Em Questão
ISSN: 1807-8893
ISSN: 1808-5245
emquestao@ufrgs.br
Universidade Federal do Rio Grande do Sul
Brasil

Um estudo da Blockchain aplicado ao contexto dos Dados de Pesquisa

Ouchi, Marcos Teruo; Arakaki, Ana Carolina Simionato
Um estudo da Blockchain aplicado ao contexto dos Dados de Pesquisa
Em Questão, vol. 26, núm. 3, 2020
Universidade Federal do Rio Grande do Sul, Brasil
Disponível em: https://www.redalyc.org/articulo.oa?id=465664724004
DOI: https://doi.org/10.19132/1808-5245263.70-93

Um estudo da Blockchain aplicado ao contexto dos Dados de Pesquisa

Blockchain study applied to the context of Scientific Research Data

Marcos Teruo Ouchi 1
Universidade Federal de São Carlos, Brasil
ouchi@isci.com.br

Ana Carolina Simionato Arakaki 2
Universidade Federal de São Carlos, Brasil
acsimionato@ufscar.br

DOI: https://doi.org/10.19132/1808-5245263.70-93
Redalyc: https://www.redalyc.org/articulo.oa?id=465664724004

Recepção: 19 Novembro 2019
Aprovação: 28 Janeiro 2020

Resumo:

Os dados coletados durante as pesquisas são essenciais, pois o resultado obtido deve ser o produto de sua rigorosa análise. Nesse escopo e associada a mecanismos de consenso distribuído, a estrutura de dados *Blockchain* pode garantir a confiabilidade dos dados de forma transparente, descentralizada e imutável, e surge como possibilidade para contribuir para o progresso da Ciência por meio de novas maneiras de tratamento das grandes quantidades de dados coletados em uma pesquisa científica. Neste sentido, o objetivo geral desse trabalho consiste em analisar a tecnologia *Blockchain* e suas possibilidades inseridas à Comunicação Científica e na Gestão de Dados de Pesquisa. Os objetivos específicos são conceituar dados de pesquisa; identificar os principais conceitos, a estrutura e o funcionamento, relacionados à tecnologia *Blockchain*; e apontar a tecnologia *Blockchain* e suas potenciais aplicações na Ciência. Trata-se de uma pesquisa exploratória e teórica de caráter qualitativo. Os resultados apresentam o levantamento realizado sobre a Comunicação Científica e sua relação com a Ciência da Informação, incidindo na importância da gestão de dados e os metadados para a descrição dos conjuntos de dados de pesquisa, e o seu impacto com o *Blockchain*. Considera-se prematuro afirmarmos que a *Blockchain*, em seus estágios atuais, resolverá os problemas relacionados à crise de reprodutibilidade. No curto prazo a *Blockchain* provavelmente seja aplicada a pontos específicos no fluxo de uma pesquisa científica ajudando a dirimir a desconfiança nos dados e nas metodologias utilizadas.

Palavras-chave: Dados científicos, Gestão dos dados de pesquisa, Blockchain.

Abstract:

The data collected during the research is essential, because the result obtained must be the product of its rigorous analysis. In this scope and associated with distributed consensus mechanisms, the Blockchain data structure can ensure data reliability in a transparent, decentralized and unchanging manner, and emerges as a possibility to contribute to the progress of science through new ways of treating large quantities. of data collected in a scientific research. In this sense, the general objective of this work is to analyze Blockchain technology and its possibilities inserted to Scientific Communication and Research Data Management. The specific objectives are to conceptualize research data; identify key concepts, structure and operation related to Blockchain technology; and point to Blockchain technology and its potential applications in science. It is an exploratory and theoretical research of qualitative character. The results present the survey conducted on Scientific Communication and its relationship with Information Science, focusing on the importance of data management and metadata for the description of research data sets, and their impact with Blockchain. It is considered premature to state that Blockchain, in its current stages, will solve problems related to the reproducibility crisis. In the short term, Blockchain is likely to be applied to specific points in the flow of scientific research, helping to dispel distrust in the data and methodologies used.

Keywords: Scientific data, Management of scientific data, Blockchain.

Autor notes

1 Mestre; Universidade Federal de São Carlos, São Carlos, SP, Brasil
ouchi@isci.com.br

2 Doutora; Universidade Federal de São Carlos, São Carlos, SP, Brasil
acsimionato@ufscar.br

1 Introdução

Ao definir a Ciência como o "Conhecimento Público", Ziman (1979, p. 24) nos esclarece que o objetivo da Ciência é mais do que obter informações, mas alcançar um consenso de opinião racional entre o pesquisador e seus pares, então, não podemos nos limitar a conceituar a Ciência apenas como "[...] uma questão de sequência de gênios a realizarem uma sequência de importantes descobertas." (PRICE, 1976, p. 93).

A Ciência avança com base no conhecimento adquirido em estudos prévios e a confiabilidade e reprodutibilidade dos resultados constituem pilares da pesquisa científica. (GIBB, 2014; MCNUTT, 2014; NASSI-CALÒ, 2017). Assim, uma pesquisa,

> [...] têm de passar por um crivo, por uma fase de análises críticas e de provas, realizadas por outros indivíduos competentes e desinteressados, os quais deverão determinar se eles são bastante convincentes para que possam ser universalmente aceitos. (ZIMAN, 1979, p. 24).

Peng (2011), portanto, argumenta que a reprodutibilidade de uma pesquisa "[...] tem o potencial de servir como um padrão mínimo para julgar alegações científicas quando a replicação independente completa de um estudo não é possível." (PENG, 2011, p. 1226).

A título de exemplo, em uma pesquisa realizada com 1.576 pesquisadores publicada pela Revista *Nature* no ano de 2016, revelou que mais de 70% dos pesquisadores não obtiveram sucesso em reproduzir experimentos de outros cientistas e mais da metade não conseguiram reproduzir seus próprios experimentos. Esses e outros casos contribuem para que a preocupação com a reprodutibilidade da pesquisa científica aumente "[...] constantemente com relatos de que os resultados de experimentos em vários domínios da Ciência não poderiam ser replicados." (GOODMAN; FANELLI; IOANNIDIS, 2016, p. 1).

Para Mayer e Zeviani (2016) o ato de reproduzir uma pesquisa significa possibilitar que outros cientistas, de áreas e pensamentos distintos e independentemente, possam obter acesso aos dados e aos métodos da pesquisa original, inclusive aos códigos computacionais, tornando-se uma alternativa entre replicar uma pesquisa e nada fazer.

A *Blockchain*, sendo uma estrutura de dados distribuída (livro-razão, do inglês *ledger*), contém dados de transações, registrados e posteriormente armazenados como blocos ligados a outros blocos - como uma corrente - de forma que esses registros se tornam invioláveis e atualizáveis apenas por consenso ou acordo entre pares (ANTONOPOULOS, 2014; BASHIR, 2017; ROUSE, 2017), permitindo "[...] ser auditado a qualquer momento [...]" (OLIVEIRA; SANTARÉM SEGUNDO, 2018, p. 5371), com características singulares, que prometem atribuir a confiabilidade desejável aos dados e conjuntos de dados de forma transparente, descentralizada e imutável, nos promete vislumbrar nela a possibilidade de sua utilização no armazenamento de dados de pesquisa científicas coletados por pesquisadores que, atualmente os mantêm "[...] armazenados localmente em seus computadores, em algum meio digital de armazenamento ou em repositórios dos laboratórios de pesquisa." (CRUZ *et al.*, 2018, p. 2776).

