) conceito diametralmente oposto à responsabilidade objetiva. Em virtude disso, segundo o autor em comento, tais dimensões ensejam as seguintes repercussões materiais:

> [...] a) *inadmissibilidade da responsabilidade objetiva pelo simples resultado;* b) somente cabe *atribuir responsabilidade penal pela prática de um fato típico e antijurídico, sobre o qual recai o juízo de culpabilidade, de modo que a responsabilidade é pelo fato e não pelo autor;* c) *a culpabilidade é a medida da pena.* [...] (BITENCOURT, 2012, p.52).

Por fim, Bitencourt (2012, p. 52) conclui que o princípio da culpabilidade se trata de "[...] uma garantia fundamental dentro do processo de atribuição de responsabilidade penal, repercutindo diretamente na composição da culpabilidade enquanto categoria dogmática".

4.1.1.7 Princípio da Proporcionalidade

[35]Art. 18 - Diz-se o crime:
Crime doloso
I - doloso, quando o agente quis o resultado ou assumiu o risco de produzi-lo;
Crime culposo
II - culposo, quando o agente deu causa ao resultado por imprudência, negligência ou imperícia. Parágrafo único - Salvo os casos expressos em lei, ninguém pode ser punido por fato previsto como crime, senão quando o pratica dolosamente. (BRASIL,1940)

Segundo Bitencourt (2012), a justificação de um *sistema penal* estará garantida quando houver equilíbrio entre a *soma das violências* que o respectivo sistema for capaz de prevenir não superar as violências que serão constituídas através da cominação de penas.

Nesse sentido, o autor em comento cita a doutrina de Hassermer que, por sua vez, preconiza o princípio da proporcionalidade como "uma concordância material entre ação e reação, causa e consequência jurídico-penal, constituindo parte do postulado de Justiça: ninguém pode ser incomodado ou lesionado em seus direitos com medidas jurídicas desproporcionadas" (HASSERMER, 1984 *apud* BITENCOURT, 2012, p.55).

Por fim, em consonância com o exposto pelo autor supracitado, Nucci (2017) sintetiza que o princípio da proporcionalidade consiste na harmonização entre a gravidade da infração penal cometida em relação às penas que lhes são imputadas, sendo inadmissível a excessiva majoração ou liberalidade descabida no ato da cominação das sanções penais.

4.1.2 Limites Conceituais sob a Ótica da Teoria do Crime

4.1.2.1 Conceito de Crime

Numa abordagem mais pontual e sintética, embora insuficiente para a dogmática penal, segundo Assis Toledo (1994, p.80), o referido autor conceituou o termo *crime* como "um fato humano que lesa ou expõe a perigo bens jurídicos (jurídico-penalmente) protegidos". Em virtude disso, o autor em comento menciona a dificuldade da abordagem conceitual do conceito de crime, consubstanciada na reflexão realizada por ROXIN, *in verbis*:

> [...] quase todas as teorias do delito, apresentadas até agora, 'são sistemas de elementos' que desintegram a conduta delitiva em uma pluralidade de características concretas (objetivas, subjetivas, normativas, descritivas etc.), as quais são incluídas nos diferentes graus da estrutura do crime e depois reunidas, como um mosaico, para a formação do fato punível. (ROXIN, 1972 *apud* ASSIS TOLEDO, 1994, p.79).

Dado o impasse conceitual acima exposto, ao longo do tempo, o estudo da teoria do crime desenvolveu acepção mais analítica, proposta por diversos juristas de diversas nacionalidades. A seguir, serão apresentados os elementos essenciais que compõem a dimensão conceitual da teoria do crime.

4.1.2.1.1 Conceito Material

Na sua dimensão material, conforme ensina Pacelli e Callegari (2016, p.156-157), considera-se como crime "[...] todo o fato humano que lesiona um interesse capaz e comprometer as condições de existência, de conservação e de desenvolvimento da sociedade". Ainda, o autor em comento cita a visão de ROXIN acerca do tema, *in verbis:*

> [...] enquanto que mediante o 'conceito formal de delito' a conduta punível só é objeto de uma definição no marco do Direito positivo, o conceito material de delito se remonta antes do respectivo Direito Penal codificado e pergunta pelos critérios materiais da conduta punível. Portanto, o conceito material de delito é anterior ao Código Penal e subministra ao legislador um critério político-criminal sobre o que o mesmo pode condenar e o que deve deixar impune. (ROXIN, 1972 *apud* PACELLI; CALLEGARI, 2016, p.156-157).

Portanto, pode-se afirmar que o conceito material de crime abrange todas as condutas humanas naturalmente reprováveis quando realizadas no convívio social, sendo estas dignas de serem transformadas em tipos penais incriminadores como uma forma de garantir a paz social e a coexistência em coletividade.

4.1.2.1.2 Conceito Formal

Por sua vez, a dimensão formal do conceito de crime trata-se da caracterização de determinada conduta humana como proibida por força de lei. Como preconiza Nucci (2017), entende-se como crime toda a conduta formalmente proibida por lei penal cujo descumprimento acarretará em aplicação de pena.

Por fim, como devidamente mencionado por Pacelli e Callegari (2016), o conceito formal de crime abrange apenas o aspecto externo da conduta criminosa, ou seja, o conteúdo desta não é contemplado neste escopo conceitual. Em virtude disso, Pacelli e Callegari (2016, p.156) ainda acrescentam que a acepção formal de crime se entende "[...] como a conduta proibida na lei penal, independentemente de qualquer análise valorativa ou de relevância".

4.1.2.1.3 Conceito Analítico (jurídico)

Conforme preleciona Assis Toledo (1994), a conduta criminosa é resultante de uma ação ou omissão humana que, por sua vez, para receber tal qualificação, a respectiva conduta deverá passar por uma tríplice ordem de valoração perante os seguintes elementos dogmáticos: tipicidade, ilicitude e culpabilidade.

Nesse sentido, NUCCI esclarece que o conceito analítico de crime, sob a luz da teoria da tripartida finalista, *in verbis*:

> [...] tem-se o crime como uma conduta típica, ilícita e culpável, vale dizer, uma ação ou omissão ajustada a um modelo legal de conduta proibida (tipicidade, onde estão contidos os elementos subjetivos dolo e culpa), contrária ao direito (antijuridicidade) e sujeita a um juízo de reprovação social incidente sobre o fato e seu autor, desde que existam imputabilidade, consciência potencial de ilicitude e exigibilidade e possibilidade de agir conforme o direito (culpabilidade). (NUCCI, 2017, p.351).

Finalmente, imperioso frisar que o conceito analítico de crime possui uma vasta diversidade doutrinária, com concepções bastante distintas acerca dos números e funções dos elementos que o compõem, bem como seus respectivos enfoques de análise quanto à conduta criminosa (teorias da ação).

4.1.2.1.3.1 Breve Panorama Doutrinário

Em linhas gerais, quanto à composição dos elementos constituintes do conceito analítico de crime, merecem destaque as seguintes correntes doutrinárias: a) bipartida; b) tripartida finalista; c) tripartida causalista; e d) quadripartida.

Na primeira corrente, entende-se o crime como um fato típico e culpável, sendo a ilicitude um elemento abrangido pela tipicidade. No que se refere à segunda corrente doutrinária, aduz-se como crime toda a conduta típica, antijurídica e culpável se houver elementos fáticos permitam a imputabilidade do agente, a verificação da consciência quanto ao potencial de ilicitude de sua conduta, bem como a existência da exigibilidade de conduta diversa. Por sua vez, a terceira corrente concebe o crime como um fato típico, antijurídico e culpável, todavia, o que difere esta corrente doutrinária em relação à anterior subjaz no fato que o elemento subjetivo do crime está contido no âmbito da culpabilidade. Por fim, a última corrente sustenta que o crime seria composto por um fato típico, antijurídico, culpável e punível, sendo o último elemento a inovação da corrente doutrinária em comento (NUCCI, 2017).

Ademais, segundo Nucci (2017), embora haja divergências conceituais entre defensores do finalismo penal e defensores do causalismo penal, a concepção tripartida do delito possui aceitação majoritária na doutrina e na jurisprudência pátria. Em maior ou menor medida, todas as correntes doutrinárias acima expostas possuem representação no Brasil e no exterior.

De outra banda, no tocante às teorias da ação, há diversas linhas doutrinárias a citar o causalismo, o neokantismo, o finalismo, a teoria social da ação, funcionalismo, dentre outros. Nesse sentido, há divergências entre os doutrinadores quanto ao sistema penal adotado pelo direito brasileiro. Nucci (2017) sustenta que, apesar da reforma penal de 1984, o Código Penal pátrio não adotou o finalismo ou sequer abandonou o causalismo ou neokantismo, cujos sistemas inspiraram sua criação. Por fim, NUCCI teceu a seguinte crítica sobre a divergência doutrinária previamente exposta:

> Alegam alguns que a doutrina clássica estaria superada após a Reforma Penal de 1984, sendo cabível considerar que, tendo sido adotada a teoria finalista, o dolo e a culpa passaram a integrar a conduta típica, razão pela qual a culpabilidade transformou-se em mero pressuposto de aplicação da pena. Continua, segundo pensamos, inconsistente tal postura. Em primeiro lugar, apesar de a reforma mencionada possuir contornos nitidamente finalistas, não foram eles suficientes para transformar a Parte Geral do Código Penal em finalista. Além disso, nenhuma modificação foi feita na estrutura do crime, como se pode observar na Exposição de Motivos de 1984. Em segundo lugar, há muitos finalistas que continuam vendo o crime como fato típico, antijurídico e culpável (NUCCI, 2017, p.351).

Ante o exposto, para fins de análise do problema jurídico que será desenvolvida na seção 4.2, será adotado o conceito analítico de crime construído a partir das premissas da teoria tripartida finalista do crime, cujo conceito será aprofundado a seguir.

4.1.2.1.3.2 A Teoria Tripartida Finalista

Como previamente mencionado, no espectro da teoria tripartida finalista, compreende-se como crime toda a conduta típica, antijurídica e culpável se houver elementos fáticos permitam a imputabilidade do agente, observada a verificação da consciência quanto ao potencial de ilicitude de sua conduta, bem como a existência da exigibilidade de conduta diversa. A seguir, serão analisados os elementos constituintes conceito analítico de crime supracitado.

4.1.2.1.3.2.1 Fato Típico ou Tipicidade

Preliminarmente, torna-se imperioso explicitar o conceito de tipo penal para assim adentrar efetivamente ao conceito de tipicidade. Nesse mérito, Nucci (2017, p.418) descreve o tipo penal como uma "[...] descrição abstrata de uma conduta, tratando-se de uma conceituação puramente funcional, que permite concretizar o princípio da reserva legal".

Por sua vez, todo o tipo penal positivado na ordem jurídica deverá possuir as seguintes estruturas: título ou "*nomem juris*", preceito primário, preceito secundário. A primeira estrutura consiste na rubrica conferida pelo legislador sobre o conteúdo do tipo penal, ou seja, o substantivo ou expressão que sintetiza a natureza da conduta proibida descrita no tipo penal. Em seguida, a segunda estrutura se refere ao conteúdo do tipo pena, bem como a descrição da conduta proibida. Por fim, a última estrutura representa a parcela sancionadora ou a pena propriamente dita, cabível quando houver infração do respectivo tipo penal, cuja existência só ocorre em tipos penais incriminatórios (NUCCI, 2017).

Ainda, a doutrina jurídica elaborou diversas classificações possíveis para contextualizar o conteúdo do tipo penal: aberto, fechado, objetivo, subjetivo, básico, derivado, simples, misto, dentre outros.

Realizada a abordagem conceitual preliminar necessária, conforme preleciona Pacelli e Callegari (2016, p.168), concebe-se a tipicidade como "[...] a conformidade, a correspondência, da conduta concretamente praticada à descrição abstrata contida na norma penal".

Em contrapartida, Nucci (2017) salienta que a tipicidade de determinada conduta implica na sua antinormatividade, contudo, nem sempre isso enseja na antijuridicidade da mesma. Para ilustrar tal premissa, NUCCI menciona as lições de Cláudio Brandão:

> [...] a averiguação da tipicidade, portanto, não é conhecida com a contradição da conduta com o ordenamento jurídico, que é a antijuridicidade, mas com a contradição da norma proibitiva, isto é, com a antinormatividade. A antinormatividade é plenamente concretizada com a realização de uma conduta que se amolde a um tipo penal, pois toda conduta amoldada àquele viola a norma que logicamente se extrai da sua definição legal (BRANDÃO, 2012 *apud* NUCCI, 2017, p.431).

Dentre as espécies de tipicidades pertinentes à análise do problema jurídico que será desenvolvida na seção 4.2, revela-se pertinente a adoção da seguinte nomenclatura: tipicidade formal e tipicidade material. A primeira forma de tipicidade ocorre quando há correspondência imediata entre identidade de um fato concreto entre uma conduta proibida descrita em um ou mais tipos penais, ao passo que a segunda forma de tipicidade incide quando determinado bem jurídico, tutelado pela ordem jurídica, é sujeitado à lesão ou perigo de lesão com efetividade.

Além disso, haja vista que o sistema penal adotado no presente trabalho como premissa conceitual é o finalismo penal, conforme idealizado por Hans Welzel, o dolo e a culpa integram como aspectos essenciais para aferição da dimensão da tipicidade da conduta criminosa. Em razão disso, a explanação de tais institutos são indispensáveis para a compreensão da análise jurídica que será exposta na seção 4.2 deste trabalho.

Numa abordagem conceitual pontual, Bitencourt apresenta classificações de condutas criminosas, admitidas no sistema penal brasileiro, de acordo com a natureza do elemento volitivo das respectivas condutas, *in verbis:*

> Diz-se o crime *doloso*, segundo definição do nosso Código Penal, quando o agente quis o resultado ou assumiu o risco de produzi-lo; *culposo*, quando o agente deu causa ao resultado por imprudência, negligência ou imperícia (art. 18 do CP). *Preterdoloso* ou preterintencional é o crime cujo resultado total é mais grave do que o pretendido pelo agente. Há uma conjugação de dolo (no antecedente) e culpa (no subsequente): o agente quer um *minus* e produz um *majus.* (BITENCOURT, 2012, p. 235).

Ainda, no tocante ao dolo, Nucci descreve elementos conceituais essenciais para caracterização do dolo na ação criminosa:

> *a) abrangência*: o dolo deve envolver todos os elementos objetivos do tipo, aquilo que MEZGER chama de "valoração paralela na esfera do leigo". Ilustrando, espera-se, no crime de homicídio, queira o autor matar (eliminar a vida), tendo por objeto alguém (pessoa humana). Se faltar dolo em qualquer dos elementos objetivos do tipo incriminador, inexiste possibilidade de se configurar o homicídio, ao menos na sua forma dolosa;
>
> *b) atualidade:* o dolo deve estar presente no momento da ação, não existindo dolo subsequente, nem dolo anterior. Algumas vozes sustentam a viabilidade de se constatar o dolo subsequente, citando, como exemplo, a apropriação indébita. O sujeito receberia um determinado bem, havendo a transferência de posse; posteriormente, quando o proprietário o pede de volta, o agente nega, apropriando-se. Ele estaria agindo com dolo subsequente à conduta, considerando-se esta como a entrega do bem. O equívoco dessa posição concentra-se na análise do verbo do tipo, que é apropriar-se. O autor somente se apropria do bem quando se recusa a devolvê-lo (dolo atual), e não quando o recebeu do proprietário em confiança;
>
> *c) possibilidade de influenciar o resultado:* é indispensável que a vontade do agente seja capaz de produzir o evento típico. Na lição de WELZEL, "a vontade impotente não é um dolo relevante de um ponto de vista jurídico penal". E ainda: "A vontade de realização do tipo objetivo pressupõe a possibilidade de influir no curso causal, pois tudo o que estiver fora da possibilidade de influência concreta do agente pode ser desejado ou esperado, mas não significa querer realizá-lo. Somente pode ser objeto da norma jurídica algo que o agente possa realizar ou omitir". (NUCCI, 2017, p. 451-452).

Nesse sentido, doutrinariamente, o dolo é compreendido como espécie de elemento volitivo consubstanciado na conduta típica que, por sua vez, possui as seguintes espécies: dolo direto, dolo eventual e preterdolo. Quanto à pertinência de tais

institutos em relação ao objeto de análise jurídica do presente trabalho, serão abordadas e aprofundadas as particularidades inerentes ao dolo direto e dolo eventual.

No que concerne ao dolo direto, este instituto é subdividido em duas modalidades: dolo direto de primeiro grau e dolo direto de segundo grau. Ambas as modalidades de dolo direto estão positivadas no art. 18, inciso I, primeira parte, do Código Penal.

O dolo direito de primeiro grau se caracteriza pela busca consciente do agente em realizar o tipo penal, independente de tal intento produzir resultados certos ou prováveis e conexos a própria ação típica perpetrada pelo agente (PACELLI; CALLEGARI, 2016).

Por sua vez, o dolo direto de segundo grau, também conhecido como *dolo de consequências necessárias,* abrange as mesmas características do dolo direto de primeiro grau quanto à intenção do agente em consumar o fato típico. Contudo, a particularidade dessa espécie de dolo consiste na premissa do agente assumir, no seu intento, consequências que lhe sejam desnecessárias ou desagradáveis para o resultado final que inicialmente almejara na conduta criminosa (PACELLI; CALLEGARI, 2016).

Sendo assim, com consciência das repercussões possíveis de seus atos, o agente agirá dolosamente, com extravagância, para garantir a consumação da finalidade que o motivou um fato típico, desde que tais atos lhe garantam o resultado pretendido na conduta criminosa primária (PACELLI; CALLEGARI, 2016).

De outra banda, no que se refere ao dolo eventual, instituto positivado no art. 18, inciso I, segunda parte, do Código Penal, consolida-se quando o agente não deseja diretamente a consumação do tipo penal, mas o aceita como possível ou até provável, agindo de forma a assumir o risco da produção do resultado (BITENCOURT, 2012). Nessa esteira, o autor em comento menciona as lições de Nelson Hungria quanto à abrangência da caracterização do dolo eventual:

> […] assumir o risco é alguma coisa mais que ter consciência de correr o risco: é consentir previamente no resultado, caso este venha efetivamente a ocorrer. Essa espécie de dolo tanto pode existir quando a intenção do agente dirige-se a um fim penalmente típico como quando dirige-se a um resultado extratípico. (HUNGRIA, 1978 *apud* BITENCOURT, 2012, p.305).

