REVISTA FATEC SEBRAE EM DEBATE:
Gestão, Tecnologias e Negócios
Volume 06 | Número 11 | JUL. – DEZ. 2019 | ISSN: 2358-9817

MONETIZANDO DADOS PESSOAIS: POSSIBILIDADES NA UTILIZAÇÃO DE BUSINESS INTELLIGENCE PARA ANALISAR DADOS PESSOAIS DE SAÚDE A PARTIR DA BLOCKCHAIN

Thamires C. Castanha

Ricardo Garrido Schwach

Resumo

Com o objetivo de repensar as possibilidades e cenários em que os dados pessoais na área da saúde são utilizados, procuraram-se maneiras de empregar o uso da Blockchain e toda sua capacidade inovativa, empregando na auditoria, fiscalização e possivelmente monetização destes dados, fazendo uso do Business Intelligence como meio de garantir a integridade de tais dados, assim como as finalidades previstas em sua utilização, pautadas na Lei Geral de Proteção a Dados e outras diretivas. Com a presente pesquisa, foi possível identificar as diferentes possibilidades de adoção da Blockchain e a forma como nossos dados pessoais de saúde vem sendo coletados e monetizados ao longo dos últimos anos, fazendo uso de cases de monetização da STEEMIT e casos de abusos na monetização de dados de saúde, como o ocorrido com a Henrietta Lacks, para criar uma ponte entre as possibilidades de transparência e imutabilidade contidas na blockchain, e a possibilidade de auditoria, controle e monetização de dados pessoais, utilizando como suporte o conceito do Business Intelligence.

FATEC Sebrae – Faculdade de Tecnologia Sebrae - CEETEPS – Centro Estadual de Educação Tecnológica Paula Souza – São Paulo, Brasil.

REVISTA FATEC SEBRAE EM DEBATE: gestão, tecnologias e negócios

Editor Geral
Prof. Dr. Mário Pereira Roque Filho

Organização e Gestão
Prof. Ms. Clayton Pedro Capellari

Correspondência
Alameda Nothmann, nº 598 Campos Elíseos, CEP 01216-000 São Paulo – SP, Brasil.
+55 (11) 3224.0889 ramal: 218
E-mail: f272dir@cps.sp.gov.br

Pode-se concluir que os critérios utilizados para aplicação se baseiam diretrizes legais já existente sobre a proteção de dados dentro e fora do país, assim como cases de Biobanks e repositórios similares, onde estudos foram realizados, para efeito comparativo.

Palavras-chave: Blockchain, Henrietta Lacks, STEEMIT, Biobanks;

Abstract

In order to rethink the possibilities and scenarios in which personal data in the health area are used, we sought ways to employ the use of Blockchain and all its innovative capacity, employing in auditing, supervision and possibly monetization of this data, making use of Business Intelligence as a means of ensuring the integrity of such data, as well as the purposes provided for in its use, based on the General Data Protection Act and other directives . With the present research, it was possible to identify the different possibilities of adoption of Blockchain and how our personal health data has been collected and monetized over the past few years, making use of STEEMIT monetization cases and cases of abuses in the monetization of health data, such as the one that occurred with Henrietta Lacks, to create a bridge between the possibilities of transparency and immutability contained in blockchain, and the possibility of auditing, controlling and monetizing personal data, using as support the concept of Business Intelligence. It can be concluded that the utilized criteria for application are based on existing legal guidelines on data protection inside and outside the country, as well as Biobanks cases and similar repositories, where studies were conducted, for comparative purposes.

Key-words: Blockchain, Henrietta Lacks, STEEMIT, Biobanks;

1. Introdução

O *Business Intelligence* (BI) é uma área de extrema preocupação em muitas organizações, porém existem deficiências de pesquisa e aplicabilidade em diversos setores. Um número considerável de companhias está implementando sistemas de BI, mas não são todos os setores que percebem os benefícios e formas de adoção do BI, e principalmente, seu conceito.

No livro *Cypherpunks*: liberdade e o futuro da internet, escrito por Julian Assange em 2012, é questionado o acesso sem limite do Estado a dados pessoais sob a máxime de protegê-los de possíveis ameaças. Para Assange (2012), a alegação de interceptação estratégica é um absurdo, isso seria como dizer que tudo deve ser captado, sendo apurado posteriormente a real necessidade do que foi coletado (TEIXEIRA; ARMELIN, 2019).