Este trabalho, portanto, busca investigar e responder a seguinte questão de pesquisa: **quais são os benefícios da aplicação da Blockchain no contexto dos Dados de Pesquisas Científicas?**

Trata-se de uma pesquisa exploratória e teórica de caráter qualitativo, que aborda os temas de: comunicação científica, *Blockchain*, curadoria de dados de pesquisa, ciclo de vida de dados de pesquisa, reprodutibilidade da pesquisa, ciência aberta e metadados.

Quanto à pesquisa exploratória, esta proporcionou uma "[...] maior familiaridade com o problema, com vistas a torná-lo mais explícito ou construir hipóteses." (GIL, 2002, p. 41). A análise exploratória e descritiva da literatura disponível sobre o tema proposto, permitiu a construção de um conhecimento teórico sobre as práticas de comunicação científica, curadoria digital, proposições e abordagens de Ciclo de Vida de Dados, definição e construção de metadados e padrões de metadados, utilização de tecnologias em pesquisas na Ciência, além claro, da *Blockchain*.

Para a contextualização teórica foram utilizadas as fontes bibliográficas e documentais como fundamentação para os resultados, por essa razão, a pesquisa refere-se a uma pesquisa bibliográfica e documental. Gil (2002, p. 44) conceitua que "A pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos." e a pesquisa documental, para ele, diferencia-se pela natureza das fontes que, no caso, "[...] vale-se de materiais que não recebem ainda um tratamento analítico, ou que ainda podem ser reelaborados de acordo com os objetos da pesquisa." (GIL, 2002, p. 45).

O recorte bibliográfico sobre os temas desta pesquisa foi realizado pelos idiomas português, espanhol e inglês, no período de 2010 a 2019. O recorte temporal foi definido tendo em consideração a concentração bibliográfica publicada sobre os temas desta pesquisa e do período em que ocorreu o surgimento do assunto principal, qual seja, a *Blockchain*, que foi apresentada publicamente em um artigo científico no ano de 2008 e tendo sua efetiva implementação e adoção em 2010 gerando, à partir de então, publicações que consideramos relevantes para o presente estudo, no entanto, alguns trabalhos clássicos ou de relevância histórica para a pesquisa foram citados.

Durante a pesquisa foram utilizadas as bases de dados: Biblioteca Digital Brasileira de Teses e Dissertações (BDTD); Base de Dados Referenciais de Artigos de Periódicos em Ciência da Informação (BRAPCI); *Library and Information Science Abstracts* (LISA); Portal de Periódicos da CAPES; *Scientific Electronic Library Online* (SciELO), *Scopus*, e *Web of Science*. Além de outras fontes de informação como o Repositório Institucional da Universidade Federal de São Carlos (UFSCar), postagens em blogs, artigos em revistas e sites institucionais, anais de eventos científicos e *white papers* de instituições públicas e privadas.

2 Dados de pesquisa

Os dados de pesquisa são cruciais, pois provêm evidências para o conhecimento científico publicado, base de evidências para os resultados de pesquisas e que são a fundação para todo o progresso científico. (MOLLOY, 2011; INGRAM, 2016). São, portanto, essenciais, não apenas para o desenvolvimento, mas também para estabelecer a validade, replicação e reprodução da pesquisa, neste sentido, tornando-se um valioso produto da pesquisa.

Santos e Sant'Ana (2013, p. 205) definem o termo dado como "[...] uma unidade de conteúdo necessariamente relacionada a determinado contexto e composta pela tríade entidade, atributo e valor [...]", sendo que neste trabalho utilizaremos o termo dado como o "[...] elemento básico nos fluxos informacionais [...]" (SANTOS; SANTANA, 2013, p. 201).

Nos termos da *Organisation for Economic Cooperation and Development* (OECD), o termo "dado de pesquisa" é definido como:

> [...] registros factuais (pontuações numéricas, registros textuais, imagens e sons) usados como fontes primárias para pesquisa científica, e que são comumente aceitos na comunidade científica como necessários para validar resultados da pesquisa. Um conjunto de dados de pesquisa constitui uma representação parcial e sistemática do assunto investigado. (OECD, 2007, p. 13).

Ingram (2016) define dados de pesquisa como "[...] todas as informações que foram coletadas, observadas, geradas ou criadas para validar os resultados da pesquisa original [...]", incluindo "[...] formatos não digitais, como cadernos de laboratório e cadernos de esboços." (INGRAM, 2016).

Considerando que os "[...] dados de pesquisa são os dados produzidos ou utilizados para o desenvolvimento de uma pesquisa." (COSTA, 2017, p. 15), para Fernandes e Ribeiro (2011, p. 3) concluem que "[...] os dados produzidos em contexto de investigação são reconhecidamente de grande valor.". Complementa-se ainda pela citação de Simmons, Nelson e Simonsohn (2011, p. 1359) "Nosso trabalho como cientistas é descobrir

verdades sobre o mundo. Nós geramos hipóteses, coletamos dados e examinamos se os dados são ou não consistentes com essas hipóteses.").

As decisões a serem tomadas por um pesquisador no decorrer da coleta e da análise de dados de suas pesquisas são muitas. Escolher quais e que tipos de dados devem ser coletados, em que quantidade e frequência, quais variáveis de controle devem ser consideradas, quais condições devem ser combinadas ou comparadas, se devo excluir e qual parte delas, são raras e "[...] às vezes impraticável, que os pesquisadores tomem todas essas decisões de antemão." (SIMMONS; NELSON; SIMONSOHN, 2011, p. 1359). Ou mesmo, "[...] é comum (e prática aceita) que os pesquisadores explorem várias alternativas analíticas, busquem uma combinação que produza 'significância estatística' e, então, relatem apenas o que 'funcionou'." (SIMMONS; NELSON; SIMONSOHN, 2011, p. 1359).

Neste sentido, o tratamento dos Dados de Pesquisa depende, segundo Ingram (2016), do tipo de dados envolvidos, como são criados ou coletados e como devem ser usados no presente e no futuro.

No caso específico das informações científicas, "[...] a importância do registro e arquivamento dos dados produzidos durante a pesquisa é fundamental." (MÁRDERO-ARELLANO, 2008, p. 23), pois "[...] quaisquer resultados ou dados de pesquisa podem ser usados para evidenciar descobertas publicadas ou podem ser combinados com outros dados para produzir novos tipos de registro de dados." (INGRAM, 2016, *on-line*).

3 BLOCKCHAIN

Criada e publicada por um autor cujo pseudônimo, Satoshi Nakamoto em um artigo de nove páginas cujo título *Bitcoin*: *A Peer-to-Peer Electronic Cash System*, não deixava transparecer a verdadeira revolução a que estava destinada a causar. Bartling et al. (2017) atribuem à sua natureza descentralizada, distribuída, imutável e transparente as características singulares que os dados na *Blockchain* adquirem, sendo armazenados sem ambiguidades e de forma transparente, permitindo-se assim que auditorias sejam realizadas.