Outrossim, Bitencourt (2012) demonstra uma abordagem possível quanto a distinção entre o dolo direto em relação ao dolo eventual: o primeiro se caracteriza pelo

emprego da vontade do agente por *causa* do resultado da conduta, ao passo de que o segundo se traduz pelo emprego da vontade deste *apesar* do resultado da conduta. Ou seja, como aduzem Pacelli e Callegari (2016, p. 209) o dolo eventual como uma conduta "[...] compreendida pela atitude de indiferença" quanto seu resultado final correspondente.

Tais modalidades de dolo, de acordo com o disposto na redação do texto Exposição de Motivos do Código Penal de 1940, são equiparadas quanto aos seus efeitos, conforme fundamentado pelo Ministro Francisco Campos, *in verbis*:

> […] O *dolo eventual* é, assim, plenamente equiparado ao *dolo direto*. É inegável que arriscar-se conscientemente a produzir um evento vale tanto quanto querê-lo: ainda que sem interesse nele, o agente o ratifica *ex ante*, presta anuência ao seu advento (BRASIL, 1969, p.126).

Em contrapartida, conforme preleciona Nucci (2017, p. 461), a culpa se caracteriza pelo "[...] comportamento voluntário desatencioso, voltado a um determinado objetivo, lícito ou ilícito, embora produza resultado ilícito, não desejado, mas previsível, que podia ter sido evitado". Tal comportamento representa a exceção do sistema penal, sendo aplicável a sanção por delito culposo quando houver disposição legal expressa (NUCCI, 2017).

Por sua vez, a aferição da possibilidade do agente de prever o resultado danoso causado deve ocorrer sob a observação de dois prismas: objetivo e subjetivo. Quanto ao aspecto objetivo, entende-se a aplicação da concepção comum do *homem médio* ou *homem prudente*, ao passo de que, quando o aspecto subjetivo é avaliado, analisam-se as circunstâncias pessoais do agente perante no contexto fático da conduta delituosa (NUCCI, 2017).

Ainda, Nucci elenca os componentes que integram conceitualmente a culpabilidade:

> a) concentração na análise da conduta voluntária do agente: o mais importante na culpa é a análise do comportamento, e não do resultado; portanto, o desvalor da ação ou omissão é o enfoque mais relevante. O resultado, por ser involuntário, não desejado pelo agente, não é valorado com a mesma precisão [...];
>
> b) ausência do dever de cuidado objetivo: significa ter o agente deixado de seguir as regras básicas de atenção e cautela, exigíveis de todos os que vivem em sociedade. Essas regras gerais de cuidado derivam da proibição de ações de risco, que vão além daquilo que a comunidade juridicamente organizada está disposta a tolerar. O denominado dever de cuidado objetivo representa a obrigação de quem vive em comunidade de seguir certas regras impostas a

> todos, por isso, são objetivas, não dependentes de interpretação subjetiva de seus destinatários, nem de habilidades especiais [...];
>
> c) resultado danoso involuntário: como regra, os crimes culposos – ao menos os mais relevantes – são de dano; aguarda-se, então, a ocorrência de um resultado naturalístico danoso, porém involuntário. Esse resultado nunca poderá ter origem, mesmo remota, no querer do agente. Quem age de forma culposa produz uma conduta descuidada, desatenciosa e ilícita, mas não tem a mente voltada para o que pode acontecer, como um fato certo. Passando-se à esfera do resultado provável, o autor da conduta ingressa no território do dolo eventual. No máximo, sai da culpa consciente e chega somente até a culpa inconsciente. De todo modo, é imprescindível que o evento lesivo jamais tenha sido desejado ou acolhido pelo agente;
>
> d) previsibilidade: é a possibilidade de prever o resultado lesivo, inerente a qualquer ser humano normal. Ausente a previsibilidade, afastada estará a culpa, pois não se exige da pessoa uma atenção extraordinária e fora do razoável. O melhor critério para constatar a previsibilidade é o critério objetivo-subjetivo, ou seja, verifica-se, no caso concreto, se a média da sociedade (homem médio ou prudente) teria condições de prever o resultado, mediante a diligência e da perspicácia comuns, passando-se em seguida à análise do grau de visão do agente do delito, vale dizer, verifica-se a capacidade pessoal que o autor tinha para evitar o resultado (NUCCI, 2017, p. 463-465).

No tocante à abordagem conceitual sobre a culpabilidade, insta esclarecer a dimensão conceitual de suas espécies e formas de manifestação, sendo suas espécies a culpa consciente e a culpa inconsciente enquanto as formas de manifestação se consumam com a imprudência, a negligência e a imperícia.

Segundo Assis Toledo (1994), a culpa consciente se compreende com a percepção plena do agente quanto à possibilidade da ocorrência do fato típico que, mesmo assim, realiza a conduta com a convicção que irá evitar a consumação do resultado do fato típico; ao passo que, na culpa inconsciente, o agente não possui qualquer vislumbre sobre os resultados típicos possíveis de sua conduta.

Quanto às formas de manifestação da culpabilidade, a imperícia é caracterizada como uma forma ativa de culpa, resultante de um comportamento destituído de cautela ou realizado com precipitação ou insensatez, assim infringindo o dever de cuidado objetivo (NUCCI, 2017).

Por sua vez, a negligência representa uma forma passiva de culpa cuja conduta passiva, inerte ou omissiva do agente, causada pelo seu descuido ou desatenção, infringe o dever de cuidado objetivo e que, por conseguinte, propicia evento danoso involuntário (NUCCI, 2017).

Finalmente, a imperícia se trata de uma forma de culpa que ocorre estritamente no campo técnico, uma vez que a conduta culposa decorre da insuficiência técnica do agente em realizar atividades características a determinada arte, ofício ou profissão (NUCCI, 2017).

Numa síntese conceitual precisa, Assis Toledo demonstra um exemplo possível de dinâmica entre as espécies de culpa e suas respectivas formas de manifestação, *in verbis*:

> Duas são as modalidades da culpa *stricto sensu*: a culpa consciente e a inconsciente. Na primeira, o agente prevê o resultado típico, tem-no como possível, mas confia em que poderá evitá-lo. Não quer o resultado, mas, por erro ou excesso de confiança (imprudência), por não empregar a diligência necessária (negligência) ou por não estar suficientemente preparado para um empreendimento cheio de riscos (imperícia), fracassa e vem a ocasioná-lo (v. exemplo na ação atribuída a Caio). Na segunda — a culpa inconsciente — o agente não prevê o resultado, comporta-se com desatenção, desleixo, descuido (negligência), afoiteza (imprudência), ou arrisca-se a práticas para as quais não está devidamente habilitado ou preparado (imperícia), transformando-se, assim, em causa cega do evento danoso (ASSIS TOLEDO, 1994, p.302).

Além disso, é imperioso ressaltar as diferenças conceituais pertinentes entre dolo eventual e culpa consciente, essenciais para o desenvolvimento da análise jurídica que será disposta no tópico 4.2 do presente trabalho.

De acordo com Nucci (2017), embora a distinção teórica entre tais institutos seja plausível, a aferição no caso concreto tende a ser complexa e difícil. Ademais, segundo o autor em comento, em ambas as circunstâncias, o agente possui a percepção do resultado provável de sua conduta, porém, na culpa consciente, o resultado típico não é admitido pelo agente, buscando, ainda, elidir sua concretização; no dolo eventual, o agente assume o risco do resultado típico, demonstrando-lhe indiferença quanto sua concretização.

Ainda, quanto à distinção teórica entre os institutos supracitados, Assis Toledo (1994, p. 302-303) assevera que "[...] na culpa consciente o agente não quer o resultado nem assume deliberadamente o risco de produzi-lo" enquanto que "No dolo eventual, o agente não só prevê o resultado danoso como também o aceita como uma das alternativas possíveis".

Face o exposto, verifica-se que a aferição do elemento volitivo possui papel preponderante na caracterização da tipicidade de determinada conduta delituosa, assim como tal exame permite estabelecer um parâmetro razoável para a elaboração dosimetria da pena, ensejando assim a aplicação de uma pena proporcional com a ofensa perpetrada pelo agente.

4.1.2.1.3.2.2 Antijuridicidade ou Ilicitude

Na visão de Pierangeli e Zaffaroni, sob o prisma do finalismo penal, a antijuridicidade pode ser compreendida a partir das premissas a seguir, *in verbis*:

> [...] é, pois, o choque da conduta com a ordem jurídica, entendida não só como uma ordem normativa (antinormatividade), mas como uma ordem normativa e de preceitos permissivos. O método, segundo o qual se comprova a presença da antijuridicidade, consiste na constatação de que a conduta típica (antinormativa) não está permitida por qualquer causa de justificação (preceito permissivo), em parte alguma da ordem jurídica (não somente no direito penal, mas tampouco no civil, comercial, administrativo, trabalhista, etc. (PIERANGELI; ZAFFARONI, 1997 *apud* NUCCI, 2017, p.521-522).

Em consonância com os autores supracitados, Pacelli e Callegari (2016) preconizam que conceito de ilicitude ou antijuridicidade possui uma relação estreita com o conceito de tipicidade. Ainda, segundo o autor em comento, embora tal premissa implique afirmar que a concretização de determinado fato típico também resulte na constatação da ilicitude desta, todavia, salvo a incidência de norma penal permissiva prevista pelo legislador, em regra, o sistema penal aborda condutas típicas com presunção de ilicitude.

Outrossim, Pacelli e Callegari (2016) ainda mencionam a relação entre as expressões antijuridicidade e injusto, sendo que a primeira representa a contradição da ação humana perante a determinada norma jurídica, enquanto que a segunda se refere à mesma ação valorada antijuridicamente, ou seja, a antijuridicidade representa o gênero ao passo que o injusto é uma espécie de antijuridicidade determinada pertencente ao referido gênero.

Em virtude disso, o ordenamento jurídico brasileiro possui previsões de tipos penais permissivos que, por sua vez, constituem hipóteses de excludente de ilicitude, a

citar o estado de necessidade, a legítima defesa, bem como nas ocasiões em que se verifica o estrito cumprimento do dever legal[36].

Por fim, cumpre frisar que a doutrina abalizada estabelece a diferenciação entre antijuridicidade formal e antijuridicidade material, sendo que a primeira forma decorre da simples contrariedade da conduta humana em relação à ordem jurídica, ao passo de que a segunda forma se extrai a partir da constatação efetiva que determinado bem jurídico tutelado pela ordem jurídica fora exposto à lesão ou perigo de lesão.

4.1.2.1.3.2.3 Culpabilidade

De acordo com Nucci (2017), a culpabilidade abrange o juízo de reprovação social oposto ao autor e ao fato considerado típico e ilícito pela ordem jurídica, sendo que tal aferição deverá ser realizada através da verificação da imputabilidade do agente, contrastada com a ciência do respectivo agente quanto o potencial de ilicitude de sua conduta, observada a possibilidade exigibilidade do referido agente em agir de forma diversa.

Nessa esteira, sob o prisma da teoria finalista da ação, ASSIS TOLEDO assevera as seguintes dimensões conceituais sobre instituto jurídico em questão, *in verbis:*

> [...] se indagarmos aos inúmeros seguidores da corrente finalista o que é a culpabilidade e onde pode ela ser encontrada, receberemos esta resposta: 1.ª) culpabilidade é, sem dúvida, um juízo valorativo, um juízo de censura que se faz ao autor de um fato criminoso; 2.ª) esse juízo só pode estar na cabeça de quem julga, mas tem por objeto o agente do crime e sua ação criminosa. (ASSIS TOLEDO, 1994, p.229-230).

Quanto aos elementos constituintes da culpabilidade, a doutrina abalizada concebe a existência dos seguintes elementos: a) imputabilidade; b) potencial consciência da ilicitude do fato; e c) inexigibilidade de conduta diversa.

A imputabilidade, segundo Pacelli e Callegari (2016, p.251), é caracterizada quando o agente "[...] no momento do fato, seja capaz de obrar responsavelmente, ou seja, compreender que o fato não está autorizado e determinar-se de acordo com esta compreensão, é dizer, abster-se da realização do fato". Tal premissa conceitual se

[36] **Exclusão de ilicitude**
Art. 23 - Não há crime quando o agente pratica o fato:
I - em estado de necessidade;
II - em legítima defesa;
III - em estrito cumprimento de dever legal ou no exercício regular de direito. (BRASIL,1940)

encontra positivada no disposto do art. 26, *caput,* do Código Penal[37]. Em linhas gerais, a doutrina abalizada entende como causas de exclusão de imputabilidade contempladas pelo Direito Penal brasileiro: a) doença mental; b) desenvolvimento mental incompleto ou retardado; c) menoridade e; d) embriaguez acidental completa resultante de caso fortuito ou força maior.

No tocante ao potencial de consciência de ilicitude do fato, a doutrina consolidou dois institutos que abrangem as possibilidades acerca da ignorância do agente quanto à ilicitude de suas ações: erro de tipo e erro de proibição. Nesse mérito, PACELLI e CALLEGARI ilustram precisamente os referidos institutos, *in verbis:*

> No erro de proibição, o autor sabe o que faz tipicamente, mas supõe erroneamente que está permitido. O erro de proibição recai sobre a consciência da ilicitude do fato, visto que o agente faz um juízo equivocado daquilo que lhe é permitido fazer, ou seja, supõe, erroneamente, que sua conduta não é contrária ao direito. O agente não erra sobre os elementos fundamentais de composição da figura delitiva (erro de tipo), mas a respeito da relação intercorrente entre o seu comportamento e a ordem jurídica na sua globalidade. Cuida-se, portanto, da crença positiva do agente de que sua conduta está autorizada, é permitida, é conforme ao ordenamento (PACELLI; CALLEGARI, 2016, p.255).

Conforme sedimentado no ordenamento jurídico brasileiro, bem como na doutrina e jurisprudência pátria, ressalvada a invencibilidade do erro de proibição, todas as demais hipóteses de erro são culpáveis e, portanto, passíveis de aplicação de sanção penal.

No que concerne à inexigibilidade de conduta diversa, conforme as lições de Pacelli e Callegari (2016), tal juízo de culpabilidade poderá ser oposto ao autor de fato típico se, nas circunstâncias concretas em que cometera o delito, existia a possibilidade de exercer uma conduta distinta e, consequentemente, atípica. Nesse aspecto, o ordenamento jurídico pátrio prevê duas hipóteses de exclusão de exigibilidade de conduta diversa: coação moral irresistível e a obediência hierárquica[38].

---

[37] **Inimputáveis**
Art. 26 - É isento de pena o agente que, por doença mental ou desenvolvimento mental incompleto ou retardado, era, ao tempo da ação ou da omissão, inteiramente incapaz de entender o caráter ilícito do fato ou de determinar-se de acordo com esse entendimento (BRASIL,1940).

[38] **Coação irresistível e obediência hierárquica**
Art. 22 - Se o fato é cometido sob coação irresistível ou em estrita obediência a ordem, não manifestamente ilegal, de superior hierárquico, só é punível o autor da coação ou da ordem (BRASIL,1940).

Em suma, se não preenchidos os elementos acima explanados, a conduta típica e ilícita será considerada culpável e, portanto, passível de sanção conforme a gravidade da lesão ou perigo de lesão cometido ao respectivo bem jurídico.

4.1.2.2 O Sistema Penal Finalista

4.1.2.2.1 Origens e Fundamentos Filosóficos

Em sua abordagem conceitual sobre o sistema penal em análise, Bitencourt apresenta a síntese, proposta por Andrei Schmidt, sobre os fundamentos da doutrina finalista, idealizada por Hans Welzel:

> Welzel desenvolveu sua doutrina finalista (entre 1930 e 1960) baseado no método fenomenológico de investigação, sustentando a formulação de um conceito pré-jurídico de pressupostos materiais (dentre os quais a conduta humana) existentes antes da valoração humana e, por isso, precedentes a qualquer valoração jurídica: para contrapor-se ao subjetivismo epistemológico do neokantismo, afirmava Welzel que não é o homem, com a colaboração de suas categorias mentais, quem determina a ordem do real, mas sim o próprio homem que se encontra inserido numa ordem real correspondente a estruturas lógico-objetivas (não subjetivas) (SCHMIDT, 2007 *apud* BITENCOURT, 2012, p.101).

Sendo assim, como aponta Pacelli e Callegari (2016), o finalismo penal tem como base filosófica o emprego de teorias ontológico-fenomenológicas, cujo propósito consiste evidenciar determinadas leis estruturais do ser humano, bem como abrangê-las enquanto premissas maiores de ciências que possuem o homem como objeto de estudo.

Finalmente, Pacelli e Callegari (2016, p.171) sustentam que a lógica que lastreia os fundamentos filosóficos da doutrina finalistas consistem em "[...] colocar um conceito básico e pré-jurídico como o da ação humana no centro da Teoria Geral do Delito e construir a partir da constituição ontológica da ação um sistema, que venha previamente dado ao legislador de estruturas lógico-objetivas".

4.1.2.2.2 Teoria Finalista da Ação

A doutrina finalista parte da premissa, segundo Hans Welzel, que "a ação humana é exercício de atividade final" (WELZEL, 1997 *apud* NUCCI, 2017, p.364). Ou seja, a ação humana sempre estará orientada de forma ontológica, essencial e fundamental à consecução de um propósito, cuja natureza pode ser criminosa ou não (NUCCI, 2017).

Ademais, com a adoção de tais premissas conceituais, o finalismo penal inaugurou a concepção de que os aspectos subjetivos do crime, dolo e culpa, estão vinculados diretamente ao elemento volitivo intrínseco a conduta criminosa perpetrada, ou seja, a qualificação da vontade influencia decisivamente na aferição da tipicidade penal perpetrada pelo agente (NUCCI, 2017). Portanto, o dolo e a culpa são aspectos essenciais para qualificar a dimensão da tipicidade da conduta perpetrada pelo agente da ação criminosa.

Sendo assim, a inovação conceitual de WELZEL consiste na retirada do dolo e da culpa, enquanto aspectos subjetivos do crime que tradicionalmente integravam o elemento da culpabilidade no sistema penal neoclássico, e os readequou como aspectos subjetivos inerentes a aferição da tipicidade da conduta criminosa (NUCCI, 2017). Portanto, no tocante à doutrina finalista, pode-se aferir que a tipicidade deixou de ter uma dimensão meramente objetiva, ao passo de que a culpabilidade adquiriu dimensões eminentemente normativas.