Os dados pessoais são considerados “o novo petróleo” da sociedade informacional, a base de um gigantesco mercado, com potencialidade de identificar perfis de consumo, oportunidades de mercado, além de inúmeras outras possibilidades altamente lucrativas (TEIXEIRA; ARMELIN, 2019).

Considerando os desafios de integrações de dados internos e externos, este trabalho dedica-se a tentar entender como empresas utilizam dados abertos e não estruturados em seus processos decisórios, observando ainda, como oportunidade, a possibilidade das organizações em trabalhar com dados disponibilizados em grande volume e variedade na *Blockchain*. De forma ampliada, debate-se como os dados podem ser utilizados pelas empresas em seus sistemas de Business Intelligence & Analytics (SILVA; MEIRELES, 2017).

No decorrer deste trabalho, será apresentado a lógica por trás dos criptoativos, a aplicação da *blockchain*, coleta de dados pessoais, estudos e formas de monetização de conteúdos, considerando diversos pontos de vista de especialistas nas áreas residentes no Brasil e exterior.

2. Fundamentação teórica

A criação e manipulação de um número cada vez maior de informações, está modificando o modo como as pessoas conversam, apresentam e demonstram dados, seja na vida cotidiana ou dentro organizações. A sociedade está constantemente fazendo análises de informações, conscientemente ou não, para chegar a conclusões em suas respectivas áreas, tanto no âmbito profissional como no pessoal.

A partir da criação e adoção de novas tecnologias, a obtenção e manipulação de informações tende a ser maior. Da mesma forma em que processos e tecnologias são criadas para facilitar a relação entre indivíduos, muitas vezes processos simples, se tornam complexos e invasivos.

Um caminho a seguir é a adoção de meios que controlem e auditem esse fluxo de informações, assim como a forma que estes dados estão sendo utilizados. Os próximos tópicos abordaram estes tópicos com maior profundidade.

Como funciona a transferência e pagamento com o Bitcoin e outras altcoins

A ideia de criação de um novo meio de pagamento, sem uma autoridade central encarregada em auditar e conferir as transações, já havia sido citada em fóruns de discussão *Cypherpunks* (ULRICH, 2014).

Segundo o *whitepaper* de Satoshi Nakamoto (2008), o modelo tradicional dos bancos limita o acesso à informação das partes envolvidas. O modelo *peer-to-peer* abordado por Nakamoto prevê a publicidade das transações através de um método que mantem assegurada a privacidade dos usuários sem quebrar o fluxo de transação entre as partes. No processo, é possível ver usuários enviando valores e outros recebendo, mas sem informações aparentes vinculando estas transações.

Na definição de Mougayar (2017), a rede *peer-to-peer* pode ser definida como um conjunto de computadores conectados através de nós em uma topologia eterna expansão. Todo nó roda o mesmo software, fornecendo redundâncias inseparáveis a

toda rede, o que significa que, se um nó para de funcionar ou não responde, o trabalho dos outros nós o compensará.

De acordo com Azzolini et al. (2018), Bitcoin é um dos primeiros meios de pagamentos decentralizados *peer-to-peer* (ponto a ponto) em um sistema baseado em *Proof-of-Work* (Provas de trabalho). Prova de trabalho, ou PoW em inglês, são algoritmos que requerem grandes poderes computacionais e sua utilização remove a necessidade de centralização em uma terceira parte. De maneira simplificada, uma prova de trabalho é a resposta para um problema considerado computacionalmente difícil de se resolver, sendo uma transação considerada válida após armazenada em algum bloco publicado na *blockchain*, e isso só é realizado após uma Prova de Trabalho ser calculada e exibida. (FILHO, 2016)

De acordo com Filho (2016), para executar uma transação, baseado no *whitepaper* de Nakamoto (2008), existem chaves criptografadas são utilizadas para processar as transações de maneira direta sem precisar de intermediários. As chaves utilizadas nestas transações nada mais são do que endereços. O modo de transação mais comum o *Pay to Pubkey Hash*, sendo este modelo baseado em um esquema de assinaturas digitais, no qual os bitcoins são transferidos para quem apresentar uma assinatura feita com uma determinada chave secreta. Olhando a chave pública dessa transação, é possível verificar se a transação foi de fato assinada por uma chave privada, legitimando a transação, já que isso confere que a transação foi registrada, além de conter data e hora quando exposta em um bloco, impedindo assim gastos duplos e fraude (ULRICH, 2014).