A estrutura tecnológica básica de uma rede *Blockchain* é composta por uma rede ponto a ponto (P2P) e uma estrutura de dados distribuída. Uma rede ponto a ponto é um conjunto de computadores, que compartilham recursos e tarefas, sem a necessidade de um controle centralizado – ao contrário de uma rede que contenha servidores - onde cada computador é denominado um "nó" desta rede.

Cada um desses 'nós' pode armazenar uma cópia exata de todos os dados das transações realizadas, então, quando um novo 'nó' é adicionado, ele pode receber uma cópia dos dados armazenados em outros nós, garantindo que quando o inverso acontece, não haja impactos na rede.

Em sua concepção inicial, para que uma transação seja realizada na *Blockchain*, por exemplo da Bitcoin, cada parte envolvida possui duas chaves, uma pública e uma privada (secreta). Podemos entender a primeira como um endereço público e a segunda um meio de autenticação. "Imagine que a Chave Pública é similar ao número de uma conta bancária e a Chave Privada similar a um PIN secreto ou uma assinatura em um cheque que provê controle sobre a conta." (ANTONOPOULOS, 2014, p. 1).

Desta forma, em uma estrutura centralizada ou descentralizada, há a necessidade de um ou mais agentes que realizam as validações de uma ou mais transações, enquanto que, em uma estrutura descentralizada, todos ou pelo menos um número escolhido por consenso de 'nós' desta rede possui a autonomia de validar essa transação por meio do atendimento de pré-requisitos acordados, processados e registrados por cada um desses nós, como ilustrado na Figura 1.

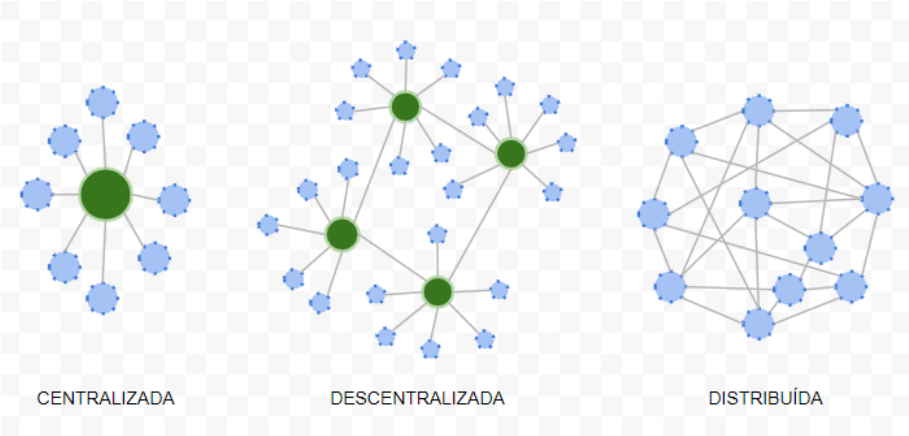

FIGURA 1
Sistema centralizado, descentralizado e distribuído
Fonte: Elaborado pelos autores.

Nesse sentido, Bartling *et al*. (2017, p. 5) destacam que

> Hoje, o proprietário (ou pesquisador, editor acadêmico, repositório de dados, etc.) tem controle total sobre o computador, os dados e os serviços que executa (por exemplo, um banco de dados) e pode tecnicamente alterar o conteúdo de maneiras arbitrárias. Após a revolução do *Blockchain*, esse não é mais o caso, já que os sistemas de fornecimento de confiança descentralizados fornecem "poder criptográfico" para garantir a integridade de um serviço de computador e a autenticidade do banco de dados subjacente.

Sendo assim, a *Blockchain* é considerada como "[...] um livro-razão compartilhado distribuído." (BASHIR, 2017). Esse atributo permite uma única versão da realidade acordada entre todos as partes da rede sem a exigência de uma autoridade central e, uma vez que os dados são gravados em uma *Blockchain*, é extremamente difícil alterá-los novamente.

Da mesma forma, a transparência estabelece que todos podem ver o conteúdo da *Blockchain*. Sendo compartilhado, o sistema se torna transparente. Essas propriedades podem ser percebidas facilmente aplicadas ao *bitcoin*.

No início da criptomoeda, um bloco gênese foi criado e serviu como o estado inicial do sistema. Ele conteve informações sobre as regras ou instruções sobre a estrutura de dados restante. Conforme as transações foram adicionadas, um novo bloco vai sendo formado e ao atender aos requisitos um novo bloco é adicionado.

Essa validação, na *bitcoin*, é realizada pelo conceito de "prova de trabalho", onde um "nó" da rede deve executar o processamento da transação e em seguida validar seu resultado com os outros "nós" da rede. Ao haver um consenso entre os resultados encontrados por esses "nós", essa transação é validada e inserida em um bloco. Esse bloco recebe uma identificação, uma assinatura que é construída criptograficamente, contendo dados do bloco adicional e do bloco anterior e que é denominada "*hash* criptográfico". Então uma "cadeia de blocos" é formada e, daí sua denominação: *Blockchain*.

A função *hash* (protocolo de transformação) são algoritmos cuja entrada se dá pela cadeia de comprimento arbitrário (uma mensagem) e cuja saída é uma cadeia de comprimento fixo (o valor *hash*), apresentando-se como "[...] um tipo de assinatura para essa mensagem" (STEVENS, 2007, p. 4).

A Figura 2 ilustra uma função *hash* em funcionamento. Note-se que independentemente do tamanho da entrada (*input*) o comprimento de saída (*digest*) é sempre o mesmo. Outro ponto de atenção é que uma pequena mudança, por exemplo, num único caractere da cadeia de entrada provoca uma saída consideravelmente diferente. As funções *hash* possuem, segundo Schneier (2004), duas propriedades vitais: a primeira é que elas são unidirecionais. Isso significa que "[...] é fácil pegar uma mensagem e calcular seu valor de *hash*, mas é impossível obter um valor de *hash* e recriar a mensagem original." (SCHNEIER, 2004, on-

line). A segunda é que funções *hash* são livres de colisão. Isso significa que "[...] é impossível encontrar duas mensagens com o mesmo valor de *hash*." (SCHNEIER, 2004, on-line).