Ainda, a proposição conceitual de Welzel buscou demonstrar a existência do *dolo natural* na conduta criminosa. Em outras palavras, isso implica afirmar que o agente pode deter a vontade de realizar condutas descritas em determinado tipo penal, contudo, tal circunstância não necessariamente repercutirá na consciência deste quanto à ilicitude de seus atos (NUCCI, 2017).

De outra banda, Pacelli e Callegari descrevem a ação finalística e suas respectivas etapas:

> 1ª etapa: Subjetiva – ocorre totalmente na esfera do pensamento, subdividindo-se em três fases: (a) adiantamento da meta (objetivo pretendido pelo autor); (b) eleição dos meios precisos para alcançar o fim; (c) consideração dos efeitos concomitantes (relação do fator causal elegido como meio e o fim a ser alcançado).
>
> 2ª etapa: Objetiva – ocorre no mundo real. O autor inicia a execução da ação de acordo com a antecipação do fim, a eleição do meio e a consideração dos efeitos concomitantes. É um processo causal posto na realidade, predeterminado pelas definições de fins e meios na esfera do pensamento. Se não se alcançar o fim, o resultado predeterminado no mundo real, a ação considera-se apenas tentada. (PACELLI; CALLEGARI, 2016, p.171)

Em contrapartida, como qualquer teoria científica, o finalismo foi alvo de críticas de representantes de outras linhas doutrinárias, sendo estas as mais comuns: a) quanto aos crimes culposos, quando o resultado é eminentemente causal, independentes

à vontade do agente, a violação do dever de cuidado consistiria numa circunstância não abrangida por uma finalidade relevante ao agente; e b) quanto aos crimes omissivos, quando a conduta do agente não puder ensejar causa para nenhum resultado e, por conseguinte, uma ação sem caráter finalístico (PACELLI; CALLEGARI, 2016).

Por sua vez, sem o propósito de esgotar o debate, Nucci defende sua contrariedade sobre determinados aspectos apresentados nas críticas supracitadas:

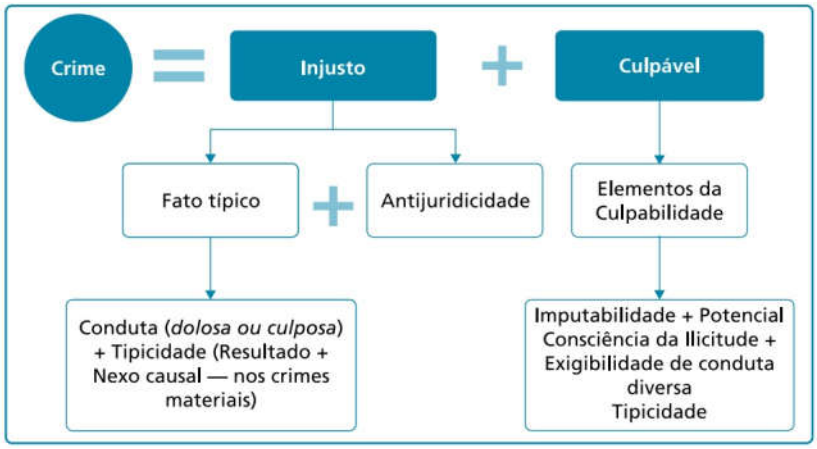
> Por certo, os causalistas, de ambas as fases, criticaram o finalismo – e até hoje o fazem. Um dos pontos fracos da teoria concentra-se na culpa, cujo resultado danoso é involuntário, ou seja, independe da vontade do agente. Contudo, isso não significa que a conduta humana não teve uma finalidade; teve um objetivo, embora possa ser penalmente irrelevante. Lembre-se que o resultado, no crime culposo, chamado também de crime de azar, acontece sem o querer do agente.
>
> Ilustrando, o agente pode dar tiros num alvo colocado numa árvore; a sua finalidade é acertá-lo (pode ser crime à parte ou não); de maneira imprudente, não percebe a possibilidade de acertar seu vizinho, cujo imóvel confronta com o seu; uma bala desvia-se do alvo e fere o vizinho. Extrai-se o seguinte quadro: o agente desferiu um tiro com a finalidade de acertar o alvo; a sua manifesta imprudência não o fez ver, embora pudesse, a eventualidade de um resultado danoso (atingir alguém). A culpa está presente, assim como a finalidade do agente, na conduta praticada.
>
> Em momento algum, defende-se que toda finalidade, nas condutas humanas, é ilícita e criminosa. Por isso, também na culpa o finalismo aplica-se com perfeição.
>
> Os críticos ainda levantam algumas questões particulares, como a atuação do agente na culpa inconsciente, bem como nas ações de ímpeto. Haveria finalidade? Embora de difícil detecção, sem dúvida. Valendo ainda o exemplo do atirador, ele pode se encontrar num estande de tiro, desferindo disparos contra um alvo e não perceber a entrada, na área de tiro, de uma pessoa. Por culpa inconsciente, termina por atingi-la. A sua finalidade não se desvirtua, que é desfechar tiros ao alvo. O mesmo aplica-se nas condutas de ímpeto: a finalidade do agente é instantânea e rápida o suficiente para permanecer fora do alcance visual do terceiro observador. Isso não significa que o agente tenha atuado sem finalidade alguma. (NUCCI, 2017, p. 364-365).

Apesar da retirada do dolo e da culpa da culpabilidade aparentar uma espécie de esvaziamento do respectivo elemento do crime, ressalta-se que tal readequação conceitual apenas retirou o traço psicológico do crime da culpabilidade. Assim, a culpabilidade se ocuparia a tratar sobre questões estritamente normativas. Tal inovação conceitual na composição dos elementos do crime é denominada como Teoria

Normativa Pura da Culpabilidade, cuja concepção psicológico-normativa veio contrapor à visão da corrente doutrinária *causalista-neokantiana* (BITENCOURT, 2012).

Finalmente, a figura a seguir ilustra a estrutura do crime sob a ótica do finalismo penal:

FIGURA 5 – Representação esquemática da estrutura analítica de crime sob o escopo finalista.



Fonte: Direito Penal Esquematizado – Parte Geral, 2016, p.315.

A seguir, serão analisadas as possibilidades de enquadramento das condutas descritas no estudo da RWTH Aachen University, bem como as respectivas descobertas obtidas no respectivo estudo, em relação aos tipos penais previstos na legislação penal pátria vigente.

4.1.3 Limites da dimensão do entendimento doutrinário e jurisprudencial quanto à abrangência do tipo penal

Nesta seção, para a consecução dos fins supracitados, serão utilizados os grupos conceituais descritos no estudo da RWTH Aachen University, apresentados no capítulo 2 do presente trabalho, como metodologia de abordagem conceitual quanto o potencial de tipicidade que a mera posse incidental dos arquivos digitais, descobertos e catalogados nos respectivos grupos conceituais, representa na legislação penal vigente no país.

Inicialmente, cabe recapitular que o presente trabalho tem como objetivo analisar os limites da criminalização de usuários mineradores do Bitcoin, cujas circunstâncias de imputação penal são resultantes posse ilícita incidental de arquivos

digitais de conteúdo não financeiros, inseridos no *blockchain* por outros usuários da referida criptomoeda.

Como descrito no capítulo 3, todo usuário da rede Bitcoin que exerce funções de mineração no sistema de pagamentos possui uma cópia local completa do *blockchain* desta moeda.

Portanto, a circunstância com potencial típico que será analisada nesta seção e nas seguintes consiste na representação do usuário que se dedica exclusivamente as atividades de mineração da criptomoeda e que, por sua vez, possui a cópia local do *blockchain* do Bitcoin com os dados descritos no estudo da RWTH Aachen University, sem realizar qualquer interação direta com tais arquivos digitais inseridos desta estrutura.

Sendo assim, cumpre frisar que a análise da tipicidade do grupo conceitual "*Malware*" não possui nenhuma serventia com o objeto do presente trabalho, uma vez que a posse incidental de um *malware* transformaria seu possuidor, potencialmente, em vítima de um injusto penal e não o oposto. Logo, a análise do potencial de tipicidade deste grupo não será empreendida no presente trabalho ante a irrelevância de tal intento.

Dito isso, quanto ao grupo conceitual "Violações de Direitos Autorais", verifica-se que a legislação penal brasileira prevê conduta típica cominada no art. 184 do Código Penal, *in verbis:*

> **Violação de direito autoral**
>
> Art. 184. Violar direitos de autor e os que lhe são conexos:
>
> Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.
>
> § 1º Se a violação consistir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente:
>
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
>
> § 2º Na mesma pena do § 1º incorre quem, com o intuito de lucro direto ou indireto, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante ou do direito do produtor de fonograma, ou, ainda, aluga

> original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente.
>
> § 3º Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente:
>
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
>
> § 4º O disposto nos §§ 1º, 2º e 3º não se aplica quando se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei nº 9.610, de 19 de fevereiro de 1998, nem a cópia de obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto (BRASIL, 1940).

Por se tratar de uma norma penal em branco homogênea[39], o conteúdo do dispositivo acima exposto deve ser complementado com as disposições das Leis nºs 9.609/1998 e 9.610/1998. De acordo com Masson (2014), o tipo penal do art. 184 do Código Penal descreve um crime de natureza comum, formal, doloso, de forma livre, plurissubsistente e instantâneo. Além disso, de acordo com autor em comento, o referido dispositivo se trata de um crime de elevado potencial ofensivo, que tutela bens móveis e admite tentativa.

Com efeito, afere-se que o tipo penal acima exposto admite apenas o dolo enquanto elemento subjetivo do tipo, bem como o único núcleo descrito pelo tipo penal – violar – abrange quaisquer transgressões dos direitos autorais positivados nas leis nºs 9.609/1998 e 9.610/1998. Em análise a ambos os diplomas legais, não há qualquer menção expressa sobre a violação de direitos autorais resultantes da mera posse incidental da obra por terceiros, desde que tal ato não constranja o proprietário de direitos autorais de utilizar, fruir e dispor de sua obra.

Ainda, tal constrangimento precisa ser doloso para ser um fato típico, ou seja, o agente precisa direcionar suas ações ou, ao mesmo, assumir o risco de suas condutas que venham ofender direitos autorais alheios. Portanto, para que a posse de direitos autorais de terceiros se caracterize como fato típico, necessita-se a presença do elemento

[39] Lei penal cuja descrição do preceito primário é complementada por outro diploma legal (MASSON, 2014).

volitivo doloso cuja direção finalística venha a ofender, violar ou infringir direitos autorais positivados nas leis nºs 9.609/1998 e 9.610/1998.

Por sua vez, ambos os grupos conceituais, "Conteúdo Politicamente Sensível" e "Violações de Privacidade", compartilham do mesmo dispositivo penal para tipificar as condutas resultantes da posse dos arquivos digitais catalogados nos respectivos grupos, *in verbis*:

> **Divulgação de segredo**
>
> Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:
>
> Pena - detenção, de um a seis meses, ou multa.
>
> § 1º Somente se procede mediante representação
>
> § 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:
>
> Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.
>
> § 2º Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada (BRASIL, 1940).

Consoante as lições de Masson (2014), o tipo penal cominado no art. 153 do Código Penal descreve um crime próprio, doloso, formal, de resultado cortado ou de consumação antecipada, de forma livre, unissubsistente ou plurissubsistente, instantâneo e unilateral. Ademais, conforme mencionado pelo autor em comento, tal tipo penal possui fulcro na garantia constitucional quanto à inviolabilidade da intimidade ou da vida privada, consubstanciada no art. 5º, inciso X, da *Carta Magna*[40], ao passo que não admite forma culposa e admite tentativa.

Nesse sentido, é imperioso frisar a importância do elemento normativo do tipo penal "sem justa causa", bem como o núcleo do tipo penal "divulgar". De acordo com Damásio (2014), a existência da justa causa da divulgação do conteúdo particular ou sigiloso enseja sua atipicidade, enquanto que o núcleo do tipo "divulgar" deve ser

[40] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
(...) X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

compreendido como um processo de narração sucessivo, empreendido pelo agente, sobre determinada informação a um número indeterminado de pessoas.

Ademais, como asseverado por Masson (2014, p.824), quanto ao elemento normativo "sem justa causa", "[…] é necessário conheça o agente o caráter confidencial da informação divulgada, a ilegitimidade da sua conduta e a possibilidade de produzir dano a outrem".

Ante tais premissas, somado ao fato que tal tipo penal não prevê forma culposa, é possível constatar que a mera posse de arquivos digitais, cujo conteúdo represente informações sensíveis ao poder governamental[41] ou detenha informações particulares de terceiros, se ausentes o dolo e a violação da conduta descrita no núcleo do tipo penal (divulgar) do art. 153, do Código Penal, a imputação criminal se torna incabível.

Quanto ao último grupo conceitual, "Conteúdo Ilegal e Condenado", conforme mencionado pelos autores do estudo da RWTH Aachen University, tal grupo possui as descobertas mais preocupantes aos usuários do Bitcoin e de criptomoedas em geral, haja vista o caráter universal do punitivismo penal rigoroso quanto à prática de exploração de pornografia infantil dentre as nações.

De acordo com o teor das descobertas do referido grupo, pode-se verificar que a legislação penal pátria prevê, especificamente no Estatuto da Criança e Adolescente – ECA (Lei nº 8.069/1990), como condutas típicas a divulgação de pornografia infantojuvenil (art. 241-A, *caput*), o asseguramento de meios ou serviços para sua divulgação (art. 241-A, §2º, incisos I e II), bem com a aquisição, posse ou armazenamento de material pornográfico infantojuvenil (art. 241-B), *in verbis*:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
>
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
>
> § 1º Nas mesmas penas incorre quem:

[41] Embora exista norma penal específica vigente para tutelar os objetivos da segurança nacional (Lei nº 7.170/1983 – Lei de Segurança Nacional), dado o teor excessivamente punitivista, bem como o provável desuso ou inadequação deste diploma legal com a ordem constitucional vigente, preferiu-se não proceder com a análise de aplicabilidade de tal texto legal quanto ao mérito descrito nesta seção do presente trabalho.

> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
>
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
>
> § 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.
>
> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
>
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
>
> § 1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.
>
> § 2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:
>
> I – agente público no exercício de suas funções;
>
> II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;
>
> III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário. (BRASIL, 1990)

No que se refere ao art. 241-A, cumpre frisar a importância doutrinária do conceito doutrinário dos núcleos do tipo – "disponibilizar" e "divulgar" – em relação ao objeto do presente trabalho. Conforme preleciona Ângelo Roberto Ilha da Silva (2017), o núcleo "disponibilizar" descreve as circunstâncias de hospedagem e compartilhamento de arquivos em redes P2P (*peer-to-peer*) cujo agente disponibiliza arquivos com conteúdo pornográfico infantil para terceiros realizarem copias (*downloads)*; ao passo que o núcleo "divulgar" consiste na difusão do material pornográfico, sem propiciar o acesso direto deste, por meio de links que direcionem o usuário para outros locais na *web*.

Além disso, quanto ao §1º, incisos I e II, do art. 241-A tipificam a conduta de assegurar meios ou serviços para divulgação de material pornográfico infantil, quanto à pertinência ao objeto do presente trabalho, o inciso I possui considerável relevância.

Nesse sentido, de acordo com Silva (2017, p.97), o referido inciso ilustra "Na hipótese, comete o delito quem garante os meios ou serviços, diversamente daquele que produz o faz circular o material pornográfico". Tais *meios*, segundo Baltazar Júnior, pode ser caracterizados como "[...] físicos, como suportes em papel, celulose, vídeo, discos compactos, DVDs, discos rígidos ou outros armazenadores de meios eletrônicos e arquivos, bem como a prestação dos serviços para o referido armazenamento" (BALTAZAR JÚNIOR, 2014 *apud* SILVA, 2017, p.97).

Em linhas gerais, como explica Silva (2017), a conduta cominada no art. 241-A do ECA caracteriza um crime doloso, permanente (nas hipóteses de disponibilização de material pornográfico) ou instantâneo (na maioria dos casos), de perigo abstrato, cujo tipo é misto alternativo (pune-se o sujeito apenas por um delito constante no tipo penal) e a tentativa como admissível.

De outra banda, no tocante ao disposto no art. 241-B do ECA, o núcleo do tipo penal – "possuir" – possui grande relevância ao objeto do presente trabalho. Consoante as lições de Silva (2017), compreende-se o verbo "possuir" como deter o domínio ou poder sobre determinada coisa. Com efeito, o autor em comento descreve o tipo penal cominado no art. 241-B do ECA como um crime doloso (sem previsão de elemento subjetivo especial), de, perigo abstrato, instantâneo (na hipótese de adquirir) ou permanente (nas hipóteses de possuir ou armazenar), cujo objeto material está consonância ao descrito aos artigos anteriores do respectivo diploma legal.

Por sua vez, o §2º do artigo supracitado prevê hipótese de minoração da pena do agente cujo vulto do resultado típico influenciará positivamente na dosimetria da pena. Finalmente, cumpre frisar que ambos os tipos penais supracitados não admitem a forma culposa.