De maneira técnica, segundo Filho (2016), nas transferências do tipo *Pay to Pubkey Hash*, o script *ScriptPubKey* (o da saída) espera ser alimentado com uma chave pública que tenha um determinado valor *hash* (endereço) e uma assinatura gerada com a chave secreta (senha) correspondente ao endereço especificado. Essa assinatura é fornecida pelo *ScriptSig* da entrada que reivindica os bitcoins e deve ser gerada sobre a versão simplificada da transação que contém essa entrada.

Filho (2016) afirma também que outro modo de transferência é o *Pay to Script Hash*. Nesse modo de transferência, o script de uma saída precisa apenas especificar um

valor *hash*. Para reivindicar essa saída, uma entrada precisa conter um script que execute sem erros e que tenha valor *hash* igual ao especificado. Com esse esquema de transferência é possível criar transações mais complexas, para implementar, por exemplo, contratos inteligentes, os quais, de acordo com EdChain (2018), são pedaços de código que podem desempenhar funções legais, como controlar uma entidade baseada em condições ou transferir ativos também restritos a condições.

Filho (2016), aponta que, toda a rede que move as transações é baseada em usuários que a operam e, para incentivar estes a investir recursos computacionais na validação dos blocos e geração de novos Bitcoins, estes recebem recompensas financeiras por seus trabalhos nestas operações.

Mougayar (2017), resume a ciência da criptografia utilizada para garantir a segurança para uma rede blockchain pautando em três conceitos básicos: *hashing*, chaves e assinaturas digitais. Para ele, um *hash* é uma impressão digital única que ajuda a verificar se informações não foi alterada, sem a necessidade de realmente ver isso, as Chaves são usadas por uma combinação mínima de duas, sendo uma pública e uma privada. Por fim, para que a transação *Pay to Pubkey Hash* ocorra, a chave pública é usada pelo remetente para codificar informações que podem ser decodificadas apenas pelo proprietário da chave privada. Uma assinatura digital é uma computação matemática usada para provar a autenticidade de uma mensagem ou documento (digitais).

Como funciona a Blockchain

O Bitcoin foi concebido em 2008 por Satoshi Nakamoto e junto a ele surgiu baseado em uma estrutura de dados pública chamada blockchain, que armazena o histórico de todas as transações já realizadas. De acordo com Filho (2016), a segurança da blockchain, incluindo sua não-maleabilidade, é garantida pela dificuldade da prova de trabalho exigida para que novas informações sejam adicionadas nessa estrutura.

Na definição de Mougayar (2017), em sua essência, o *blockchain* é uma tecnologia que grava transações permanentemente de uma maneira imutável, as quais somente

podem ser atualizadas sequencialmente, mantendo um rastro histórico sem fim, tornando a capacidade de provar que algo aconteceu uma especialidade do blockchain.

Boulos et al. (2018) defende que uma das capacidades da *blockchain* é sua complexidade criptográfica, cuja capacidade consegue de comprovar propriedades de dados/ativos e validação, sendo a imutabilidade um subproduto da segurança criptográfica e da descentralização.

Boulos et al. (2018) também explica a criptografia como uma das maiores bases do blockchain, incluindo a prova de dados e validação, sendo duas formas de criptografia comumente empregadas com blockchains sendo as funções de hash unidirecional e criptografia assimétrica utilizando chaves públicas e privadas (endereços). Cada uma dessas formas de criptografia tem um papel na proteção, na comprovação da propriedade e na prevenção de modificações, sejam privadas ou aplicadas exclusivamente a criptomoedas. As transações de blockchain podem se referir à transferência de qualquer ativo digital — incluindo dados.

A criptografia amplamente utilizada, principalmente quando falamos de criptoativos, é a criptografia assimétrica, conhecida como criptografia de chave pública (endereço). Esse modelo começar criptografando ou embaralhando os dados, usando um par de chaves, tornando os dados inúteis se eles acabaram na posse de alguém que não está na posse da chave necessária para descriptografá-los. A criptografia de chave pública pode ser usada de duas maneiras básicas: criptografar dados que apenas o detentor da chave privada pode descriptografar e usar e provar que os dados vieram de uma fonte confiável por uma confirmação com a utilizção de uma chave privada. (BOULOS et al., 2018)

Boulos et al.(2018) aponta que para entender como a imutabilidade confere segurança, é preciso analisar uma anatomia simplificada de um bloco no blockchain, sendo o bloco considerado como um contêiner para alguns dados espalhados por vários nós e as taxas de transação pagas aos mineiros (PoW) um pagamento para manter esses nós abertos, o que, por sua vez, mantém a blockchain segura no

compartilhamento de dados, seja através do armazenamento dos dados propriamente dito ou instruções sobre quem pode acessar esses dados.