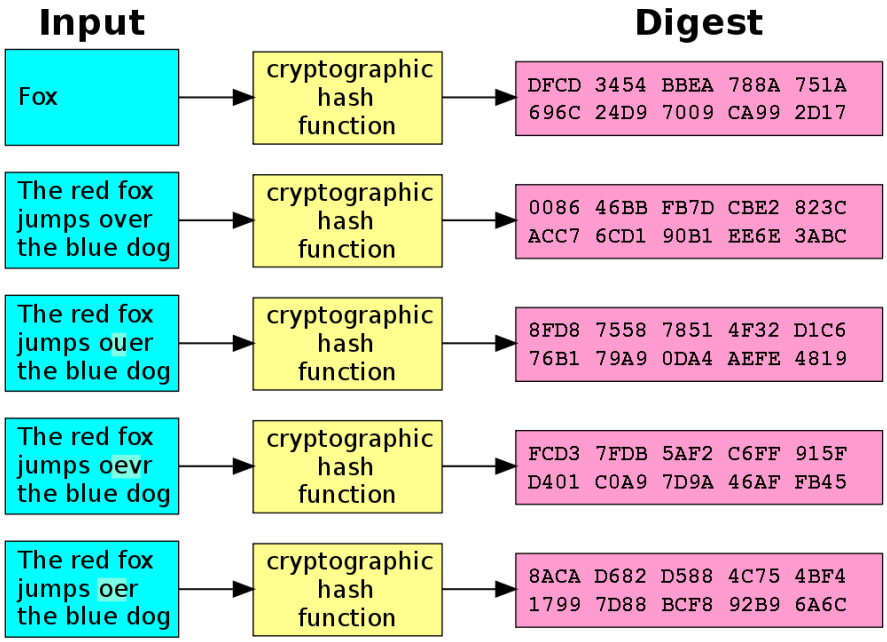

FIGURA 2
Uma função hash criptográfico em funcionamento.
Fonte: Stolfi (2008).

Christidis e Devetsikiotis (2016) ilustram a *Blockchain* como um registro sequencial de dados de transações agrupados em blocos contendo a data e hora em que cada um foi realizado.

Cada bloco é identificado por seu *hash* criptográfico e cada novo bloco faz referência ao *hash* do bloco anterior. Isso estabelece uma conexão entre os blocos, criando assim uma cadeia de blocos, ou *Blockchain*, conforme ilustrado na Figura 3:

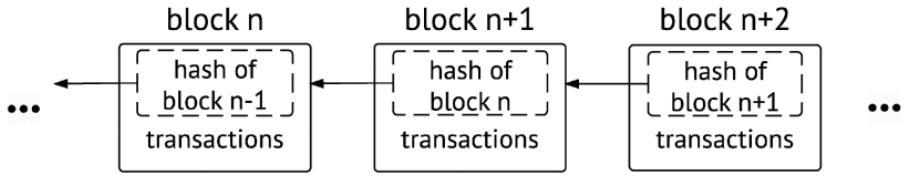

FIGURA 3
A *Blockchain* representada graficamente
Fonte: Bartling *et al.* (2017).

Qualquer nó da rede, com acesso a essa lista de blocos ordenados e vinculados poderá lê-lo e descobrir qual é o estado global dos dados que estão sendo transacionados. Em geral, a estrutura de um bloco na *Blockchain*, como por exemplo, o da Bitcoin tem duas partes, conforme ilustrado na Figura 4.

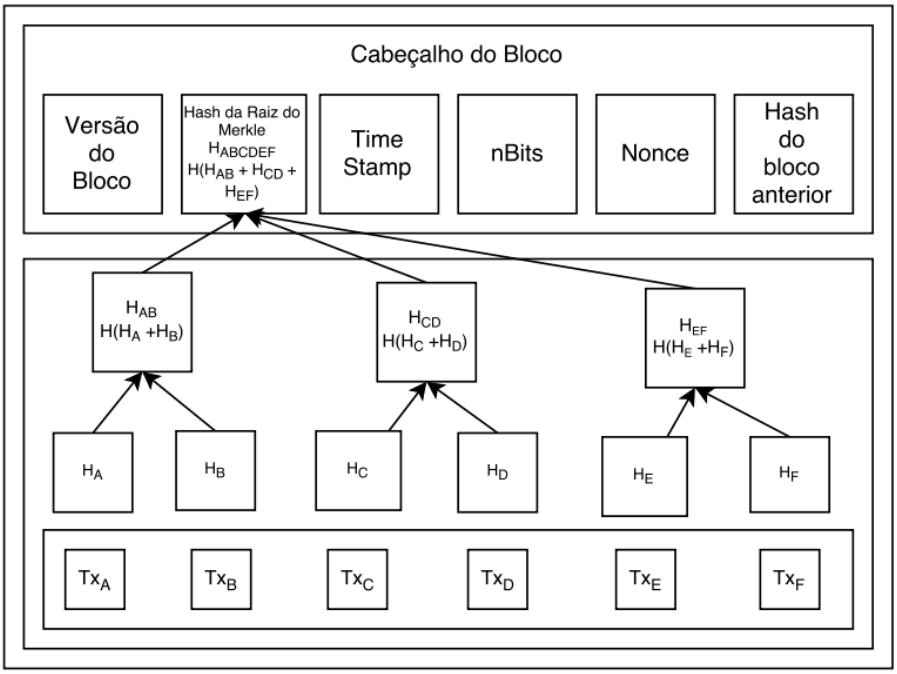

FIGURA 4
Estrutura da bitcoin
Fonte: Aliaga e Henriques (2017).

Como visto na Figura 4, a primeira parte, seu cabeçalho, é composta de metadados que indicam as regras de validação dos blocos (Versão), a *hash* que representa todas as transações (*Hash* Raiz da Árvore de Merkle[1]), a hora universal em que o bloco foi criado (*TimeStamp*), o indicativo de dificuldade para realização da mineração (*Nbits*), o valor arbitrário usado na mineração para se produzir o *hash* do desafio (*Nonce*), e o *hash* do bloco anterior que é usado no cálculo do hash de desafio. A segunda parte, o Corpo do Bloco, com o conteúdo propriamente dito, incorpora a Árvore de Merkle das transações e as transações propriamente ditas.

Tais características, acrescida da capacidade de interpretação de regras de negócios, têm possibilitado o uso da *Blockchain* em quaisquer outras aplicações onde partes desejam realizar transações automaticamente, sem a necessidade de intermediários.

> O que é necessário é um sistema de pagamento eletrônico baseado em prova criptográfica em vez de confiança, permitindo que duas partes interessadas negociem diretamente entre si sem a necessidade de uma terceira parte confiável. (NAKAMOTO, 2008, *on-line*).

Basicamente, a *Blockchain* resolve um dos grandes problemas relacionados a sistemas distribuídos. Conhecido como o Problema dos Generais Bizantinos (*Byzantine Generals Problem – BGP*), que consiste em "[...] tentar tomar uma decisão através do intercâmbio de informações sobre uma rede pouco confiável e potencialmente comprometida." (ANTONOPOULOS, 2014, p. 30). Esses mecanismos devem permitir que partes desconhecidas cheguem a um consenso sobre o estado dos dados armazenados em uma *Blockchain*.

O consenso é um processo de concordância entre nós desconfiados em um estado final de dados. "A chave para o funcionamento da cadeia de blocos é que a rede deve concordar coletivamente sobre o conteúdo do livro-razão" (KOSTAREV, 2017, p. 17). Para alcançar consenso, diferentes algoritmos podem ser usados. É fácil chegar a um acordo entre dois nós (por exemplo, em sistemas cliente-servidor), mas quando vários nós participam de um sistema distribuído e precisam concordar em um único valor, torna-se muito difícil chegar a um consenso. Esse conceito de alcançar consenso entre vários nós é conhecido como consenso distribuído (BASHIR, 2017).