Quanto à jurisprudência pátria em relação ao tema previamente exposto, em contraste com o escopo tratado no presente trabalho, o julgado colacionado[42] a seguir

[42] A pesquisa jurisprudencial realizada neste trabalho obteve 263 ocorrências de julgados, dentre todos os tribunais regionais federais do país, relacionados aos crimes cominados nos arts. 241-A e 241-B do ECA. Portanto, dada a convergência dos tribunais federais quanto à abordagem conceitual e jurídica desses ilícitos penais, preferiu-se apresentar o julgado mais analítico dentre os demais que foram obtidos nas amostras da referida pesquisa.

expõe, com grande abrangência, sobre como é abordada tal questão criminal nos tribunais federais brasileiros[43], *in verbis*:

> **EMENTA:** DIREITO PENAL E PROCESSUAL. ARTIGOS 241-A E 241-B DO ESTATUTO DA CRIANÇA E DO ADOLESCENTE. OPERAÇÃO DIRTYNET. COMPARTILHAMENTO E ARMAZENAMENTO INTERNET DE FOTOS E VÍDEOS PORNOGRÁFICOS ENVOLVENDO CRIANÇAS E ADOLESCENTES PELO PROGRAMA GIGATRIBE COM RESULTADO DENTRO E FORA DO TERRITÓRIO BRASILEIRO. TRANSNACIONALIDADE. COMPETÊNCIA DA JUSTIÇA FEDERAL NO CASO CONCRETO. INÉPCIA DA DENÚNCIA E ILEGITIMIDADE PASSIVA. NÃO OCORRÊNCIA. TESES PRELIMINARES AFASTADAS. MÉRITO. MATERIALIDADE, AUTORIA E DOLO COMPROVADOS. ERRO SOBRE ILICITUDE DO FATO. CONDENAÇÃO MANTIDA. ARMAZENAMENTO E DIVULGAÇÃO EM MOMENTOS DISTINTOS. CONDUTAS AUTÔNOMAS. CONCURSO MATERIAL. OCORRÊNCIA. DOSIMETRIA. CIRCUNSTÂNCIAS JUDICIAIS. PENA-BASE E QUANTIDADE DE DIAS-MULTA DO CRIME DO ART. 241-A DO ECA. ADEQUAÇÃO. PRESCRIÇÃO DA PENA RELATIVA AO DELITO DO ART. 241-B DA LEI 8.069/90. APLICAÇÃO DO DISPOSTO NO ART. 115 COMBINADO COM ART. 109, VI DO CP. ADEQUAÇÃO. SANÇÕES ALTERNATIVAS. EXECUÇÃO PROVISÓRIA DA PENA. ESGOTAMENTO DA JURISDIÇÃO ORDINÁRIA DA CORTE DE APELAÇÃO. POSSIBILIDADE. PRECEDENTE STF COM REPERCUSSÃO GERAL. SÚMULA 122 TRF4. COMUNICAÇÃO AO JUÍZO DE ORIGEM. 1. Trata-se de crimes cuja previsão resulta das orientações traçadas em acordos e tratados internacionais - dos quais o Brasil é signatário - visando a combater a pedofilia via internet. A incorporação da Convenção da ONU sobre pornografia infantil no Direito Pátrio deu-se mediante o Decreto legislativo 28/90 com promulgação pelo Decreto Presidencial nº 99.710/90. 2. No caso, a ação penal que originou-se da operação policial em território pátrio que decorreu das investigações realizadas na chamada Operação DirtyNet, desenvolvida no final do ano de 2011 e no decorrer de 2012. Segundo apurado, as ações criminosas de compartilhamento entre usuários estrangeiros e brasileiros de material envolvendo cenas de pornografia infantil e de conteúdo pedófilo na rede mundial de computadores, por meio do software Gigatribe (programa fechado de rede social), cuja comunicação eletrônica é disponibilizada para qualquer indivíduo, dentro e fora do Brasil, restando, por conseguinte, evidenciada a prova da internacionalidade, a atrair a competência da Justiça Federal. 3. Logo, as teses defensivas de que o material obtido ilicitamente não ultrapassou as fronteiras nacionais e que não existia potencialidade de acesso por alienígenas, pois os contatos do réu pelo Gigatribe não vão além do território nacional não comporta acolhimento para infirmar a competência da Justiça Federal. Isso porque o programa Gigatribe permite a comunicação eletrônica entre os usuários e o compartilhamento de arquivos de fotos e

[43] Dado o caráter de internacionalidade do Bitcoin, bem como sua estrutura de dados (*blockchain)* e conteúdos potencialmente ilícitos inseridos nesta estrutura*,* no caso em tela, presumiu-se a competência da Justiça Federal para tratar do tema conforme pacificado pelo STF na Repercussão Geral tratada no RE 628.624/MG. Portanto, apenas a jurisprudência oriunda dos tribunais regionais federais foi abordada no presente trabalho.

vídeos envolvendo pornografia infantojuvenil em qualquer lugar em que esteja o usuário, quer no território pátrio ou no estrangeiro. 4. Tema pacificado pelo STF em Repercussão Geral. no RE 628.624/MG. 5. Tendo os fatos criminosos imputados ao acusado (armazenamento e compartilhamento de material com conteúdo de pornografia envolvendo crianças e adolescentes) sido descritos de forma clara e precisa, apresentando ainda elementos comprobatórios de materialidade e autoria, com o que restou garantido o pleno conhecimento do fato e o exercício absoluto da ampla defesa e do contraditório, não há falar em inépcia da denúncia. 6. Exsurge dos autos que o acusado travava diálogos com outros usuários e compartilhava pelo aplicativo Gigatribe, arquivos contendo imagens (fotos e vídeos) de crianças e adolescentes em cenas de sexo explícito e pornográfico, resta configurada a prática da conduta descrita no art. 241-A da Lei 8.069/90. 7. Da mesma forma, comprovado o armazenamento de imagens (vídeos e fotos) contendo cenas de sexo explícito envolvendo crianças e adolescentes em pastas do próprio programa fechado de relacionamento social, bem como em outras mídias digitais e aparelhos fotográficos, resulta perfectibilizada a conduta ilícita prevista no artigo 241-B do ECA. 8. No que tange ao aventado erro sobre a ilicitude do fato (erro de proibição), a simples alegação de desconhecimento do fato de que compartilhar e armazenar vídeos e fotografias de sexo explícito e pornografia envolvendo crianças e adolescentes se tratassem de condutas ilícitas não exime o apelante de sua responsabilidade criminal. 9. Somente incorre na excludente de culpabilidade do erro de proibição aquele que não possui condições de conhecer e entender o caráter ilícito de sua conduta, o que, certamente, não é o caso do recorrente que possui experiência na área de informática e de navegação na internet, e que conhecia o funcionamento do aplicativo Gigatribe. Além disso, o réu, à época dos fatos, contava com diversos meios de comunicação ao seu dispor, tendo plenas condições de conhecer a lei e, consequentemente, a ilegalidade de seu ato. 10. Destarte, o réu tinha plena consciência de que os materiais por ele salvos e armazenados em seu computador estavam sendo disponibilizados a terceiros pela internet, o que s.m.j. afasta a tese defensiva de erro sobre a ilicitude do fato. 11. Em alguns casos pode não só ocorrer concurso formal de crimes como também absorção da conduta inscrita no art. 241-B do ECA (Lei 8.069/90) - nas modalidades adquirir, possuir e armazenar - por aquela prevista no art. 241-A do mesmo estatuto (disponibilizar, transmitir, divulgar, trocar, publicar). Todavia, para tanto, é necessário que se comprove que o agente, de alguma forma, já possui ou tem guardados arquivos contendo imagens pornográficas (fotos e vídeos) envolvendo crianças e adolescente em locais específicos do computador (pastas), em email próprio utilizado ou mesmo, em pastas e arquivos próprios dos mais diversos programas de compartilhamento encontrados na internet, cuja disponibilização, divulgação e transmissão desses mesmos conteúdos armazenados são franqueadas diretamente pelo usuário, ou é automático e imediato a partir do momento em que é acessada a rede mundial de computadores e aludidos programas. 12. De outro lado, quando o agente, de alguma forma, adquire ou baixa arquivos contendo imagens pornográficas (fotos e vídeos) envolvendo crianças e adolescente e os guarda em outras mídias de armazenamento (cd's, pen drives, dvd's, emails), no próprio HD, ou ainda, em pastas distintas daquelas do programa utilizado para compartilhamento, é perfeitamente possível o concurso material das condutas "possuir" e "armazenar" (art. 241-B do ECA) com as condutas "publicar" ou "disponibilizar" e "transmitir" (art. 241-A). 13. Além disso, o crime de armazenamento é permanente, ou seja, a

> potencialidade lesiva não se encerra com a transmissão, divulgação e publicação (condutas do art. 241-A do ECA). 14. No caso, mostra-se incabível a aplicação do concurso da consunção, tampouco do concurso formal de crime previsto no art. 70 do Código Penal, porquanto, restou comprovado que o acusado - com mais de uma ação e em momentos distintos -, não só disponibilizou arquivos de pedofilia infantil através do programa Gigatribe, como também armazenou material com essa temática em um CD encontrado em sua residência, ensejando, portanto, o reconhecimento da regra do art. 69, CP, como realizado na sentença.[...] (TRF4, ACR 5005920-33.2015.4.04.7100, SÉTIMA TURMA, Relatora SALISE MONTEIRO SANCHOTENE, juntado aos autos em 21/02/2018); **[grifo do autor]**

Por fim, como mencionado no julgado acima colacionado, o concurso formal entre as condutas tipificadas nos arts. 241-A e 241-B do ECA pode ensejar a aplicabilidade do princípio da consunção entre os respectivos tipos penais, bem como o concurso material entre as condutas tipificadas entre os referidos dispositivos; contudo, o contexto fático-probatório deve demonstrar a possibilidade de tais abordagens jurídicas.

Em suma, embora a mera posse de conteúdos pornográficos com natureza infantojuvenil enseja a tipicidade formal consubstanciada nos arts. 241-A e 241-B do ECA, para que realmente a tipicidade material consubstanciada nos respectivos dispositivos legais, necessita-se aferir o elemento subjetivo ou volitivo do tipo penal fora preenchido, ou seja, se a vontade empregada na direção finalística pelo agente é dolosa.

A seguir, será realizado o silogismo entre as premissas fático-técnicas e jurídicas apresentadas, até o presente momento, ao longo deste trabalho.

4.2 A APLICABILIDADE DAS PREMISSAS DOUTRINÁRIAS E PRECEDENTES JURISPRUDENCIAIS PERANTE OS RESULTADOS OBTIDOS NO ESTUDO DA RWTH AACHEN UNIVERSITY

Inicialmente, é importante salientar a relevância das questões fáticas e técnicas que motivaram a elaboração do presente trabalho. As criptomoedas, tendo o Bitcoin como a moeda genitora e maior expoente deste gênero tecnológico, representam uma

nova forma de anomia social e, consequentemente, jurídica para diversas nações do mundo, inclusive o Brasil[44].

Como aduzido ao longo dos capítulos 2 e 3, as criptomoedas, especialmente o Bitcoin, podem ser vistas com diversas ressalvas. No sentido ideológico, o Bitcoin foi criado com influência de ideais libertários, no sentido de retirar a regulação do poder econômico das instituições bancárias tradicionais e propiciar que os próprios agentes econômicos venham a se autotutelar no mercado.

Por sua vez, a implementação técnica do Bitcoin obteve, em certa medida, tais resultados, visto que atualmente as trocas econômicas por bens tangíveis, mediante o emprego de criptomoedas, independem de um intermediário financeiro para gerar credibilidade e consenso nas transações financeiras realizadas por esta modalidade de sistema de pagamentos.

O Bitcoin teve o mérito de inaugurar um sistema de pagamentos cuja credibilidade é construída pelos seus próprios usuários, mediante o emprego da criptografia para garantir das transações financeiras, bem como a inviolabilidade dos registros das transações financeiras já realizadas no respectivo sistema. Tal conceito seria denominado de consenso descentralizado, uma vez que as transações financeiras seriam verificadas e validadas por outros usuários da rede, contrariando assim a concepção tradicional de um agente econômico central com monopólio na regulação das trocas econômicas.

Ademais, essa criptomoeda inaugurou a possibilidade do anonimato pleno dentro do sistema de pagamentos, cuja valoração e emissão de sua moeda são reguladas pela própria comunidade de usuários que a utilizam. Inexoravelmente, o Bitcoin teve sucesso ao inaugurar uma ordem econômica alternativa ao mundo, que transcende fronteiras nacionais. Infelizmente, durante a história do Bitcoin, os potenciais da criptomoeda foram utilizados ostensivamente em transações financeiras com finalidades criminosas como aquisição de entorpecentes, crimes cibernéticos em geral, furto de

[44] Atualmente, há diversas nações que estão banindo o uso de criptomoedas ou, ao menos, impondo restrições significativas para seu uso. Disponível em: <https://www.ccn.com/top-10-countries-bitcoin-banned/>. Acesso em: 18/06/2018.

informações pessoais sensíveis, serviços de assassinato por encomenda, pornografia ilegal, dentre outros (FOLEY *et al*. ,2018).

Nesse mérito, de acordo com o estudo "*Sex, Drugs, and bicoin: How much illegal activity is financed through cryptocurrencies*?", desenvolvido pela Universidade de Tecnologia de Sydney, Austrália, apurou-se que pelo menos ¼ dos usuários da rede Bitcoin, bem como a metade das transações realizadas com a criptomoeda são associadas a atividades com finalidades ilegais, sendo o montante anual de tais transações avaliada em 72 bilhões de dólares (FOLEY *et al*. ,2018).

Em virtude dessas premissas, incontestavelmente, as criptomoedas, especialmente o Bitcoin, possuem diversas circunstâncias controversas ou desfavoráveis que, por sua vez, dificultam a receptividade para a utilização, comercialização e, por conseguinte, a legalização destes sistemas de pagamento. Embora as criptomoedas ofereçam um sistema de pagamento relativamente seguro e barato em comparação com os sistemas bancários tradicionais, o anonimato oferecido aos usuários pelas criptomoedas contribui substancialmente para custeio de atividades ilegais de elevado potencial ofensivo.

Ante o exposto, embora não haja uma posição muito uniforme entre as nações quanto à possibilidade de regulamentação das criptomoedas, sendo a maioria delas indiferentes quanto à regulação ou criminalização destas, a estrutura de funcionamento das criptomoedas propicia uma permissividade significativa na consolidação ou negociação de práticas ilícitas.

Dito isso, no tocante às premissas jurídicas, ao longo do presente trabalho, foram apresentadas todos os elementos conceituais necessários para abordar o problema que perfaz o objeto deste trabalho: a análise dos limites da imputação penal cabíveis aos usuários da rede Bitcoin que se dedicam exclusivamente as atividades de mineração da criptomoeda e que, por sua vez, possuem a cópia local do *blockchain* do Bitcoin com os dados descritos no estudo da RWTH Aachen University, sem realizar quaisquer interações diretas com tais arquivos digitais contidos nesta estrutura.

Como previamente mencionado, é importante salientar que, apesar de o Bitcoin ter sido a única criptomoeda analisada no estudo da RWTH Aachen University, dada a similitude do mecanismo de funcionamento das criptomoedas, as premissas técnicas se

aplicam as demais criptomoedas, assim como as premissas jurídicas caso sejam descobertos achados semelhantes do estudo da RWTH Aachen University em *blockchains* de outras criptomoedas.

Delimitado os referenciais fáticos para análise da aplicação da norma penal, conforme analisado na seção anterior, de plano, pode-se afirmar que todas as descobertas do estudo da RWTH Aachen University representam condutas atípicas na legislação penal vigente. Utilizando-se os grupos conceituais anteriormente citados, constatamos que a posse incidental dos arquivos catalogados nos grupos "Malware", "Violações de Direitos Autorais", "Conteúdo Politicamente Sensível", "Violações de Privacidade" e "Conteúdo Ilegal e Condenado" são impassíveis de serem consideradas como condutas típicas e, por conseguinte, sujeitas a aplicação de sanção penal.

Numa breve recapitulação sobre as considerações realizadas na seção anterior, o grupo "*Malware*" não foi objeto de análise jurídica, uma vez que a posse de tal arquivo, se manipulado, colocaria o seu detentor na condição de vítima, cujo fato não guarda nenhuma pertinência com o objeto do presente trabalho.

No segundo grupo, "Violações de Direitos Autorais", para que a posse de direitos autorais de terceiros se caracterize como fato típico, necessita-se a presença do elemento volitivo doloso, comissivo ou omissivo, cuja direção finalística venha a ofender, violar ou infringir direitos autorais positivados nas leis nºs 9.609/1998 e 9.610/1998.

Relativo ao terceiro e quarto grupo, consolidou-se que mera posse de arquivos digitais, cujo conteúdo represente informações sensíveis ao poder governamental ou detenha informações particulares de terceiros, se ausentes o dolo e a violação da conduta descrita no núcleo do tipo penal (divulgar), sem justo motivo (elemento normativo do tipo) do art. 153, do Código Penal, não configura conduta típica e, portanto, não há aplicação de sanção penal.

Finalmente, o último grupo detém as descobertas com maior potencial ofensivo, correlatos à exploração de conteúdos de pornografia infantil. Na legislação penal pátria, a disponibilização, a divulgação, disponibilização e a posse de conteúdo pornográfico infantojuvenil são consideradas penalmente típicas, consoante o disposto nos arts. 241-

A e 241-B do ECA. Ambos os tipos penais são dolosos, de perigo abstrato, permanentes ou instantâneos, admitem a tentativa e não possuem modalidade culposa.

Por conseguinte, embora a mera posse de conteúdos pornográficos com natureza infantojuvenil enseja a tipicidade formal consubstanciada nos arts. 241-A e 241-B do ECA, tratando-se de hipótese de crime permanente os núcleos do tipo penal "disponibilizar"(art. 241-A) e "possuir" (241-B), ambos tipos penais necessitam o preenchimento do elemento subjetivo do tipo tenha natureza dolosa para que, por sua vez, a conduta seja considerada como materialmente típica.

Em contraste com a circunstância fática adotada como objeto de análise do presente trabalho, em todos os tipos penais supracitados, pode-se aduzir que houve a ausência de, pelo menos, um dos elementos seguintes: elemento subjetivo do tipo (dolo), elemento objetivo caracterizador da conduta delitiva (núcleo) ou elemento normativo do tipo (*v.g.* "sem justo motivo").

Abordando a questão sob a ótica da teoria do crime, no que concerne ao elemento volitivo do agente, a circunstância fática em exame demonstra que, dependendo dos conhecimentos de informática do agente, a possibilidade que o usuário minerador preveja a existência de arquivos digitais ilícitos na sua cópia local do *blockchain* é remota.

Com efeito, embora seja tecnicamente possível a inserção de dados não financeiros com conteúdo ilegal na estrutura do *blockchain*, dado o protocolo do algoritmo do Bitcoin estabelecer um limite físico aproximado de 1 Mb para cada bloco de informação que venha a integrar o *blockchain*[45], percebe-se que, dependendo do tipo de conteúdo não financeiro, sua fragmentação ou compressão se torna obrigatória para que a inserção seja possível na respectiva estrutura. Não é improvável, ainda, que tal conteúdo possa ter sofrido processo de cifragem (criptografia), tornando ainda mais improvável a identificação de arquivos ilícitos na cópia local do *blockchain.*

Sendo assim, a tendência é que todos os arquivos não financeiros com dimensões superiores a 100 Kb necessitam ser reconstruídos para que possam ser

[45] Gráfico da média da dimensão computacional dos blocos de informação inseridos no *blockchain* do Bitcoin. Disponível em: <https://blockchain.info/pt/charts/avg-block-size>. Acesso em: 18/06/2018.

visualizados imediatamente pelo usuário[46]. Tal premissa é crucial para aferição do elemento volitivo do agente descrito na circunstância fática que perfaz o objeto do presente trabalho, em razão das seguintes repercussões: a) 100 Kb é um valor computacional ínfimo nos termos atuais; fotos, vídeos, alguns arquivos de textos e outros tipos de arquivos digitais já superam consideravelmente tal valor de dimensão computacional; b) para a inserção de dados não financeiros, bem como a visualização dos mesmos, nos termos supracitados, demanda certa engenhosidade tanto daquele que os insere quando daqueles que os visualizam, ou seja, não é todo o usuário de informática que é capaz de realizar ambas as ações.