Na concepção de Mougayar (2017), existe uma hierarquia dos métodos de provas, que varia desde estarem embutidos como parte de um protocolo de consenso (como a prova de trabalho ou a prova de participação), a prova como serviço (como prova de uma identidade ou propriedade), até a prova em serviço, que prova que algo é parte de outro serviço (tal como registro de terras ou casamento) mantendo a propriedade e segurança de acesso à estes dados na adoção da Blockchain.

Outro benefício apontado por Mougayar (2017), é a transparência em oferecer a informação certa para a pessoa certa, protegendo os negociantes e consumidores através de controles granulares, melhora a visibilidade, diminuindo o risco a fraude e adulterações.

A adoção da Blockchain também possui aspectos que podem se tornar pouco favoráveis, como apontados por Kuo et al. (2017), com sua relação entre confidencialidade e transparência, dado que, sua uma grande transparência pode diminuir a confidencialidade proporcionalmente podendo ser considerado uma limitação. Mesmo que, um usuário seja anonimizados, ele ainda pode ser reidentificado através de uma análise dos dados públicos da blockchain. Ester ponto é criticamente relevante para usos na área da saúde, em vista que, dados de saúde são altamente sensíveis.

Outro ponto de atenção sobre a Blockchain considerado um desafio por Kuo et al.(2017), é a sua dúvida sobre a velocidade e escalabilidade das aplicações, um exemplo dado por ele é com relação aos protocolos de prova de trabalho utilizadas pelo Bitcoin, cuja média diária eram de 150 milhões de transações por dia, sendo o máximo de realizações em 2017 de 7 transações por segundo frente as 4000 transações por segundo realizadas pela VISA.

Mougayar (2017) já defende os benefícios da transparência da *blockchain* como uma maneira de oferecer as informações certas para as pessoas certas, protegendo negociantes e consumidores por mio de controles granulares, diminuindo o risco de adulterações. Outro ponto defendido por ele é que o crescimento do uso do *blockchain*

tem uma vantagem em relação à trajetória da web, pois seu ponto de início é amplificado por quatro segmentos: usuários da web, usuários de telefone celulares, proprietários de sites, possivelmente tornando sua adoção escalável com isto.

Possibilidades de análise e auditoria dos dados contidos na Blockchain

O *Business Intelligence* (BI) pode ser considerado como uma infraestrutura processual e técnica que coleta, armazena e analisa os dados produzidos por um campo de atividades ou por uma empresa, sendo que o BI destina-se a coletar dados que são necessários por um negócio e apresenta-los de maneira simplificada, que facilite a sua tomada de decisão (BOTOS, 2017)

As ações comumente incluídas nas áreas relacionadas ao BI são: métricas de relatórios, consultas, scorecards, análise e monitoramento operacional, estudos quantitativos, mineração de dados, modelagem de dados, análise de dados, testes multivariados entre outros. Previamente a análise de dados, para modelar e limpar os dados, podem ser utilizados meios estatísticos. Existem etapas a serem definidas previamente, como a determinação de requisitos antes de sua coleta, meios de processamento e limpeza, determinando o produto necessário e, no final, realizar a comunicação dos resultados as partes envolvidas (BARBIERI, 2011).

Segundo Ulrich (2014), é possível coletar identidades observando a *Blockchain* a partir de técnicas de agrupamento baseadas em padrões estruturais no comportamento, podendo revelar a identidade de 40% dos usuários que realizam transações em Bitcoin (apud OBER, KATZEINBESSER e HAMACHER, 2013).