O Algoritmo de Prova de Trabalho ou *The Proof-of-Work* (POW) em inglês é, sem dúvida, o mecanismo de consenso mais conhecido, em decorrência do pioneirismo e aceitação da criptomoeda *Bitcoin*. Bashir (2017) explica que este mecanismo depende da prova de que recursos computacionais suficientes foram gastos antes de propor um valor para aceitação pela rede. Nesse sentido, "Os computadores competem para encontrar um *hash* com propriedades específicas." (KOSTAREV, 2017, p. 10). Esse processo é conhecido como "mineração". Segundo (MATOS, 2018), o algoritmo adiciona um número arbitrário chamado "*nonce*" ao final do bloco e exige que o minerador encontre um valor que, adicionado aos dados do bloco e ao conteúdo das novas transações, seja gerado um *hash* com uma determinada quantidade de números zeros em seu início. A POW garante o consenso na rede por meio da solução deste problema criptográfico. Quando esse problema é resolvido, um novo bloco na *Blockchain* é criado. Esse bloco é então transmitido a todos os outros nós que armazenam uma cópia completa da *Blockchain* e verificam individualmente sua validade. À medida que um bloco é adicionado, a dificuldade para modificar dados de blocos anteriores vai aumentando, pois, o esforço para mudar um bloco exige a mudança de todos os blocos posteriores. E isso exige um grande poder computacional para resolver o algoritmo de cada um desses blocos. Por esse motivo, a cadeia considerada válida é sempre a mais longa.

Almeida (2012) atribui ao direito natural e ao surgimento do capitalismo a forma como entendemos o conceito de contrato na atualidade. No princípio, buscava-se eliminar barreiras e garantir os princípios que nortearam os ideais capitalistas como a autorregulação do mercado, neste sentido, no contexto do direito contratual

> [...] a principal ideia traçada nesse período era a da liberdade de contratar. [...]. Não era dado ao Estado impor às partes um determinado tipo de contrato ou a contratar com determinado parceiro contratual. (ALMEIDA, 2012, p. 1-3).

Com o passar do tempo os contratos "[...] passam a ser uma forma de opressão para os economicamente mais fracos" (ALMEIDA, 2012, p. 3) forçando o Estado a passar "[...] a dirigir os contratos para que esses mantenham o equilíbrio. Passa-se a admitir a revisão de um contrato que passasse a ser desequilibrado" (ALMEIDA, 2012, p. 3), assim, o contrato

> [...] continua fazendo lei entre as partes, mas com respeito à dignidade da pessoa humana e de todas as normas de ordem pública que o capacitam a ser instrumento de circulação de riquezas, mas destinado a ser um instrumento mais democrático e justo do direito privado. (LEITE, 2007, *on-line*).

Assim, surge a figura do terceiro confiável como entidade mediadora aceita pelas partes de um contrato e que vem sendo o alicerce de todas as atividades envolvendo relações, em especial, as econômicas. Esta situação prevalece ainda hoje, entretanto com o surgimento de tecnologias como os Contratos Inteligentes temos novamente amplas possibilidades.

O conceito de Contrato Inteligente foi formulado por Nick Szabo (1997), definindo-o como "[...] um protocolo de transação informatizado que executa os termos de um contrato." (SZABO, 1997, p. 15). A ideia básica por trás dos contratos inteligentes é que muitos tipos de cláusulas contratuais "[...] podem ser incorporados no *hardware* e *software* com os quais lidamos, de modo que violar o contrato seja proibitivamente caro para o infrator" (SZABO, 1997, p. 15).

Não é um conceito novo. Szabo (1997) ilustra o conceito utilizando como exemplo uma máquina de venda automática (*vending machine*) que, para ele pode ser considerada a ancestral dos Contratos Inteligentes.

> Dentro de uma quantidade limitada de possibilidade de perda (o valor disponível no caixa deve ser menor do que o custo de romper o mecanismo), a máquina recebe moedas e, por meio de um mecanismo simples, que cria um problema de informática no projeto com autômatos finitos, entrega o produto de acordo com o preço exibido. A máquina de venda automática é um contrato com o portador: qualquer pessoa com moedas pode participar de uma troca com o vendedor. O cofre e outros mecanismos de segurança protegem as moedas e o conteúdo armazenados dos invasores, o suficiente para permitir a implantação lucrativa de máquinas de venda automática em uma ampla variedade de áreas. (SZABO, 1997, *on-line*).

Evidentemente que Szabo (1997) esclarece que os Contratos Inteligentes vão muito além das possibilidades de uma máquina automática de vendas, apresentando vários exemplos hipotéticos de aplicação para automóveis, como: segurança, transferência de propriedade, garantia de crédito, locação, arrendamento, etc.

Com o surgimento da *Blockchain*, dos Mecanismos de Consenso e dos Contratos Inteligentes que são tecnologias que, no âmbito jurídico, devem "[...] transformar a resolução de disputas [...]" (HOGEMANN, 2018, p. 111), não restando dúvidas de que a combinação de tecnologia *Blockchain* aos contratos inteligentes estão "[...] afetando os pressupostos, doutrinas e conceitos legais tradicionais." (HOGEMANN, 2018, p. 109), ao ponto em que "[...] os algoritmos substituirão os juízes em alguns casos, com documentos escritos em código legível por máquina, como contratos inteligentes auto impositivos" (HOGEMANN, 2018, p. 111).

Ao menos, em teoria e até o presente momento, Contratos Inteligentes são muito eficazes como "[...] instrumentos portadores digitais em plataformas descentralizadas como o *Bitcoin*." (SONG, 2018, *on-line*), mas problemáticos quando há a necessidade de, por exemplo, vincular um ativo digital a um ativo físico (tokenização),

> [...] seja frutas, carros ou casas, pelo menos em um contexto descentralizado. Os ativos físicos são regulados pela jurisdição em que você se encontra e isso significa que eles estão, de certo modo, confiando em algo além do contrato inteligente que você criou. (SONG, 2018, *on-line*).

Isso não significa, portanto, que mesmo que a posse de um ativo seja transferida digitalmente, a posse física tenha sido realizada no mundo real, fazendo com que o Contrato Inteligente, neste caso, sofra "[...] do mesmo problema de confiança dos contratos normais." (SONG, 2018, *on-line*). O problema só seria resolvido se o ativo físico (*hardware*) em questão fosse ou tivesse incorporado em um Contrato Inteligente. Isso seria possível se cada objeto se tornasse um dispositivo conectado (IoT) ao mesmo sistema que executaria o contrato inteligente, facultando, por exemplo, o acionamento e uso do dispositivo apenas ao seu proprietário.