Ante tais premissas, torna-se bastante plausível vislumbrar a possibilidade do usuário do Bitcoin incorrer numa conduta culposa, uma vez que arquivos não financeiros com conteúdo ilícito, inseridos do *blockchain* do Bitcoin por meio diversas transações, provavelmente estejam fragmentados ou comprimidos na respectiva estrutura. Ainda que o conteúdo do *blockchain* esteja disponível para acesso imediato para qualquer usuário da rede, apenas aqueles detiverem os conhecimentos mais avançados em informática obterão conhecimento efetivo da existência de arquivos ilícitos na respectiva estrutura. Logo, um usuário da rede Bitcoin com conhecimentos modestos de informática, na pior das hipóteses, incorreria em culpa consciente.

De outra banda, acreditamos seja possível ocorrer na mesma circunstância fática uma conduta dolosa na modalidade eventual. Para isso, o agente deve tomar conhecimento do conteúdo ilícito dos arquivos de conteúdo ilícitos contidos no *blockchain* do Bitcoin, ou seja, acessá-los. Inevitavelmente, de acordo com as premissas supracitadas, o agente agirá com dolo eventual quando possui consciência plena sobre a existência dos arquivos ilícitos contidos na estrutura do *blockchain* do Bitcoin e, ante tal descoberta, agir com indiferença e consentir com os riscos oriundos desta. Ainda, imperioso ressaltar que o agente que agir nessa modalidade de dolo provavelmente possua conhecimentos mais avançados em informática em relação ao usuário médio de informática.

---

[46] Insta salientar que as transações financeiras do Bitcoin possuem um limite da carga útil para transmissão de dados bastante reduzido (80 B a 100 Kb), conforme descrito na tabela 1 do presente trabalho. Portanto, tal fato evidencia ainda mais que o conteúdo ilícito contido no *blockchain* do Bitcoin fora inserido de forma fragmentada, comprimida ou de ambos os modos.

Portanto, as duas situações expostas são possíveis, mas a efetivação do elemento volitivo da conduta é bastante distinta. Enquanto gênero, a conduta culposa estará caracterizada pela determinação finalística do agente não buscar o resultado típico e nem assumi-lo se este vier a ocorrer, independente de sua consciência quanto à possibilidade da consolidação de tal evento. Em contrapartida, com a plena ciência quanto à possibilidade do resultado típico, o dolo eventual se caracterizará quando o agente assume o risco da produção do resultado típico secundário a sua conduta finalística primária, sendo indiferente quanto à consumação do fato típico inerente ao evento secundário.

No caso em exame, em tese, a não ser que o usuário venha descobrir os arquivos digitais ilícitos, acessá-los e posteriormente retomasse suas atividades na rede Bitcoin "como se nada tivesse ocorrido" (dolo eventual) ou, ainda, aperfeiçoar a posse de tais arquivos mediante a garantia do armazenamento e preservação dos mesmos (dolo direto); constata-se como desproporcional a imputação penal sobre qualquer usuário da rede Bitcoin nos termos da circunstância fática analisada nesta seção.

Visto que a posse de tais arquivos, em regra, ocorreu de forma incidental, no momento em que o respectivo usuário optou por realizar atividades de mineração, independente das circunstâncias controversas sobre a criptomoeda, percebe-se que haveria uma criminalização exacerbada sobre tal conduta cujo consentimento ou consciência dos usuários sobre os resultados típicos, na maioria dos casos, são mínimos.

Cabe salientar que a legislação pátria quanto à regulamentação do uso e comercialização de criptomoedas é incipiente[47], bem como também é ineficaz para sustentar uma política criminal adequada para coibir a ocorrência de circunstâncias semelhantes as que foram apresentadas ao longo do presente trabalho. Diante desse panorama, a possibilidade de punir os usuários da rede Bitcoin, em virtude das circunstâncias fáticas previamente expostas, representaria uma afronta direta aos princípios norteadores do Direito Penal brasileiro, haja vista que é dever do poder estatal ponderar o alcance de suas intervenções coercitivas, bem como reduzindo-as ao mínimo necessário, buscando assim formas alternativas para a composição de conflitos sociais.

[47] Atualmente, o PL nº 2.303/2015 é o único esforço estatal para regulamentação de criptomoedas. Em suma, o projeto prevê a atribuição de competência ao Banco Central do Brasil para regulamentar o uso e comercialização de criptomoedas. Não há nenhuma política criminal concreta acerca desse desiderato.

Ante o exposto, ponderando-se as premissas expostas ao longo do presente trabalho, conclui-se que a posse incidental dos arquivos digitais resultantes das práticas de mineração de moedas na rede Bitcoin, cujo conteúdo ou posse pode representar hipóteses de tipicidade formal na legislação penal brasileira, é atípica diante da ausência do preenchimento do elemento subjetivo do tipo (dolo), necessários em todos os tipos penais passíveis de aplicação no caso examinado; tratando-se, portanto, de conduta insuscetível de criminalização e de imposição de qualquer forma de sanção penal.

5. CONSIDERAÇÕES FINAIS

O presente trabalho teve o propósito de provocar uma reflexão sobre um fato que ocorrerá de forma súbita nos próximos anos: a reavaliação de instituições sociais, culturais e econômicas face às repercussões da revolução tecnológica. Como podemos perceber, o avanço tecnológico veloz da nossa época está moldando substancialmente o paradigma social moderno, tanto dos atores sociais quanto das instituições que regem o sistema de convivência coletiva.

Percebemos que tal mudança será bastante acentuada e isso trará dificuldades aos operadores do Direito para abordar questões sociais emergentes, seja pela dificuldade das instituições jurídicas se adaptarem tempestivamente as mudanças e demandas sociais, seja pela dificuldade dos próprios operadores de entender conceitualmente os respectivos problemas.

Em outras palavras, estamos a falar aqui sobre a nova roupagem que os avanços tecnológicos estão conferindo a institutos e instituições tradicionais. No presente trabalho, tratamos sobre uma tecnologia disruptiva com potencial significativo para restruturar a forma como entendemos o tradicional sistema de trocas econômicas: o Bitcoin.

Tal inovação tecnológica inaugurou uma quebra de paradigma vultuoso: um sistema de pagamento credível que não necessita de um terceiro para consolidar as transações financeiras, papel tradicional do sistema bancário. Além disso, esse sistema realizou outro avanço significativo: transcendeu as limitações das barreiras nacionais, seja no ponto de vista territorial, seja no aspecto institucional.

Observa-se que o Bitcoin propiciou um questionamento, ainda que implícito, sobre quais papéis sociais cujos indivíduos são capazes de desempenhar na construção das instituições que possibilitam a coexistência social. Tal fato vem repercutindo também como as nações estão se organizando para se adequarem a nova concepção de ordem mundial, cuja consolidação está ocorrendo de forma mais acentuada dia após dia com o avanço tecnológico: o conhecido fenômeno da globalização.

Em que pese o fato dos avanços tecnológicos propiciarem progresso em diversas frentes, em contrapartida, o mesmo advento pode trazer muitos conflitos a ordem das coisas previamente estabelecidas. Nesse sentido, o Bitcoin ofereceu uma ferramenta apta a propiciar que os agentes econômicos pudessem se autotutelar no mercado.

Todavia, além do problema analisado ao longo deste trabalho, essa tecnologia também ofereceu riscos a seus usuários quando estes, na condição de mineradores, validam involuntariamente transações financeiras de outros usuários anônimos na rede Bitcoin, cuja boa parcela dos casos se tratam de operações com finalidades ilícitas, conforme citado na seção anterior. Portanto, entendemos que o controle adequado do uso tecnológico é um desafio inevitável que instituições estatais terão que enfrentar, ao longo dos anos seguintes, para garantir a ordem e a paz social.

Ao longo do presente trabalho, ao analisarmos o artigo científico da RWTH Aachen University – *A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin* – tanto no escopo técnico e quanto no escopo jurídico, buscamos esclarecer as peculiaridades atinentes ao mecanismo de funcionamento das criptomoedas, bem como oferecer uma abordagem jurídica possível, sob a luz dos institutos jurídicos do Direito Brasileiro, sobre um dos principais problemas citados pelo estudo referenciado: o risco de imputação penal sobre usuários mineradores que venham a desconhecer os dados potencialmente ilícitos que estão inseridos na estrutura do *blockchain* do Bitcoin atualmente.

Para tal finalidade, apresentamos o teor do estudo da RWTH Aachen University, em seguida, descrevemos o mecanismo de funcionamento das criptomoedas e concluímos parcialmente sobre as implicações técnicas e fáticas relativas às descobertas do referido estudo e como elas poderiam causar repercussões jurídicas significativas no ordenamento jurídico brasileiro.

Por conseguinte, procedemos à exposição dos institutos jurídicos essenciais para análise jurídica da circunstância fática que perfaz o objeto do presente trabalho. Foram apresentadas premissas doutrinárias e jurisprudenciais sobre os possíveis vetores de aplicação da norma penal na referida circunstância fática. Após a exposição das premissas menores e maiores do trabalho respectivamente, procedemos com o silogismo entre as mesmas.

Como mencionado ao longo do trabalho, o Bitcoin possui circunstâncias tanto abonadoras quanto desabonadoras ao longo de sua história. Talvez haja quem pense que tais circunstâncias desabonadoras são mais significativas que as abonadoras, todavia, para fins de análise jurídica, "lugares-comuns" como este podem ser um perigoso critério para formação de juízo de convicção para aplicação da lei, especialmente quando esta se tratar de uma lei penal.

Assim, acreditamos que é necessária parcimônia na abordagem de fatos sociais com cunho tecnológico preponderante, uma vez que o desconhecimento dos meandros deste fenômeno pode ensejar injustiças na aplicação da lei, especialmente no que concerne a tutela jurisdicional penal.

Ante o exposto, dada a ausência de uma política criminal mais adequada, quanto ao combate de crimes cibernéticos, bem como a incipiente regulamentação do uso e comercialização de criptomoedas no país, conclui-se que a criminalização dos usuários mineradores de criptomoedas, que, porventura, venham a obter a posse incidental de arquivos digitais com conteúdos ilícitos, contidos na estrutura do *blockchain* da respectiva moeda, é uma medida descabida e desproporcional se analisado em contraste com as premissas apresentadas neste trabalho.

REFERÊNCIAS

ANTONOPOULOS, Andreas M.. **Mastering Bitcoin** – 1ª ed. – O' Reilly Media, Inc, 2014.

SWAN, Melanie. **Blockchain, Blueprint for a New Economy** – 1ª ed. – O' Reilly Media, Inc., 2015.

GUPTA, Manav. **Blockchain for Dummies, IBM Limited Edition** – 1ª ed. – John Wiley & Sons, Inc., 2017.

STALLINGS, William. **Criptografia e segurança de redes: princípios e práticas** – 6ª ed. – São Paulo: Pearson Education do Brasil, Inc, 2015.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain Revolution: como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo**. São Paulo: SENAI-SP Editora, 2016.

MATZUTT *et al.*. **A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin**, 2018. Disponível em: <https://publications.rwth-aachen.de/record/721552>. Acesso em: 15/03/2018.

FOLEY, Sean; KARLSEN, Jonathan R.; PUTNINS, Tãlis J.. **Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?**, 2014. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645>. Acesso em: 31/03/2018.

CHOHAN, Usman W.. **A History of Bitcoin**, 2017. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047875>. Acesso em: 21/05/2018.

KAPLANOV, Nikolei M..**Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation**, 2012. Disponível em: <https://lawecommons.luc.edu/cgi/viewcontent.cgi?article=1920&context=lclr>. Acesso em: 21/05/2018.

MÖSER, Malte; BÖHME, Rainer; BREUKER, Dominic. **An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem**, 2013. Disponível em: <https://maltemoeser.de/paper/money-laundering.pdf>. Acesso em: 23/05/2018.

GRINGBERG, Reuben. **Bitcoin: An Innovative Alternative Digital Currency**, 2011. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857.>. Acesso em: 22/05/2018.

BERGSTRA, Jan A.; LEEUW, Karl de. **Bitcoin and Beyond: Exclusively Informational Money**, 2013. Disponível em: <https://arxiv.org/abs/1304.4758>. Acesso em: 26/05/2018.

BÖHME, Rainer. **Internet Protocol Adoption: Learning from Bitcoin**, 2013. Disponível em: <https://www.wi.uni-muenster.de/sites/wi/files/news/2013120419/

boehme2013_iab_itat_position_paper_internet_protocol_adoption.pdf>. Acesso em: 24/05/2018.

BREZO, Félix; BRINGAS, Pablo G.. **Issues and Risks Associated with Cryptocurrencies such as Bitcoin**, 2012. Disponível em: <https://www.researchgate.net/publication/234845612_Issues_and_Risks_Associated_with_Cryptocurrencies_such_as_Bitcoin>. Acesso em: 26/05/2018.

DION, Derek A.. **I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in The E-Conomy of Hacker-Cash**, 2013. Disponível em: <http://illinoisjltp.com/journal/wp-content/uploads/2013/05/Dion.pdf>. Acesso em: 22/05/2018.

BRITO, Jerry; SHADAB, Houman B.; CASTILLO, Andrea. **Bitcoin Financial Regulation: Securities,Derivatives, Prediction Markets, and Gambling**, 2014. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2423461>. Acesso em: 28/05/2018.

CLEMENT et al.. **On the (Limited) Power of Non-Equivocation**, 2012. Disponível em: <http://www.gsd.inesc-id.pt/~rodrigo/nonequiv_podc12.pdf>. Acesso em: 28/05/2018.

SCHILLING, Linda; UHLIG, Harald. **Some simple Bitcoin Economics**, 2018. Disponível em: <https://www.imfs-frankfurt.de/fileadmin/user_upload/Events_2018/MMCI_Conference/Papers/Schilling_Uhlig_BitcoinEcon_v30.pdf>. Acesso em: 23/05/2018.

SCHEUERMANN, Björn; TSCHORSCH, Florian. **Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies**, 2016. Disponível em: < http://www.dsi.tu-berlin.de/menue/group/tschorsch/publications/?tx_sibibtex_pi1%5Bcontentelement%5D=tt_content%3A796955&tx_sibibtex_pi1%5BshowUid%5D=1309142&cHash=dbb48d7ec96c9947bf311989b4211e49 >. Acesso em: 30/05/2018.

CLEMENT et al.. **On the (Limited) Power of Non-Equivocation**, 2012. Disponível em: <http://www.gsd.inesc-id.pt/~rodrigo/nonequiv_podc12.pdf>. Acesso em: 30/05/2018.

CERT.br, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet, versão 4.0**. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf >. Acesso em: 20/05/2018.

BRASIL. **Exposição de motivos do Ministro Francisco Campos, Código Penal de 1940**, Revista de Informação Legislativa – outubro a dezembro, p.120-153, 1969. Disponível em: <https://www2.senado.leg.br/bdsf/bitstream/handle/id/224132/_000341193.pdf?sequence=1>.Acesso em: 18/06/2018

BRASIL. **Código Penal – Decreto Lei nº 2.848**, 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm> Acesso em: 18/06/2018

BRASIL. **Estatuto da Criança e do Adolescente** - Lei n.º 8.069, de 13 de Julho de 1990. Disponível:<http://www.planalto.gov.br/ccivil_03/leis/L8069.htm>. Acesso em: 18/06/2018.

BRASIL. **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988. 48ª Edição. São Paulo: Saraiva, 2013.

REALE, Miguel. **Lições Preliminares de Direito** – 27ª ed., 11ª tiragem – São Paulo: Saraiva, 2002.

ASSIS TOLEDO, Francisco. **Princípios Básicos de Direito Penal** – 5ª ed.– São Paulo: Saraiva, 1994.

PACELLI, Eugênio; CALLEGARI, André. **Manual de Direito Penal: parte geral** – 2ª ed. ver. e atual. – São Paulo: Atlas, 2016.

NUCCI, Guilherme de Souza. **Curso de Direito Penal: parte geral, arts. 1º a 120 do Código Penal** – Rio de Janeiro: Forense, 2017.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal: parte geral, vol. 1** – 17ª ed. rev., ampl. e atual. de acordo com a Lei n. 12.550, de 2011 – São Paulo: Saraiva, 2012.

ESTEFAM, André; GONÇALVES, Victor Eduardo Rios. **Direito Penal Esquematizado: parte geral** – 5ª ed.– São Paulo: Saraiva, 2016.

JESUS, Damásio de. **Código Penal Anotado** – 22ª ed.– São Paulo: Saraiva, 2014.

MASSON, Cléber. **Código Penal Comentado** – 2ª ed. rev., ampl. e atual.– Rio de Janeiro: Forense; São Paulo: MÉTODO, 2014.

SILVA, Ângelo Roberto Ilha da (Org.); SHIMABUKURO, Adriana *et al*.. **Crimes Cibernéticos: racismo, *cyberbulling*, *deep web*, pedofilia e pornografia infantil, infiltração de agentes por meio virtual, obtenção de provas digitais, nova lei antiterrorismo, outros temas** – 1ª ed. – Porto Alegre: Livraria do Advogado, 2017.