É relevante enumerar as barreiras para uma análise de dados efetiva. Se a informação não é clara e concisa, pode haver preconceitos cognitivos e o resultado pode ser errôneo. Quando se fala na utilização do BI para análise do Bitcoin, não há uma fonte geral de informações que podem ser acessados, a fim de obter informações financeiras relevantes como volumes de transação, *over the counter* (OTC) ou padrão para câmbio, número de usuários únicos, número de mineradores ou número de estações de mineração, etc. (BOTOS, 2017)

Mougayar, em seu livro, descreve o *blockchain* como um banco de dados *back-end* que mantem um registro distribuído podendo ser inspecionado abertamente. Para ele o *blockchain* pode substituir bases de dados que mantem registros distribuídos abertamente, cuja finalidade seja troca entre partes ou mecanismos de validação de transações que não requerem apoio de intermediários

Apesar das dificuldades em aplicar e entender a *blockchain*, Botos (2017) diz que quando se fala em cadeia de blocos, pode-se referir à análise de um banco de dados de Big data, sendo o maior objetivo, a fim de ter uma análise de dados abrangente e relevante, ser determinado exatamente os elementos que vão ser de relevância das informações que o *Blockchain* pode fornecer para trabalhar.

Na concepção de Edd Dumbill (2012), Big Data pode ser definido como dados que excedem a capacidade de processamento dos sistemas convencionais de gestão de dados, movendo se rapidamente ou não cabendo em uma estrutura de dados. Por mais que ainda não existam linguagens de consulta para a *Blockchain*, já existem ferramentas como o BigchainDB que combina os benefícios de um banco de dados distribuídos (NoSQL) e a *blockchain*.

Para analisar os dados e em muitos casos apresentá-los, é necessário o uso de softwares. Para a análise de um grande volume de dados, os software recomendado são: Alteryx, IBM (SPSS), Knime, Revolution R Enterprise, Oracle Advanced Analytics, SAP Predictive Analytics, SAS, Teradata Aster Discovery Platform. Algumas ferramentas de análise exigem programação e outras não, como Olikview, tableau ou DSS, IBM Analytics, Matlab, Microsoft Power BI, Sisense, Python, BigChainDB. Apesar da infinidade de ferramentas, escolher uma é determinar a direção da análise é parte fundamental da inteligência (BOTOS, 2017).

Utilização de dados pessoais na área da saúde

Desde 1968, computadores já eram financiados pela indústria a fim de serem inseridos em hospitais, com o objetivo de coletar informações sobre tratamento de pacientes, principalmente dados demográficos, com perguntas focadas em tratamentos de saúde,

buscando identificar padrões de doenças pré-existentes ou futuras, utilizando isto como base de apoio aos médicos, cabendo a eles terminarem o diagnóstico e conduzir o tratamento (Tanner, 2016).

Em 1978, um programa criado por um player farmacêutico, queria entender como era a performance dos medicamentos individualmente, com isso ranqueou médicos e suas prescrições mais realizadas. Para compor tal análise, o programa enviou milhares de questionários a médicos, pagando entre $2 e $10 por prescrições e medicamentos favoritos. Como resultado, as companhias puderam criar segmentações de médicos e focar nos representantes e medicamentos vendidos pelos mesmos, podendo melhorar seu poder de convencimento (TANNER, 2016).

Tanner (2016), também relata que nas primeiras décadas após as bombas atômicas, com o consentimento dos sobreviventes, estudos longitudinais foram realizados. Estudos no mesmo formato foram iniciados em 1948, resultando em um grupo ativo de adultos na faixa entre 80 e 90 anos em 2014 que continuam participando. Estes estudos custam milhões por ano, mas criam uma base de *insights* extensos que podem identificar padrões de doenças como pressão alta, diabetes, colesterol, padrões genéticos, eficácia de tratamentos, entre outros.

Da mesma forma, existem grupos de estudos longitudinais que não sabem que participam de tais grupos e, consequentemente, não tem seu consentimento expressado para tal, mas raramente descobrem que estão em meio a este processo de coleta (TANNER, 2016).

Os pontos mais monitorados em estudos, e relevantes, utilizados por indústrias farmacêuticas sobre suas drogas são: Quanto tempo um paciente continua com particular droga ou componente, o quão bem/certo um paciente segue a prescrição, o que motiva um paciente a trocar para concorrência e quais outras drogas o paciente faz ou pode a vir fazer uso durante o tratamento da droga em questão (TANNER, 2016).

Tanner também aponta que tais dados coletados podem ajudar a estimar e definir novas drogas, custos públicos com saúde, qualidade no atendimento, análises sociais, políticas públicas, além de salvar vidas, como o caso de pessoas que estão em

emergências e possuem condições pré-existentes podendo definir casos de vida ou morte.

Da mesma forma, o lado negativo de tais coletas é que estes dados podem ajudar na discriminação, como a requisição de uma pessoa mais saudável para ser contratada ou promovida, doenças preexistentes como HIV, condições psiquiátricas ou até mesmo tendências de desenvolvimento de doenças a partir de histórico familiar (TANNER, 2016).