Em relação aos metadados da *Blockchain*, os autores Elena García-Barriocanal, Salvador Sánchez-Alonso e Miguel-Angel Sicilia (2017, p. 2) afirmam que o

> [...] *Blockchain* e as tecnologias associadas fornecem um novo tipo de plataforma para superar alguns dos problemas da atual tecnologia de depósito de dados e, portanto, sugerem aos usuários a construção de uma abordagem descentralizada para o arquivamento de recursos digitais. No entanto, a reformulação do atual sistema de arquivos, agregadores e serviços digitais requer uma consideração cuidadosa das funções dos metadados, suas propriedades desejáveis e até que ponto as diferentes tecnologias são capazes de apoiá-los. Além disso, sistemas descentralizados baseados em Blockchain não são isentos de riscos, especialmente porque são construídos em torno de sistemas de incentivos para os participantes da rede, portanto a sustentabilidade deve ser incorporada em seu design.

Nesse sentido, aponta-se a importância dos metadados e padrões de metadados na organização e representação desses dados, inclusive na tecnologia *Blockchain*. Sua importância fica mais clara quando é observado quando os requisitos que são ou não suportados pela rede *Blockchain*. Os requisitos não suportados, incluem a digitação de mídia, relacionado à capacidade de longo prazo de entender, processar e renderizar objetos digitais. O armazenamento descentralizado só é referido aos metadados ao *software* de especificações necessárias, mas isso continua a ser uma questão de preservar a capacidade de processamento que foi adicionada antes, tipicamente via emulação ou migração. (GARCÍA-BARRIOCANAL; SÁNCHEZ-ALONSO; SICILIA, 2017, p. 4). Os requisitos que são impactados por soluções descentralizadas, são percebidos por meio da indexação, e não é um recurso diretamente suportado pelas *Blockchains* públicas, assim, estes requisitos precisam de uma infraestrutura adicional para a proveniência inviolável e ainda, ocorre com referenciamento (*link*) que assume uma forma diferente se referência recursos em sistemas descentralizados. (GARCÍA-BARRIOCANAL; SÁNCHEZ-ALONSO; SICILIA, 2017, p. 4). Por fim, os requisitos que são diretamente suportados pela rede *Blockchain*, incluem os metadados de identificação, desreferenciação e prova de declaração como funções que são diretamente

suportadas por uma combinação da *Blockchain* e um sistema de arquivo descentralizado (GARCÍA-BARRIOCANAL; SÁNCHEZ-ALONSO; SICILIA, 2017, p. 4).

A partir disso, nota-se que a *Blockchain* pode atingir níveis mais altos de disponibilidade, transparência e resistência a adulterações, o que resolveria alguns dos problemas dos sistemas de metadados atuais construídos em bancos de dados convencionais e, normalmente, em sistemas presentes da *Web*.

4 A Blockchain e suas potenciais aplicações na Ciência

No campo científico, o movimento *Blockchain for Science* tem realizado diversos estudos colaborativos do uso da *Blockchain* na Ciência. O movimento possui uma denominação legal chamada *International Society of Blockchain For Science* (IBFS), que

> [...] é formada por uma ampla gama de especialistas em *Blockchain*, incluindo pesquisadores, bibliotecários, defensores de direitos, empreendedores de tecnologia, especialistas em publicação acadêmica, especialistas em comunicação e gerenciamento comunitário e economistas criptográficos. (BLOCKCHAIN FOR SCIENCE, 2018, *on-line*).

Uma vez que a *Blockchain* é um mecanismo de confiança, sua aplicação se efetivaria na adoção de uma filosofia baseada na abertura e descentralização da Ciência, permitindo a reprodução dos resultados da pesquisa de forma transparente, inclusive, com o uso de dados gerados fora do âmbito acadêmico, aumentando o impacto social do pesquisador e economizando tempo e dinheiro tanto para pesquisadores quanto para instituições de pesquisa.

Sabemos que, além do projeto, algumas agências vêm solicitando a preparação de documentos que demonstrem como os dados da pesquisa serão coletados, gerados, tratados, analisados, armazenados e compartilhados. Esse documento, denominado Plano de Gestão de Dados, do inglês *Data Management Plan* (DMP), é majoritariamente apresentado como um texto e que devem delimitar o princípio de quais dados serão gerados pelo projeto e como eles serão preservados e disponibilizados, considerando questões éticas, legais, de confidencialidade e outras (FAPESP, 2019, *on-line*).

A *Blockchain* já poderia ser utilizada neste momento. Todas as diretivas principais do projeto poderiam ser convertidas em uma *Smart Contract* que conteria parte ou até mesmo todas as cláusulas referentes a cada uma das etapas do projeto, como num contrato, com a diferença de que os termos devem ser descritos de forma a serem processados automaticamente por sistemas computacionais.

A agência pode ainda estabelecer *tokens* referentes ao projeto e repassar os valores ao grupo de pesquisa interessado por meio de criptomoedas. Isso pode garantir a transparência nas transações financeiras. Adicionalmente, o projeto poderia captar fundos para uma oferta inicial de criptomoeda (ICO).

O mais importante para o trabalho proposto seria a coleta dos dados. Vamos nos limitar a um único conjunto de dados: a temperatura da água ao longo do tempo. Esta coleta seria feita por um dispositivo eletrônico computacional (um *hardware*) que poderia conter diversos sensores, exemplarmente neste caso, um termômetro.

Esse aparelho, ligado à internet, seria considerado um dispositivo de *Internet of Things* (IoT) ou Internet das coisas. Esse dispositivo conteria um GPS e um relógio interno. O GPS informaria a exata localização e o relógio a data e hora exata da coleta. Ele seria previamente programado com as diretivas dos *Smart Contracts* que poderiam conter a frequência com que os dados seriam coletados, o volume, as condições etc. O dispositivo a partir de então seria "lacrado" e sua identificação, um endereço físico único associado ao dispositivo eletrônico de comunicação em uma rede (um MAC *Address*) por exemplo, relacionada ao projeto em questão.

Esses dados seriam enviados a uma Blockchain, cujo mecanismo de consenso poderia ser similar ao Mecanismo de Prova de Importância (*Proof of Importance - PoI*) que se baseia na "[...] ideia de que a atividade de rede produtiva, e não apenas a quantidade de moedas, deve ser recompensada." (KOSTAREV, 2017, *on-*

line). A chance de minerar um bloco levaria em consideração diversos fatores, incluindo a reputação, índices bibliométricos, altimétricos e cientométricos do minerador e o número de transações feitas para e a partir do seu endereço.

Ao serem minerados, esses dados fariam parte da *Blockchain* e tornando-se imutáveis ao longo do tempo, garantindo que os dados brutos para a análise sejam comprovadamente autênticos e teoricamente à prova de manipulações.

As consequências de um sistema como esse, permitiria o desenvolvimento de uma nova pesquisa, e assim, é possível vislumbrar impactos positivos relacionados à reprodutibilidade da pesquisa e ao reuso dos dados dessas pesquisas.

Com os dados coletados e gravados a partir de um dispositivo "lacrado" e cujos parâmetros foram configurados a partir de um *Smart Contract* que representa o projeto de pesquisa, ficará muito difícil que a pesquisa tome rumos que não os acordados no início do projeto, sem que uma nova concordância entre o pesquisador e o grupo de pesquisa e a agência financiadora. Além disso, cada alteração ficaria registrada, gerando assim um registro transparente de toda e qualquer alteração necessária ao projeto e que pode ser considerado em pesquisas de reprodutibilidade posteriores.