ANEXO A – A QUANTITATIVE ANALYSIS OF THE IMPACT OF ARBITRARY BLOCKCHAIN CONTENT ON BITCOIN

A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin

Roman Matzutt[1], Jens Hiller[1], Martin Henze[1], Jan Henrik Ziegeldorf[1], Dirk Müllmann[2], Oliver Hohlfeld[1], and Klaus Wehrle[1]

[1] Communication and Distributed Systems, RWTH Aachen University, Germany,
{matzutt,hiller,henze,ziegeldorf,hohlfeld,wehrle}@comsys.rwth-aachen.de
[2] Data Protection Research Institute, Goethe University, Frankfurt/Main,
muellmann@jur.uni-frankfurt.de

Abstract. Blockchains primarily enable credible accounting of digital events, e.g., money transfers in cryptocurrencies. However, beyond this original purpose, blockchains also irrevocably record *arbitrary* data, ranging from short messages to pictures. This does not come without risk for users as each participant has to locally replicate the complete blockchain, particularly including potentially harmful content. We provide the first systematic analysis of the benefits and threats of arbitrary blockchain content. Our analysis shows that certain content, e.g., illegal pornography, can render the mere possession of a blockchain illegal. Based on these insights, we conduct a thorough quantitative and qualitative analysis of unintended content on Bitcoin's blockchain. Although most data originates from benign extensions to Bitcoin's protocol, our analysis reveals more than 1600 files on the blockchain, over 99 % of which are texts or images. Among these files there is clearly objectionable content such as links to child pornography, which is distributed to all Bitcoin participants. With our analysis, we thus highlight the importance for future blockchain designs to address the possibility of unintended data insertion and protect blockchain users accordingly.

1 Introduction

Bitcoin [45] was the first completely distributed digital currency and remains the most popular and widely accepted of its kind with a market price of ∼4750 USD per bitcoin as of August 31st, 2017 [14]. The enabler and key innovation of Bitcoin is the *blockchain*, a public append-only and tamper-proof log of all transactions ever issued. These properties establish trust in an otherwise trustless, completely distributed environment, enabling a wide range of new applications, up to distributed general-purpose data management systems [69] and purely digital data-sharing markets [41]. In this work, we focus on the arbitrary, non-financial data on Bitcoin's famous blockchain, which primarily stores financial transactions. This non-financial data fuels, e.g., digital notary services [50], secure releases of cryptographic commitments [16], or non-equivocation schemes [62].

However, since all Bitcoin participants maintain a *complete local copy* of the blockchain (e.g., to ensure correctness of blockchain updates and to bootstrap

new users), these desired and vital features put all users at risk when *objectionable content* is irrevocably stored on the blockchain. This risk potential is exemplified by the (mis)use of Bitcoin's blockchain as an anonymous and irrevocable content store [40,56,35]. In this paper, we systematically analyse non-financial content on Bitcoin's blockchain. While most of this content is harmless, there is also content to be considered objectionable in many jurisdictions, e.g., the depiction of nudity of a young woman or hundreds of links to child pornography. As a result, it could become illegal (or even already is today) to possess the blockchain, which is required to participate in Bitcoin. Hence, objectionable content can jeopardize the currently popular multi-billion dollar blockchain systems.

These observations raise the question whether or not unintended content is ultimately beneficial or destructive for blockchain-based systems. To address this question, we provide the first *comprehensive* and *systematic* study of unintended content on Bitcoin's blockchain. We first *survey and explain* methods to store arbitrary, non-financial content on Bitcoin's blockchain and discuss potential benefits as well as threats, most notably w.r.t. content considered illegal in different jurisdictions. Subsequently and in contrast to related work [56,40,12], we *quantify and discuss* unintended blockchain content w.r.t. the wide range of insertion methods. We believe that objectionable blockchain content is a pressuring issue despite potential benefits and hope to stimulate research to mitigate the resulting risks for novel as well as existing systems such as Bitcoin.

This paper is organized as follows. We survey methods to insert arbitrary data into Bitcoin's blockchain in Section 2 and discuss their benefits and risks in Section 3. In Section 4, we systematically analyze non-financial content in Bitcoin's blockchain and assess resulting consequences. We discuss related work in Section 5 and conclude this paper in Section 6.

2 Data Insertion Methods for Bitcoin

Beyond intended recording of financial transactions, Bitcoin's blockchain also allows for injection of *non-financial* data, either short messages via special transaction types or even complete files by encoding arbitrary data as standard transactions. We first briefly introduce Bitcoin transactions and subsequently survey methods available to store arbitrary content on the blockchain via transactions.

Bitcoin *transactions* transfer funds between a payer (sender) and a payee (receiver), who are identified by public-private key pairs. Payers announce their transactions to the *Bitcoin network*. The *miners* then publish these transactions in new *blocks* using their computational power in exchange for a *fee*. These fees vary, but averaged at 215 satoshi per Byte during August 2017 [4] (1 satoshi = 10^{-8} bitcoin). Each transaction consists of several *input scripts*, which unlock funds of previous transactions, and of several *output scripts*, which specify who receives these funds. To unlock funds, input scripts contain a signature for the previous transaction generated by the owner of the funds. To prevent malicious scripts from causing excessive transaction verification overheads, Bitcoin uses transaction script *templates* and expects peers to discard non-compliant scripts.

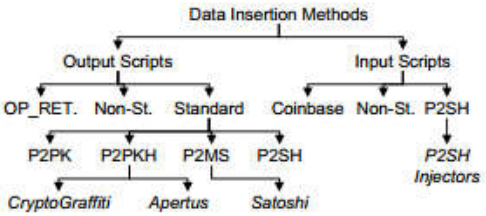


Fig. 1: Bitcoin data insertion methods (italics show content insertion services)

Method	Payload	Costs/B	Eff.
OP_RET.	80 B	3.18–173.55 ct	poor
Coinbase	96 B	—	poor
Non-St. Out.	99 044 B	1.03–198.05 ct	poor
Non-St. In.			med.
P2PK	85 345 B	1.24–207.79 ct	high
P2PKH	58 720 B	1.87–197.58 ct	high
P2MS	92 625 B	1.11–234.33 ct	high
P2SH Out.	62 400 B	1.77–195.54 ct	high
P2SH In.	99 018 B	1.03–225.61 ct	high

Table 1: Payload, costs, and efficiency of low-level data insertion methods

Figure 1 shows the insertion methods for non-financial data we identified in Bitcoin. We distinguish *low-level data insertion methods* inserting small data chunks and *content insertion services*, which systematically utilize the low-level methods to insert larger chunks of data. In the following, we refer to non-financial blockchain data as *content* if it has a self-contained structure, e.g., a file or readable text, or as *data* otherwise, e.g., fragments inserted via a low-level method.

2.1 Low-level Data Insertion Methods

We first survey the efficiency of the low-level data insertion methods w.r.t. to *insertable payload* and *costs* per transaction (Table 1). To this end, we first explain our comparison methodology, before we detail i) intended data insertion methods (OP_RETURN and coinbase), ii) utilization of non-standard transactions, and iii) manipulation of standard transactions to insert arbitrary data.

Comparison Methodology. We measure the *payload per transaction (PpT)*, i.e., the number of non-financial Bytes that can be added to a single standard-sized transaction ($\leq$ 100 000 B). *Costs* are given as the minimum and maximum costs per Byte (CpB) for the longest data chunk a transaction can hold, and for inserting 1 B. Costs are inflicted by paying transaction fees and possibly *burning* currency (at least 546 satoshi per output script), i.e., making it unspendable. For our cost analysis we assume Bitcoin's market price of 4748.25 USD as of August 31st, 2017 [14] and the average fees of 215 satoshi per Byte as of August 2017 [4]. Note that high variation of market price and fees results in frequent changes of presented absolute costs per Byte. Finally, we rate the overall *efficiency* of an approach w.r.t. insertion of arbitrary-length content. Intuitively, a method is efficient if it allows for easy insertion of large payloads at low costs.

OP_RETURN. This special transaction template allows attaching one small data chunk to a transaction and thus provides a *controlled channel* to annotate transactions without negative side effects. E.g., in typical implementations peers increase performance by caching spendable transaction outputs and OP_RETURN outputs can safely be excluded from this cache. However, data chunk sizes are limited to 80 B per transaction.

Coinbase. In Bitcoin, each block contains exactly one coinbase transaction, which introduces new currency into the system to incentivize miners to dedi-

cate their computational power to maintain the blockchain. The input script of coinbase transactions is up to 100 B long and consists of a variable-length field encoding the new block's position in the blockchain [9]. Stating a larger size than the overall script length allows placing arbitrary data in the resulting gap. This method is inefficient as only active miners can insert only small data chunks.

Non-standard Transactions. Transactions can deviate from the approved transaction templates [48] via their output scripts as well as input scripts. In theory, such transactions can carry arbitrarily encoded data chunks. Transactions using non-standard *output* scripts can carry up to 96.72 KiB at comparably low costs. However, they are inefficient as miners ignore them with high probability. Yet, non-standard output scripts occasionally enter the blockchain if miners insufficiently check them (cf. Section 4.2). Contrarily, non-standard *input* scripts are only required to match their respective output script. Hence, input scripts can be altered to carry arbitrary data if their semantics are not changed, e.g., by using dead conditional branches. This makes non-standard input scripts slightly better suited for large-scale content insertion than non-standard output scripts.

Standard Financial Transactions. Even *standard financial transactions* can be (mis)used to insert data using mutable values of output scripts. There are four approved templates for standard financial transactions: Pay to public-key (P2PK) and pay to public-key hash (P2PKH) transactions send currency to a dedicated receiver, identified by an address derived from her private key, which is required to spend any funds received [48]. Similarly, multi-signature (P2MS) transactions require m out of n private keys to authorize payments. Pay to script hash (P2SH) transactions refer to a *script* instead of keys to enable complex spending conditions [48], e.g., to replace P2MS [10]. The respective public keys (P2PK, P2MS) and script hash values (P2PKH, P2SH) can be replaced with arbitrary data as Bitcoin peers can not verify their correctness before they are referenced by a subsequent input script. While this method can store large amounts of content, it involves significant costs: In addition to transaction fees, the user must burn bitcoins as she replaces valid receiver identifiers with arbitrary data (i.e., invalid receiver identities), making the output unspendable. Using multiple outputs enables PpTs ranging from 57.34 KiB (P2PKH) to 96.70 KiB (P2SH inputs) at CpBs from 1.03 ct to 1.87 ct. As they behave similarly w.r.t. data insertion, we collectively refer to all standard financial transactions as P2X in the following. P2SH scripts also allow for efficient data insertion into input scripts as P2SH input scripts are published with their redeem script. Due to miners' verification of P2SH transactions, transaction are not discarded if the redeem script is not template-compliant (but the overall P2SH transaction is).

We now survey different services that systematically leverage the discussed data insertion methods to add larger amounts of content to the blockchain.

2.2 Content Insertion Services

Content insertion services rely on the low-level data insertion methods to add content, i.e., files such as documents or images, to the blockchain. We identify four conceptually different content insertion services and present their protocols.

CryptoGraffiti. This web-based service [30] reads and writes messages and files from and to Bitcoin's blockchain. It adds content via multiple P2PKH output scripts within a single transaction, storing up to 60 KiB of content. To retrieve previously added content, CryptoGraffiti scans for transactions that either consist of at least 90 % printable characters or contain an image file.
Satoshi Uploader. The Satoshi Uploader [56] inserts content using a single transaction with multiple P2X outputs. The inserted data is stored together with a length field and a CRC32 checksum to ease decoding of the content.
P2SH Injectors. Several services [35] insert content via slightly varying P2SH input scripts. They store chunks of a file in P2SH input scripts. To ensure file integrity, the P2SH redeem scripts contain and verify hash values of each chunk.
Apertus. This service [29] allows *fragmenting* content over multiple transactions using an arbitrary number of P2PKH output scripts. Subsequently, these fragments are referenced in an *archive* stored on the blockchain, which is used to retrieve and reassemble the fragments. The chosen encoding optionally allows augmenting content with a comment, file name, or digital signature.

To conclude, Bitcoin offers various options to insert arbitrary, non-financial data. These options range from small-scale data insertion methods exclusive to active miners to services that allow any user to store files of arbitrary length. This wide spectrum of options for data insertion raises the question which benefits and risks arise from storing content on Bitcoin's blockchain.

3 Benefits and Risks of Arbitrary Blockchain Content

Bitcoin's design includes several methods to insert arbitrary, non-financial data into its blockchain in both intended and unintended ways. In this section, we discuss potential benefits of engraving arbitrary data into Bitcoin's blockchain as well as risks of (mis)using these channels for content insertion.

3.1 Benefits of Arbitrary Blockchain Content

Besides the manipulation of standard financial transactions, Bitcoin offers coinbase and OP_RETURN transactions as explicit channels to irrevocably insert small chunks of non-financial data into its blockchain (cf. Section 2). As we discuss in the following, each insertion method has distinguishing benefits:
OP_RETURN. Augmenting transactions with short pieces of arbitrary data is beneficial for a wide area of applications [40,12,62]. Different services use OP_RETURN to link non-financial assets, e.g., vouchers, to Bitcoin's blockchain [40,12], to attest the existence of digital documents at a certain point of time as a digital notary service [58,50,12], to realize distributed digital rights management [70,12], or to create non-equivocation logs [62,8].
Coinbase. Coinbase transactions differ from OP_RETURN as only miners, who dedicate significant computational resources to maintain the blockchain, can use them to add extra chunks of data to their newly mined blocks. Beyond advertisements or short text messages [40], coinbase transactions can aid the

mining process. Adding random bytes to the coinbase transactions allows miners to increase entropy when repeatedly testing random nonces to solve the proof-of-work puzzle [48]. Furthermore, adding identifiable *voting flags* to transactions enables miners to vote on proposed features, e.g., the adoption of P2SH [10].

Large-scale Data Insertion. Engraving large amounts of data into the blockchain creates a long-term non-manipulable file storage. This enables, e.g., the archiving of historical data or censorship-resistant publication, which helps protecting whistleblowers or critical journalists [66]. However, their content is replicated to all users, who do not have a choice to reject storing it.

Hence, non-financial data on the blockchain enables new applications that leverage Bitcoin's security guarantees. In the following, we discuss threats of forcing honest users to download copies of all blockchain content.

3.2 Risks of Arbitrary Blockchain Content

Despite potential benefits of data in the blockchain, insertion of objectionable content can put all participants of the Bitcoin network at risk [43,11,40], as such unwanted content is unchangeable and locally replicated by each peer of the Bitcoin network as benign data. To underpin this threat, we first derive an extensive catalog of content that poses high risks if possessed by individuals and subsequently argue that objectionable blockchain content is able to harm honest users. In the following, we identify five categories of objectionable content:

Copyright Violations. With the advent of file-sharing networks, pirated data has become a huge challenge for copyright holders. To tackle this problem, copyright holders predominantly target users that actively distribute pirated data. E.g., German law firms sue users who distribute copyright-protected content via file-sharing networks for fines on behalf of the copyright holders [28]. In recent years, prosecutors also convicted downloaders of pirated data. For instance, France temporarily suspended users' Internet access and subsequently switched to issuing high fines [36]. As users distribute their blockchain copy to new peers, copyright-protected material on the blockchain can thus provoke legal disputes about copyright infringement.

Malware. Another threat is to download malware [20,42], which could potentially be spread via blockchains [31]. Malware has serious consequences as it can destroy sensitive documents, make devices inoperable, or cause financial losses [34]. Furthermore, blockchain malware can irritate users as it causes antivirus software to deny access to important blockchain files. E.g., Microsoft's antivirus software detected a non-functional virus signature from 1987 on the blockchain, which had to be fixed manually [68].

Privacy Violations. By disclosing sensitive personal data, individuals can harm their own privacy and that of others. This threat peaks when individuals deliberately violate the privacy of others, e.g., by blackmailing victims under the threat of disclosing sensitive data about them on the blockchain. Real-world manifestations of these threats are well-known, e.g., non-consensually releasing private nude photos or videos [54] or fully disclosing an individual's identity to the public with malicious intents [21]. Jurisdictions such as the whole European

Union begin to actively prosecute the unauthorized disclosure *and forwarding* of private information in social networks to counter this novel threat [5].

Politically Sensitive Content. Governments have concerns regarding the leakage of classified information such as state secrets or information that otherwise harms national security, e.g., propaganda. Although whistleblowers reveal nuisances such as corruption, they force all blockchain users to keep a copy of leaked material. Depending on the jurisdiction, the intentional disclosure or the mere possession of such content may be illegal. While, e.g., the US government usually tends to prosecute *intentional* theft or disclosure of state secrets [63], in China the mere possession of state secrets can result in longtime prison sentences [49]. Furthermore, China's definition of state secrets is vague [49] and covers, e.g., "activities for safeguarding state security" [60]. Such vague allegations w.r.t. state secrets have been applied to critical news in the past [18,24].

Illegal and Condemned Content. Some categories of content are virtually universally condemned and prosecuted. Most notably, possession of *child pornography* is illegal at least in the 112 countries [64] that ratified an optional protocol to the Convention on the Rights of the Child [65]. *Religious content* such as certain symbols, prayers, or sacred texts can be objectionable in extremely religious countries that forbid other religions and under oppressive regimes that forbid religion in general. As an example, possession of items associated with an objected religion, e.g., Bibles in Islamist countries, or blasphemy have proven risky and were sometimes even punished by death [13,38].

In conclusion, a wide range of objectionable content can cause direct harm if possessed by users. In contrast to systems such as social media platforms, file-sharing networks, or online storage systems, such content can be stored on blockchains anonymously and irrevocably. Since all blockchain data is downloaded and persistently stored by users, they are liable for any objectionable content added to the blockchain by others. Consequently, it would be illegal to participate in a blockchain-based systems as soon as it contains illegal content.

While this risk has previously been acknowledged [43], definitive answers require court rulings yet to come. However, considering legal texts we anticipate a high potential for illegal blockchain content to jeopardize blockchain-based system such as Bitcoin in the future. Our belief stems from the fact that, w.r.t. child pornography as an extreme case of illegal content, legal texts from countries such as the USA [47], England [3], Ireland [32] deem all data illegal that can be converted into a visual representation of illegal content. As we stated in Section 2, it is easily possible to locate and reassemble such content on the blockchain. Hence, even though convertibility usually covers creating a visual representation by, e.g., decoding an image file, we expect that the term can be interpreted to include blockchain data in the future. For instance, this is already covered implicitly by German law, as a person is culpable for possession of illegal content if she *knowingly possesses* an *accessible document* holding said content [2]. It is critical here that German law perceives the hard disk holding the blockchain as an document [1] and that users can easily reassemble any illegal content within the blockchain. Furthermore, users can be assumed to *knowingly* maintain control

over such illegal content w.r.t. German law if sufficient media coverage causes the content's existence to become public knowledge among Bitcoin users [61], as has been attempted by Interpol [31]. We thus believe that legislators will speak law w.r.t. non-financial blockchain content and that this has the potential to jeopardize systems such as Bitcoin if they hold illegal content.