Essa proposta ajudaria a minimizar os riscos gerados pelas causas de não reprodutibilidade elencados no documento intitulado *Replication Studies: Improving reproducibility in the empirical sciences, da Royal Netherlands Academy of Arts and Sciences* (2018), especialmente os causados pelo projeto experimental ineficiente associado a controle de vieses falho, fraude ou fabricação de dados, omissão de resultados nulos ou análise seletiva que faz os nulos parecerem positivos, não compartilhamento de dados ou de detalhes metodológicos, escolha de variáveis que se adequam aos resultados, formulação de hipótese depois que os resultados são conhecidos, discrepância entre os resultados registrados e os publicados, sistema de financiamento à pesquisa demasiadamente competitivos e falta de recompensa para práticas que favoreçam a replicação de estudos.

5 Considerações finais

Blockchain não é apenas sobre dinheiro e a Ciência não é apenas sobre obter informações. Ambos são sobre confiança, ou melhor, sobre confiabilidade e consenso. Em Ciência buscamos consenso racional entre os pares e em *Blockchain* consenso sobre o estado de um conjunto de registros de transações.

Em ambos os casos o consenso pode ser obtido por meio de mecanismos que possam garantir transparência por todo o ciclo da pesquisa.

Assim, por seus atributos, vislumbramos na tecnologia *Blockchain* possibilidades de elevar os índices de reprodutibilidade, através de mecanismos que possam aumentar a transparência e a confiabilidade dos resultados de uma pesquisa, alcançando assim o objetivo geral da pesquisa que consiste em analisar a *Blockchain* nas iniciativas de reprodutibilidade dos resultados das pesquisas científicas.

Se replicar uma pesquisa de alta complexidade se tornou praticamente impossível, resta-nos verificar as evidências reunidas nela e é este o ponto que acreditamos mais vulnerável do atual modelo de prática científica.

É muito cedo para afirmarmos que a *Blockchain* ou qualquer uma das tecnologias em seu entorno, devido aos custos de sua implementação e em seus estágios atuais de desenvolvimento, resolverão todos os problemas relacionados à crise de reprodutibilidade. No curto prazo, o mais provável é que a *Blockchain* seja aplicada a pontos específicos dentro do fluxo de uma pesquisa científica e ajude a dirimir a desconfiança nos dados e nas metodologias utilizadas.

Assim, são nítidas as relações entre a Ciência da Informação e as temáticas relacionadas aos dados científicos e à *Blockchain*. A Ciência, e em especial, a Ciência da Informação devem contribuir melhorando

> [...] a descoberta de conhecimento através da assistência a seres humanos e seus agentes computacionais, na descoberta, acesso e integração e análise de tarefas apropriadas aos dados científicos e outros objetos digitais acadêmicos. (WILKINSON et al., 2016, p. 10).

Portanto, são inúmeras as oportunidades de pesquisas futuras relacionadas ao presente trabalho a começar pela própria implementação das tecnologias *Blockchain* e *Smart contracts* apresentadas nesta pesquisa em um protótipo funcional.

Entender que os impactos causados por esta mentalidade descentralizada e aberta geram uma série de questionamentos passíveis de pesquisa. A revisão por pares, por exemplo, apontada como uma das vinte causas de não reprodutibilidade pela *Royal Netherlands Academy of Arts and Sciences*, poderia ser aprimorada ou talvez até mesmo suprimida do processo por meio de novos modelos de revisão automatizada.

Outro aspecto a ser verificado é se a utilização de contratos inteligentes poderiam motivar o pesquisador a realizar um melhor planejamento de sua pesquisa, uma vez que cada um dos aspectos seriam firmados em acordos que seriam executados automaticamente à partir do cumprimento das condições acordadas, permitindo, inclusive o desenvolvimento de novos modelos de sistemas de reputação científica que podem ser construídos usando *Blockchain* sem um terceiro confiável.

Por outro lado, o uso de criptomoedas associadas aos smart contracts permitiriam um modelo mais justo e distribuído de recompensas de acordo com a contribuição de cada participante de uma pesquisa e, assim, o financiamento descentralizado das pesquisas talvez seja possível por meio de uma participação mais democrática no desenvolvimento de pesquisas com real interesse para a sociedade. Aspectos como a descrição dos conjuntos de dados na *Blockchain* suscitam pesquisas mais detalhadas, uma vez que uma ampla variedade de tipos de dados de pesquisa está envolvida em inúmeras áreas.

Referências

ALIAGA, Y. E. M.; HENRIQUES, M. A. A. Uma comparação de mecanismos de consenso em *Blockchain*s. *In*: Encontro dos Alunos e Docentes do Departamento de Engenharia de Computação e Automação Industrial, 10., 2017, Campinas. **Anais** [...]. Campinas: UNICAMP, 2017. 4 p.

ALMEIDA, J. E. de. A evolução histórica do conceito de contrato: em busca de um modelo democrático de contrato. **Âmbito Jurídico**, São Paulo, n. 99, abr. 2012.

ANTONOPOULOS, A. M. **Mastering Bitcoin**: Unlocking Digital Cryptocurrencies. [S. l.]: O'Reilly Media, 2014.

BARTLING, S. *et al*. *Blockchain* **for Open Science and Knowledge Creation:** a technical fix to the reproducibility crisis? [*S.l.*]: [*s.n.*], 2017.

BASHIR, I. **Mastering** *Blockchain* : deeper insights into decentralization cryptography, Bitcoin and popular Blockchain frameworks. Birmingham: Packt Publishing, 2017.

BLOCKCHAIN FOR SCIENCE. IBFS - International Society of *Blockchain* For Science. **Blockchain for Science**, Berlin, 10 may 2018. Disponível em: https://www.*Blockchain*forscience.com/ibfs-international-society-*Blockchain*-science/. Acesso em: 30 dez. 2018.

CHRISTIDIS, K.; DEVETSIKIOTIS, M. *Blockchain*s and Smart Contracts for the Internet of Things. **IEEE Access**, [*S.l.*], v. 4, p. 2292–2303, 2016.

COSTA, M. P. da. **Fatores que influenciam a comunicação de dados de pesquisa sobre o vírus da zika, na perspectiva de pesquisadores**. 2017. Tese (Doutorado em Ciência da Informação) – Faculdade de Ciência da Informação, Universidade de Brasília, Brasília, 2017.

CRUZ, J. C. *et al*. Tecnologia *Blockchain*: um novo paradigma nas ciências abertas. *In*: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 19., 2018, Marília. **Anais** [...]. Marília: Unesp, 2018.

FAPESP - Fundação de Amparo à Pesquisa do Estado de São Paulo. **Gestão de Dados**. FAPESP, São Paulo. Disponível em: http://www.fapesp.br/gestaodedados/. Acesso em: 7 maio 2019.

FERNANDES, M. E. M.; RIBEIRO, C. Curadoria de Dados na U. Porto: Identificação de práticas em diversas áreas disciplinares. *In*: CONFERÊNCIA LUSO-BRASILEIRA SOBRE ACESSO ABERTO, 2., 2011, Rio de Janeiro. **Anais** [...]. Rio de Janeiro: U. Porto, 2011. Disponível em: http://hdl.handle.net/10216/73435. Acesso em: 17 out. 2017.