4 Blockchain Content Landscape

To understand the landscape of non-financial blockchain data and assess its potentials and risks, we thoroughly analyze Bitcoin's blockchain as it is the most widely used blockchain today. Especially, we are interested in i) the *degree of utilization* of data and content insertion methods, ii) the *temporal evolution* of data insertion, and iii) the *types* of content on Bitcoin's blockchain, especially w.r.t. *objectionable* content. In the following, we first outline our measurement methodology before we present an overview and the evolution of non-financial data on Bitcoin's blockchain. Finally, we analyze files stored on the blockchain to derive if any objectionable content is already present on the blockchain.

4.1 Methodology

We detect data-holding transactions recorded on Bitcoin's blockchain based on our study of data insertion methods and content insertion services (cf. Section 2). We distinguish detectors for data insertion methods and detectors for content insertion services. To reduce false positives, e.g., due to public-key hash values that resemble text, we exclude all standard transaction outputs that include already-spent funds from analysis. This is sensible as data-holding transactions replace public keys or hashes such that spending requires computing corresponding private keys or pre-images, which is assumed to be infeasible. Contrarily, even though we thoroughly analyzed possible insertion methods, there is still a chance that we do not exhaustively detect all non-financial data. Nevertheless, our content type analysis establishes a solid lower bound as we only consider readable files retrieved from Bitcoin's blockchain. In the following, we explain the key characteristics of the two classes of our blockchain content detectors.

Low-level Insertion Method Detectors. The first class of detectors is tailored to match individual transactions that are likely to contain non-financial data (cf. Section 2.1). These detectors detect manipulated financial transactions as well as OP_RETURN, non-standard, and coinbase transactions.

Our text detector scans for P2X output scripts for mutable values containing $\geq 90\,\%$ printable ASCII characters (to avoid false positives). The detector returns the concatenation of all output scripts of the same transaction that contain text.

Finally, we consider all coinbase and OP_RETURN transactions as well as non-standard output scripts. We detect coinbase transactions based on the length field mismatch described in Section 2.1. OP_RETURN scripts are detectable as they always begin with an `OP_RETURN` operation. Non-standard output scripts comprise all output scripts which are not template-conform.

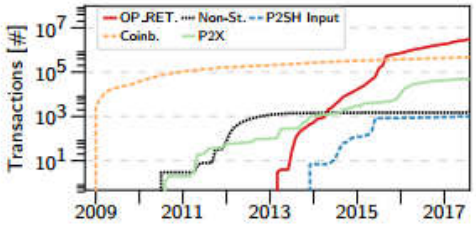


Fig. 2: Cumulative numbers of detected transactions per data insertion method

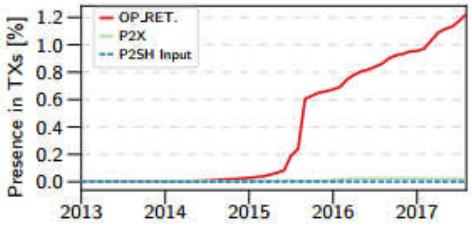


Fig. 3: Ratio of transactions that utilize data insertion methods

Service Detectors. We implemented detectors specific to the content insertion services we identified in Section 2.2. These service-specific detectors enable us to *detect and extract* files based on the services' protocols. These detectors also track the data insertion method used in service-created transactions.

The CryptoGraffiti detector matches transactions with an output that sends a tip to a public-key hash controlled by its provider. For such a transaction, we concatenate all mutable values of output scripts that spend fewer than 10 000 satoshi and store them in a file. This threshold is used to ignore non-manipulated output scripts, e.g., the service provider spending their earnings.

To detect a Satoshi Uploader transaction, we concatenate all of its mutable values that spend the same small amount of bitcoins. If we find the first eight bytes to contain a valid combination of length and CRC32 checksum for the transaction's payload, we store the payload as an individual file.

We detect P2SH Injector content based on redeem scripts containing more than one hash operation (standard transactions use at most one). We then extract the concatenation of the second inputs of all redeem scripts (the first one contains a signature) of a transaction as one file.

Finally, the Apertus detector recursively scans the blockchain for Apertus archives, i.e., Apertus-encoded lists of previous transaction identifiers. Once a referred Apertus payload does not constitute another archive, we retrieve its payload file and optional comment by parsing the Apertus protocol.

Suspicious Transaction Detector. To account for less wide-spread insertion services, we finally analyze standard transactions that likely carry non-financial data but are not detected otherwise. We only consider transactions with at least 50 *suspicious outputs*, i.e., roughly 1 KiB of content. We consider a set of outputs suspicious if all outputs i) spend the same small amount ($< 10\,000$ satoshi) and ii) are unspent. This detector trades off detection rate against false-positive rate. Due to overlaps with service detectors, we exclude matches of this detector from our quantitative analysis, but discuss individual findings in Section 4.3.

4.2 Utilization of Data Insertion Methods

Data and content insertion in Bitcoin has evolved over time, transitioning from single miners exploiting coinbase transactions to sophisticated services that enable the insertion of whole files into the blockchain. We study this evolution in

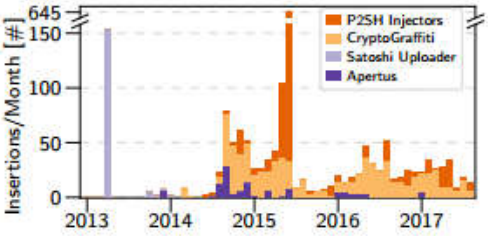


Fig. 4: Number of files inserted via content insertion services per month

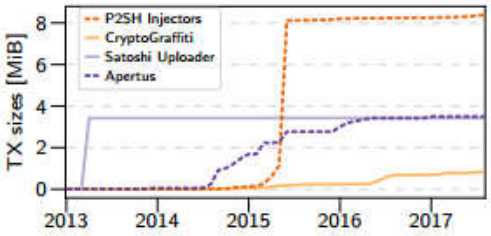


Fig. 5: Cumulative sizes of transactions from content insertion services

terms of used data insertion methods as well as content insertion services and quantify the amount of blockchain data using our developed detectors. Our key insights are that OP_RETURN constitutes a well-accepted success story while content insertion services are currently only infrequently utilized. However, the introduction of OP_RETURN did not shut down other insertion methods, e.g., P2X manipulation, which enable single users to insert objectionable content.

Our measurements are based on Bitcoin's complete blockchain as of August 31st, 2017, containing 482 870 blocks and 250 845 217 transactions with a total disk size of 122.64 GiB. We first analyze the popularity of different data insertion methods and subsequently turn towards the utilization of content insertion services to assess how non-financial data enters the blockchain.

Data Insertion Methods. As described in Section 2.1, OP_RETURN and coinbase transactions constitute *intended* data insertion methods, whereas P2X and non-standard P2SH inputs manipulate legitimate transaction templates to contain arbitrary data. Figure 2 shows the cumulative number of transactions containing non-financial data on a logarithmic scale. In total, our detectors found 3 535 855 transactions carrying a total payload of 118.53 MiB, i.e., only 1.4 % of Bitcoin transactions contain non-financial data. However, we strive to further understand the characteristics of non-financial blockchain content as even a single instance of objectionable content can potentially jeopardize the overall system.

The vast majority of extracted transactions are OP_RETURN (86.8 % of all matches) and coinbase (13.13 %) transactions. Combined, they constitute 95.90 MiB (80.91 % of all extracted data). Out of all blocks, 96.15 % have content-holding coinbase transactions. While only 0.26 % of these contain $\geq$ 90 % printable text, 33.49 % of them contain $\geq$ 15 consecutive printable ASCII characters (mostly surrounded by data without obvious structure). Of these short messages, 14.39 % contain voting flags for new features (cf. Section 3.1). Apart from this, miners often advertise themselves or leave short messages, e.g., prayer verses.

OP_RETURN transactions were introduced in 2013 to offer a benign way to augment single transactions with non-financial data. This feature is widely used, as shown by Figure 3. Among all methods, OP_RETURN is the only one to be present with a rising tendency, with currently 1.2 % of all transactions containing OP_RETURN outputs. These transactions predominantly manage off-blockchain assets or originate from notary services [12]. While P2X transactions are contin-

uously being manipulated, they make up only 0.02 % of all transactions; P2SH inputs are virtually irrelevant. Hence, short non-financial data chunks are well-accepted, viable extensions to the Bitcoin system (cf. Section 3.1).

P2X transactions are asymmetric w.r.t. the number and sizes of data-carrying transactions. Although constituting only 1.6 % of all detector hits, they make up 9.08 % of non-financial data (10.76 MiB). This again highlights the high content-insertion efficiency of P2X transactions (cf. Section 2.1).

Finally, we discuss non-standard transactions and non-standard P2SH input scripts. In total, we found 1703 transactions containing non-standard outputs. The three first non-standard transactions (July 2010) repeatedly used the `OP_CHECKSIG` operation. We dedicate this to an attempted DoS attack that targets to cause high verification times. Furthermore, we found 23 P2PKH transactions from October 2011 that contained `OP_0` instead of a hash value. The steady increase of non-standard transactions in 2012 is due to scripts that consist of 32 seemingly random bytes. Contrarily, P2SH input scripts sporadically carry non-standard redeem scripts and are then often used to insert larger data chunks (as they are used by P2SH Injectors). This is due to P2SH scripts not being checked for template conformity. We found 888 such transactions holding 8.37 MiB of data. Although peers should reject such transactions [48], they still often manage to enter the blockchain. Non-standard P2SH scripts even carry a substantial amount of data (7.07 % of the total data originate from P2SH Injectors).

Content Insertion Services. We now investigate to which extent content insertion services are used to store content on Bitcoin's blockchain. Figure 4 shows utilization patterns for each service and Figure 5 shows the cumulative size of non-financial data inserted via the respective service. Notably, only few users are likely responsible for the majority of service-inserted content.

In total, content insertion services account for 16.12 MiB of non-financial data. More than a half of this content (8.37 MiB) originates from P2SH Injectors. The remainder was mostly inserted using Apertus (21.70 % of service-inserted data) and Satoshi Uploader (21.24 %). Finally, CryptoGraffiti accounts for 0.82 MiB (5.10 %) of content related to content insertion services. In the following, we study how the individual services have been used over time.

Our key observation is that both CryptoGraffiti and P2SH Injectors are infrequently but steadily used; since 2016 we recognize on average 23.65 data items being added per month using these services. Contrarily, Apertus has been used only 26 times since 2016, while the Satoshi Uploader has not been used at all. In fact, the Satoshi Uploader was effectively used only during a brief period: 92.73 % of all transactions emerged in April 2013. During this time, the service was used to upload four archives, six backup text files, and a PDF file.

Although Apertus and the Satoshi Uploader have been used only infrequently, together they constitute 64.32 % of all P2X data we detected. This stems from the utilization of those services to engrave files into the blockchain, e.g., archives or documents (Satoshi Uploader), or images (Apertus). Similarly, P2SH Injectors are used to backup conversations regarding development of the Bitcoin client, especially online chat logs, forum threads, and emails, with a significant peak

File Type	Via Service? yes	Via Service? no	Overall Portion	File Type	Via Service? yes	Via Service? no	Overall Portion
Text	1353	54	87.07 %	Archive	4	0	0.25 %
Images	144	2	9.03 %	Audio	2	0	0.12 %
HTML	45	0	2.78 %	PDF	2	0	0.12 %
Source Code	7	3	0.62 %	**Total**	1557	59	100.0 %

Table 2: Distribution of blockchain file types according to our content-insertion-service and suspicious-transactions detectors.

utilization between May and June 2015 (76.46 % of P2SH Injector matches). Especially Apertus is well-suited for this task as files are spread over multiple transactions. Based on the median, the average Apertus file has a size of 17.15 KiB and is spread over 10 transactions, including all overheads. The largest Apertus file is 310.72 KiB large (including overheads), i.e., three times the size of a standard transaction, and is spread over 96 transactions. The most heavily fragmented Apertus file is even spread over 664 transactions. Contrarily, 95.7 % of CryptoGraffiti matches are short text messages with a median length of 80 Byte.

In conclusion, content insertion services are only infrequently used with varying intentions and large portions of content was uploaded in bursts, indicating that only few users are likely responsible for the majority of service-inserted blockchain content. While CryptoGraffiti is mostly used to insert short text messages that also fit into one OP_RETURN transaction, other services are predominantly used to store, e.g., images or documents. As such files can constitute objectionable content, we further investigate them in the following.

4.3 Investigating Blockchain Files

After quantifying basic content insertion in Bitcoin, we now focus on readable files that are extractable from the blockchain. We refer to *files* as findings of our content-insertion-service or suspicious-transaction detectors that are viewable using appropriate standard software. We reassemble fragmented files only if this is unambiguously possible, e.g., via an Apertus archive. Out of the 22.63 MiB of blockchain data not originating from coinbase or OP_RETURN transactions, we can extract and analyze 1557 files with meaningful content. In addition to these, we could extract 59 files using our suspicious-transaction detector (92.25 % text). Table 2 summarizes the different file types of the analyzed files. The vast majority are text-based files and images (99.34 %).

In the following, we discuss our findings with respect to objectionable content. We manually evaluated all readable files with respect to the problematic categories we identified in Section 3.2. This analysis reveals that content from all those categories already exists in Bitcoin's blockchain today. For each of these categories, we discuss the most severe examples. To protect the safety and privacy of individuals, we omit personal identifiable information and refrain from providing exact information on the location of critical content in the blockchain.

Copyright Violations. We found seven files that publish (intellectual) property and showcase Bitcoin's potential to aid copyright violations. Engraved are the

text of a book, a copy of the original Bitcoin paper [45,56], and two short textual white papers. Furthermore, we found two leaked cryptographic keys: one RSA private key and a firmware secret key. Finally, the blockchain contains a so-called illegal prime, encoding software to break the copy protection of DVDs [56].

Malware. We could not find actual malware in Bitcoin's blockchain. However, an individual non-standard transaction contains a non-malicious cross-site scripting detector. A security researcher inserted this small piece of code which, if interpreted by an online blockchain parser, notifies the author about the vulnerability. Such malicious code could become a threat for users as most websites offering an online blockchain parser also offer online Bitcoin accounts.

Privacy Violations. Users store memorable private moments on the blockchain. We extracted six wedding-related images and one image showing a group of people, labeled with their online pseudonyms. Furthermore, 609 transactions contain online public chat logs, emails, and forum posts discussing Bitcoin, including topics such as money laundering. Storing *private* chat logs on the blockchain can, e.g., leak single user's private information irrevocably. Moreover, third parties can release information without knowledge nor consent of affected users. Most notably, we found at least two instances of *doxing*, i.e., the complete disclosure of another individual's personal information. This data includes phone numbers, addresses, bank accounts, passwords, and multiple online identities. Recently, jurisdictions such as the European Union began to punish such serious privacy violations, including the distribution of doxing data [5]. Again, carrying out such assaults via blockchains fortifies the problem due to their immutability.

Politically Sensitive Content. The blockchain has been used by whistleblowers as a censorship-resistant permanent storage for leaked information. We found backups of the WikiLeaks Cablegate data [37] as well as an online news article concerning pro-democracy demonstrations in Hong Kong in 2014 [25]. As stated in Section 3.2, restrictive governments are known to prosecute the possession of such content. For example, state-critical media coverage has already put individuals in China [18] or Turkey [24] at the risk of prosecution.

Illegal and Condemned Content. Bitcoin's blockchain contains at least eight files with sexual content. While five files only show, describe, or link to mildly pornographic content, we consider the remaining three instances objectionable for almost all jurisdictions: Two of them are backups of link lists to child pornography, containing 274 links to websites, 142 of which refer to Tor hidden services. The remaining instance is an image depicting mild nudity of a young woman. In an online forum this image is claimed to show child pornography, albeit this claim cannot be verified (due to ethical concerns we refrain from providing a citation). Notably, two of the explicit images were only detected by our suspicious-transaction detector, i.e., they were not inserted via known services.

While largely harmless, potentially objectionable blockchain content is infrequently inserted, e.g., links to alleged child pornography or privacy violations. We thus believe that future blockchain designs must proactively cope with objectionable content. Peers can, e.g., filter incoming transactions or revert content-holding transactions [11,51], but this must be scalable and transparent.

5 Related Work

Previous work related to ours comprises i) mitigating the distribution of objectionable content in file-sharing peer-to-peer networks, ii) studies on Bitcoin's blockchain, iii) reports on Bitcoin's susceptibility for content insertion, and iv) approaches to retrospectively remove blockchain content.

The trade-off between enabling open systems for data distribution and risking that unwanted or even illegal content is being shared is already known from peer-to-peer networks. Peer-to-peer-based file-sharing protocols typically limit the spreading of objectionable *public* content by tracking the reputation of users offering files [6,26,55,73] or assigning a reputation to files themselves [19,67]. This way, users can reject objectionable content or content from untrustworthy sources. Contrarily, distributed content stores usually resort to encrypt *private* files before outsourcing them to other peers [17,7]. By storing only encrypted files, users can plausibly deny possessing any content of others and can thus obliviously store it on their hard disk. Unfortunately, these protection mechanisms are not applicable to blockchains, as content cannot be deleted once it has been added to the blockchain and the utilization of encryption cannot be enforced reliably.

Bitcoin's blockchain was analyzed w.r.t. different aspects by numerous studies. In a first step, multiple research groups [53,33,71,72,39] studied the currency flows in Bitcoin, e.g., to perform wealth analyses. From a different line of research, several approaches focused on user privacy and investigated the identities used in Bitcoin [52,46,44,59,23]. These works analyzed to which extent users can be de-anonymized by clustering identities [52,46,44,59,23] and augmenting these clusters with side-channel information [52,44,59,23]. Finally, the blockchain was analyzed w.r.t. the use cases of OP_RETURN transactions [12]. While this work is very close to ours, we provide a first comprehensive study of the complete landscape of non-financial data on Bitcoin's blockchain.

The seriousness of objectionable content stored on public blockchains has been motivated by multiple works [56,57,43,11,40,51]. These works, however, focus on reporting individual incidents or consist of preliminary analyses of the distribution and general utilization of content insertion. To the best of our knowledge, this paper gives the first comprehensive analysis of this problem space, including a categorization of objectionable content and a survey of potential risks for users if such content enters the blockchain. In contrast to previously considered attacks on Bitcoin's ecosystem [22,27], illegal content can be inserted instantly at comparably low costs and can put all participants at risk.