GARCÍA-BARRIOCANAL, E.; SÁNCHEZ-ALONSO, S.; SICILIA, M. Deploying metadata on blockchain technologies. *In*: Research Conference on Metadata and Semantics Research**, 11., 2017, Tallinn. Proceedings** [...] Tallinn: MTSR, 2017. p. 38-49.

GIBB, B. C. **Reproducibility**: comments and opinion. Acesso em: 1 nov. 2018.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GOODMAN, S. N.; FANELLI, D.; IOANNIDIS, J. P. A. What does research reproducibility mean? **Science Translational Medicine**, Washinton, v. 8, n. 341, jun. 2016.

HOGEMANN, E. R. O futuro do Direito e do ensino jurídico diante das novas tecnologias. **Revista Interdisciplinar de Direito**, Valença, v. 16, n. 1, p. 105–115, 20 jun. 2018.

INGRAM, C. How and why you should manage your research data: a guide for researchers. **JISC**, Bristol, 7 jan. 2016.

KOSTAREV, G. **Review of *Blockchain* consensus mechanisms**. Waves Platform, [*S.l.*], 31 jul. 2017. Disponível em: https://blog.wavesplatform.com/review-of-*Blockchain*-consensus-mechanisms-f575afae38f2. Acesso em: 7 jan. 2019.

LEITE, G. A evolução doutrinária do contrato. **Âmbito Jurídico**, São Paulo, n. 45, set. 2007.

MÁRDERO-ARELLANO, M. Á. **Critérios para a preservação digital da informação científica**. 2008. Tese (Doutorado em Ciência da Informação) – Faculdade de Economia, Administração, Contabilidade e Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2008.

MATOS, M. Como funciona o Proof of Work na *Blockchain* do Bitcoin, **Livecoins**, [*S.l.*],11 abr. 2018. Disponível em: https://livecoins.com.br/proof-of-work-*Blockchain*-bitcoin/. Acesso em: 2 jan. 2019.

MAYER, F.; ZEVIANI, W. Pesquisa Reproduzível, **Pesquisa Reproduzível com R**, Salvador, maio 2016. Disponível em: http://cursos.leg.ufpr.br/prr/capPesqRep.html. Acesso em: 27 maio 2018.

MCNUTT, M. Reproducibility. **Science**, [*S.l.*], v. 343, n. 6168, p. 229–229, 17 jan. 2014.

MOLLOY, J. C. The Open Knowledge Foundation: open data means better science. **PLoS Biology**, San Francisco, v. 9, n. 12, 6 dez. 2011.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. (2008). Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 10 set. 2018.

NASSI-CALÒ, L. Avaliação sobre a reprodutibilidade de resultados de pesquisa traz mais perguntas que respostas. **SciElo em Perspectiva**, [*S.l.*], 8 Feb. 2017. Disponível em: https://blog.scielo.org/blog/2017/02/08/avaliacao-sobre-a-reprodutibilidade-de-resultados-de-pesquisa-traz-mais-perguntas-que-respostas/#.W-1lFOhKjDc. Acesso em: 15 nov. 2018.

OECD. OECD Principles and Guidelines for Access to Research Data from Public Funding. 12 abr. 2007. Disponível em: https://www.oecd.org/sti/inno/38500813.pdf . Acesso em: 20 de maio 2019.

OLIVEIRA, J. A. M. M.; SANTARÉM SEGUNDO, J. E. A possibilidade de identificacao de violações a direitos autorais com base em metadados gerados na *Blockchain*: avaliação da plataforma original.my. *In*: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 19., 2018, Londrina. **Anais** [...]. Londrina: Universidade Estadual de Londrina, 2018.

PENG, R. D. Reproducible Research in Computational Science. **Science**, [*S.l.*], v. 334, n. 6060, p. 1226–1227, 2 dez. 2011.

PRICE, D. de S. **A ciencia desde a Babilonia**. Belo Horizonte; São Paulo (SP): Itatiaia; Ed. USP, 1976.

ROUSE, M. What is *Blockchain*? **Whatls.com**, Newton, c2020. Disponível em: https://searchcio.techtarget.com/definition/*Blockchain*. Acesso em: 10 set. 2018.

ROYAL NETHERLANDS ACADEMY OF ARTS AND SCIENCES. **Replication Studies**: Improving reproducibility in the empirical sciences. Amsterdam: Royal Netherlands Academy of Arts and Sciences (KNAW), 2018.

SANTOS, P. L. V. A. C.; SANTANA, R. C. G. Dado e Granularidade na perspectiva da Informação e Tecnologia: uma interpretação pela Ciência da Informação. **Ciência da Informação**, Brasília, v. 42, n. 2, p. 199–209, 2013.

SCHNEIER, B. Cryptanalysis of MD5 and SHA: Time for a New Standard. **Schneier on Security**, [*S.l.*], 19 ago. 2004. Disponível em: https://www.schneier.com/essays/archives/2004/08/cryptanalysis_of_md5.html. Acesso em: 20 maio 2019.

SIMMONS, J. P.; NELSON, L. D.; SIMONSOHN, U. False-Positive Psychology: Undisclosed Flexibility in Data Collection and Analysis Allows Presenting Anything as Significant. **Psychological Science**, [*S.l.*], v. 22, n. 11, p. 1359–1366, Nov. 2011.

SONG, J. **The Truth about Smart Contracts**. Medium, [*S.l.*], 11 Jun. 2018. Disponível em: https://medium.com/@jimmysong/the-truth-about-smart-contracts-ae825271811f. Acesso em: 21 maio 2019.

STEVENS, M. M. J. On Collisions for MD5. 2007. Dissertação (Mestrado) - Eindhoven University of Technology. Disponível em: https://www.win.tue.nl/hashclash/On%20Collisions%20for%20MD5%20-%20M.M.J.%20Stevens.pdf . Acesso em: 17 Abr. 2019.

STOLFI, J. Shows a typical cryptographic *hash* function (SHA-1) at work. Note that small differences in the input result in very different digests, **Wikimedia Commons,** [*S.l.*], 27 nov. 2008. Disponível em: https://commons.wikimedia.org/wiki/File:Cryptographic_ *Hash*_Function.svg. Acesso em: 20 maio 2019.

SZABO, N. Formalizing and Securing Relationships on Public Networks. **First Monday**, Chicago, v. 2, n. 9, set. 1997.

WILKINSON, M. D. *et al*. The FAIR Guiding Principles for scientific data management and stewardship. **Scientific Data**, London, v. 3, p. 160018, 15 Mar. 2016.

ZIMAN, J. M. **Conhecimento público**. Belo Horizonte; São Paulo: Itatiaia; Ed. Univ. São Paulo, 1979.

Notas

1 Em criptografia e ciência da computação, árvores de dispersão ou árvores de Merkle são um tipo de estrutura de dados que contém uma árvore de informações resumidas sobre um pedaço maior de dados.