The utilization of chameleon hash functions [15] to chain blocks recently opened up a potential approach to mitigate unwanted or illegal blockchain content [11]. Here, a single blockchain maintainer or a small group of maintainers can retrospectively revert single transactions, e.g., due to illegal content. To overcome arising trust issues, μchain [51] leverages the consensus approach of traditional blockchains to vote on alterations of the blockchain history. As these approaches tackle unwanted content for newly designed blockchains, we seek to motivate a discussion on countermeasures also for *existing* systems, e.g., Bitcoin.

6 Conclusion

The possibility to store non-financial data on cryptocurrency blockchains is both beneficial and threating for its users. Although controlled channels to insert non-financial data at small rates opens up a field of new applications such as digital notary services, rights management, or non-equivocation systems, objectionable or even illegal content has the potential to jeopardize a whole cryptocurrency. Although court rulings do not yet exist, legislative texts from countries such as Germany, the UK, or the USA suggest that illegal content such as child pornography can make the blockchain illegal to possess for all users.

As we have shown in this paper, a plethora of fundamentally different methods to store non-financial–potentially objectionable–content on the blockchain exists in Bitcoin. As of now, this can affect at least 112 countries in which possessing content such as child pornography is illegal. This especially endangers the multi-billion dollar markets powering cryptocurrencies such as Bitcoin.

To assess this problem's severity, we comprehensively analyzed the *quantity* and *quality* of non-financial blockchain data in Bitcoin today. Our quantitative analysis shows that 1.4 % of the roughly 251 million transactions in Bitcoin's blockchain carry arbitrary data. We could retrieve over 1600 files, with new content infrequently being added. Despite a majority of arguably harmless content, we also identify different categories of objectionable content. The harmful potential of *single instances* of objectionable blockchain content is already showcased by findings such as links to illegal pornography or serious privacy violations.

Acknowledgements

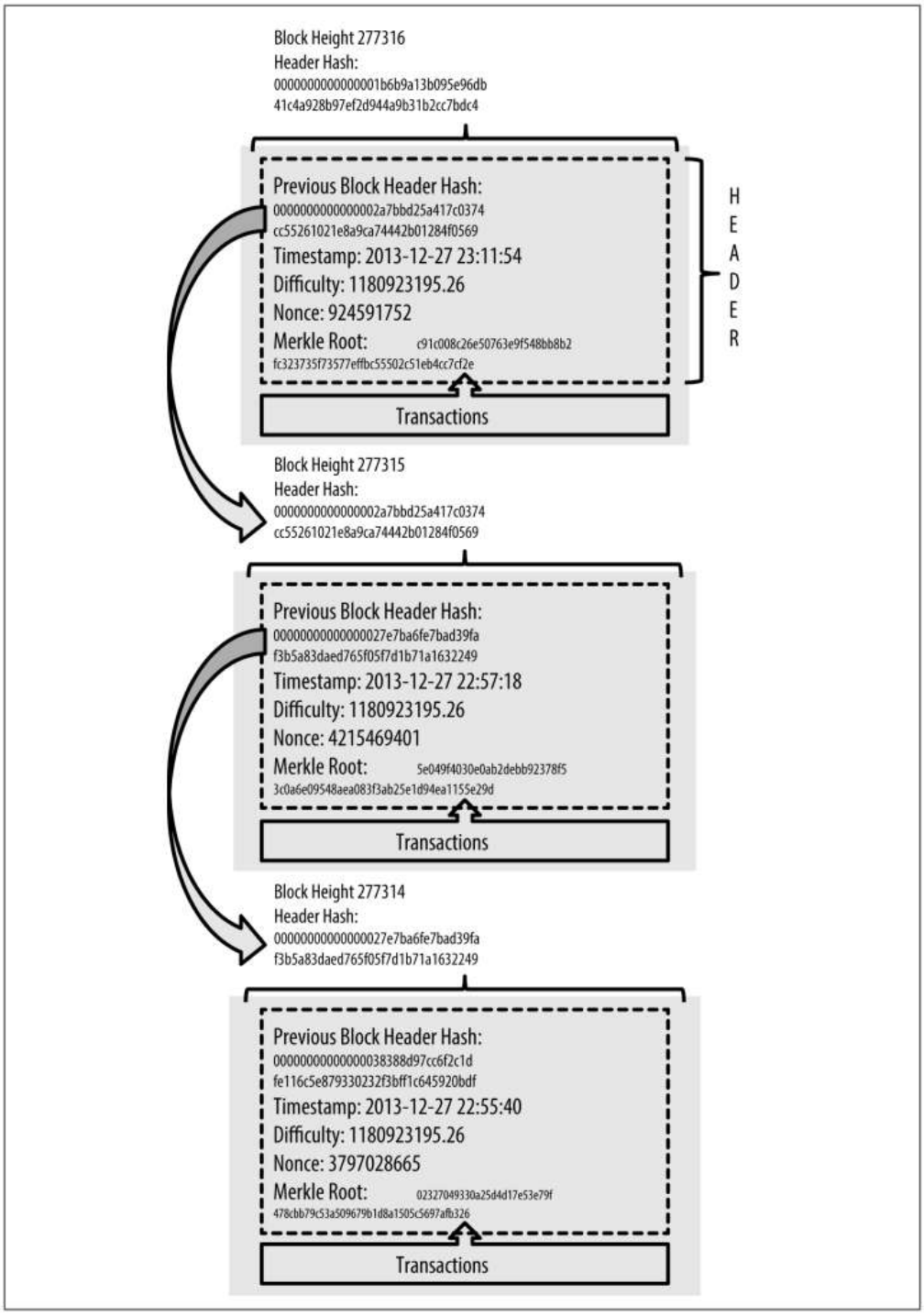
This work has been funded by the German Federal Ministry of Education and Research (BMBF) under funding reference number 16KIS0443. The responsibility for the content of this publication lies with the authors.

References

1. German Criminal Code, Section 11 (2013)
2. German Criminal Code, Sections 184b and 184c (2013)
3. Protection of Children Act, Chapter 37, Section 7 (2015)
4. Bitcoin Transaction Fees. `https://bitcoinfees.info` (2016) Accessed 09/23/2017.
5. General Data Protection Regulation, Section 24 (2016)
6. Aberer, K., Despotovic, Z.: Managing Trust in a Peer-2-Peer Information System. In: ACM CIKM. (2001) pp. 310–317
7. Adya, A., Bolosky, W.J., Castro, M., Cermak, G., Chaiken, R., Douceur, J.R., Howell, J., Lorch, J.R., Theimer, M., Wattenhofer, R.P.: FARSITE: Federated, Available, and Reliable Storage for an Incompletely Trusted Environment. SIGOPS Oper. Syst. Rev. **36**(SI) (2002) pp. 1–14
8. Ali, M., Shea, R., Nelson, J., Freedman, M.J.: Blockstack: A New Decentralized Internet. (2017) Accessed 09/23/2017.

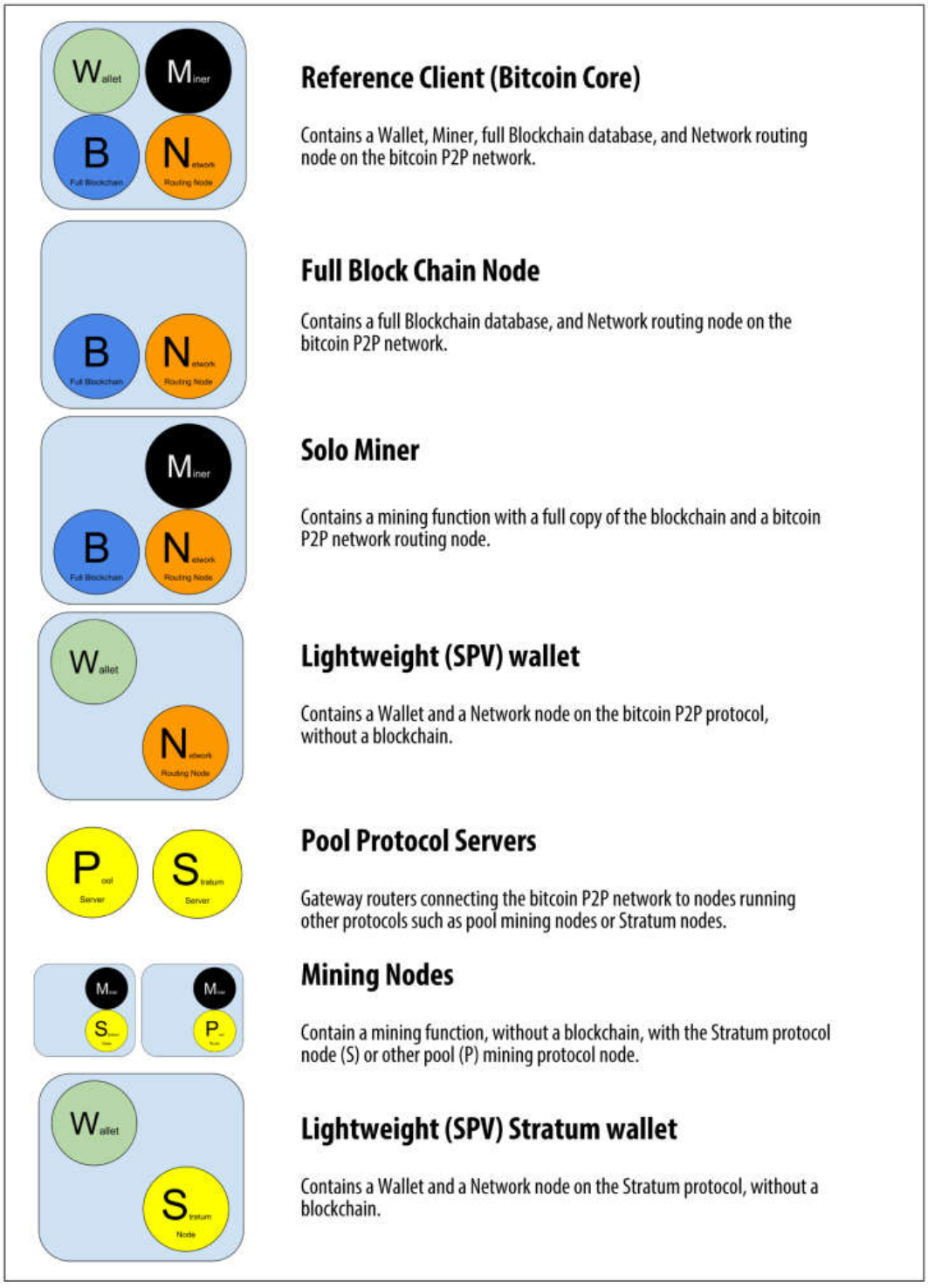
54. Scheller, S.H.: A Picture Is Worth a Thousand Words: The Legal Implications of Revenge Porn. North Carolina Law Review **93**(2) (2015) pp. 551–595
55. Selcuk, A.A., Uzun, E., Pariente, M.R.: A Reputation-based Trust Management System for P2P Networks. In: IEEE CCGrid. (2004) pp. 251–258
56. Shirriff, K.: Hidden surprises in the Bitcoin blockchain and how they are stored: Nelson Mandela, Wikileaks, photos, and Python software. http://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html (2014) Accessed 09/23/2017.
57. Sleiman, M.D., Lauf, A.P., Yampolskiy, R.: Bitcoin message: Data insertion on a proof-of-work cryptocurrency system. In: ACM CW. (2015) pp. 332–336
58. Snow, P., Deery, B., Lu, J., Johnston, D., Kirby, P.: Factom: Business Processes Secured by Immutable Audit Trails on the Blockchain. https://www.factom.com/devs/docs/guide/factom-white-paper-1-0 (2014) Accessed 09/23/2017.
59. Spagnuolo, M., Maggi, F., Zanero, S.: BitIodine: Extracting Intelligence from the Bitcoin Network. In: FC. (2014) pp. 457–468
60. Standing Committee of the National People's Congress: Law of the People's Republic of China on Guarding State Secrets. (1989) Accessed 09/23/2017.
61. Taylor, G.: Concepts of Intention in German Criminal Law. Oxford Journal of Legal Studies **24**(1) (2004) pp. 99–127
62. Tomescu, A., Devadas, S.: Catena: Efficient non-equivocation via bitcoin. In: IEEE S&P. (2017) pp. 393–409
63. Tucker, E.: A Look at Federal Cases on Handling Classified Information. http://www.military.com/daily-news/2016/01/30/a-look-at-federal-cases-on-handling-classified-information.html (2016) Accessed 09/23/2017.
64. United Nations: Appendix to the Optional protocols to the Convention on the Rights of the Child on the involvement of children in armed conflict and on the sale of children, child prostitution and child pornography (2000)
65. United Nations: Optional protocols to the Convention on the Rights of the Child on the involvement of children in armed conflict and on the sale of children, child prostitution and child pornography. **2171** (2000) pp. 247–254
66. Waldman, M., Rubin, A.D., Cranor, L.: Publius: A Robust, Tamper-Evident, Censorship-Resistant and Source-Anonymous Web Publishing System. In: USENIX Security. (2000) pp. 59–72
67. Walsh, K., Sirer, E.G.: Experience with an Object Reputation System for Peer-to-peer Filesharing. In: NSDI. (2006)
68. Wei, W.: Ancient 'STONED' Virus Signatures found in Bitcoin Blockchain. https://thehackernews.com/2014/05/microsoft-security-essential-found.html (2014) Accessed 09/23/2017.
69. Wood, G.: Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper (2016) Accessed 09/23/2017.
70. Zeilinger, M.: Digital art as 'monetised graphics': Enforcing intellectual property on the blockchain. Philosophy & Technology (2016)
71. Ziegeldorf, J.H., Grossmann, F., Henze, M., Inden, N., Wehrle, K.: CoinParty: Secure Multi-Party Mixing of Bitcoins. In: ACM CODASPY. (2015) pp. 75–86
72. Ziegeldorf, J.H., Matzutt, R., Henze, M., Grossmann, F., Wehrle, K.: Secure and Anonymous Decentralized Bitcoin Mixing. FGCS **80** (3 2018) 448–466
73. Zimmermann, T., Rüth, J., Wirtz, H., Wehrle, K.: Maintaining Integrity and Reputation in Content Offloading. In: IEEE/IFIP WONS. (2016) pp. 1–8

ANEXO B – ESTRUTURA CONCEITUAL DO BLOCKCHAIN



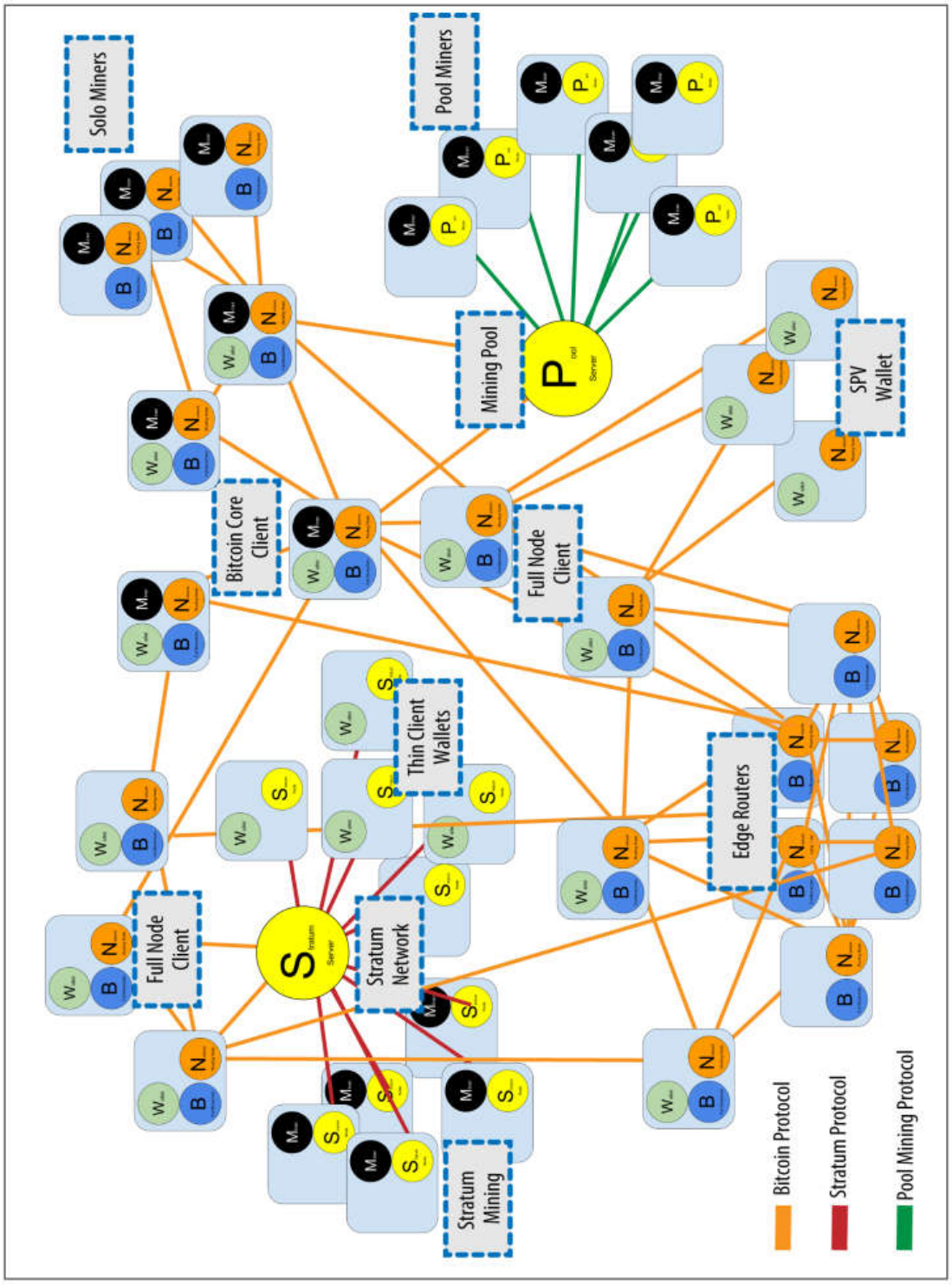
Fonte: Mastering Bitcoin, 2014, p.111.

ANEXO C – TIPOS DE USUÁRIOS DA REDE BITCOIN



Fonte: Mastering Bitcoin, 2014, p.140.

ANEXO D – REPRESENTAÇÃO CONCEITUAL DA REDE BITCOIN



Fonte: Mastering Bitcoin, 2014, p.141.