Tanner (2016) expõe que, por mais que os dados sejam anonimizados, existem a possibilidade de reidentificação pela identificação do padrão o qual foi anonimizados ou pela grande quantidade de informação coletada, principalmente quando estes possuem doenças raras ou condições específicas. Um estudo em 1997, nos Estados Unidos, identificou que removendo nome, deixando apenas código postal, data de nascimento e gênero era possível identificar 87,1% de usuários em uma base (TANNER, 2016)

Elger e Caplan (2006) já haviam defendido que o mesmo acontecia com materiais biológicos são informações associadas como o tipo de tumor, tratamento médico, idade do doador e assim por diante, mas todas as informações que permitam a identificação do participante da pesquisa ou do paciente é irreversivelmente.

A terminologia utilizada pelos documentos europeus (CDBI, 2006; COE, 2006) se baseia em cinco níveis de anonimização para amostras humanas: anônimo, desvinculado anonimizados, vinculado anonimizados, codificados e identificados. Se as amostras contêm qualquer traço de DNA, eles não são verdadeiramente anônimos, porque é sempre possível identificar o doador através de impressões digitais de DNA.

De acordo com Kaiser (2002), o armazenamento e coleta de dados médicos mudaram, e desde o início dos anos 2000, existe um crescimento súbito de biobancos populacionais, como cada vez mais países estabelecendo novas coleções de amostras. Elger e Caplan (2006) definiram a origem do termo biobanco em 1996 e sua aplicação a partir dos anos 2000, sendo um termo utilizado para descrever repositórios biológicos humanos — órgãos, tecidos, sangue, células e outros fluidos corporais — que contém pelo menos vestígios de DNA ou RNA que permitem a análise genética,

muitas vezes compreendendo informações sobre o doador do material, tais como características demográficas, o tipo de doença associada

Entre os mais conhecidos estão: o banco de dados do setor de saúde da Islândia; o projeto genoma estoniano; o Biobank do Reino Unido; o projeto CARTaGENE em Quebec, Canadá; o Banco Nacional de ADN em Espanha; o Projeto Internacional HapMap; e vários biobancos dos EUA, como o estudo nacional das crianças, o projeto de pesquisa de medicina personalizada da clínica Marshfield e os inquéritos nacionais de exames de saúde e nutrição (ELGER; CAPLAN, 2006)

Em 2004 os irmãos Ámason, demonstraram que existem duas preocupações sobre o manuseio de dados genéticos, uma delas seria a alegação de que ninguém pode dar o consentimento informado para fornecer dados genéticos, pois não há planos de pesquisa específicos disponíveis e seus riscos, além da preocupação sobre os bancos de tecidos, nos quais os tecidos recolhidos para estudos científicos, só podem ser mantidos após o estudo ou transferidos para um banco de tecidos se o prestador da amostra expressar seu consentimento, tornando paradoxal a relação de manuseio e pesquisa (ÁMASON; ÁMASON, 2004).

De fato, um grande problema ético para os biobancos prospectivos é como garantir o consentimento dos participantes quando não se sabe o que estão consentindo em pesquisas futuras. A questão da importância e do significado do consentimento informado é uma das principais razões pelas quais as orientações internacionais sobre os biobancos não têm nenhum consenso (ELGER; CAPLAN, 2006).

O que prevê a LGPD

O tema sobre proteção de dados pessoais recebe destaque na sociedade desde a década de 70 com países que começaram a regular praticas relacionadas, como é o caso da Alemanha, iniciando a primeira onda de regulações na Europa, as quais foram consolidadas com a Diretiva 95/46/CE que evoluíram e foram substituídas pela Regulamentação Geral de Proteção de Dados Pessoais da União Europeia 2016/679 – GDPR, em vigor desde 2018 (TEIXEIRA; ARMELIN, 2019)

No Brasil, algumas leis existem para compor um sistema protetivo dos dados pessoais, que consideram a intimidade e a vida privada, garantem o direito ao conhecimento de informações relativas à pessoa, bem como retificar os dados, o tratamento das informações pessoais deva ser feito de forma transparente e com respeito à intimidade, vida privada, honra e, como um princípio do uso da internet, assegurando como direito a especificação da finalidade para a coleta, o uso e o compartilhamento dos dados pessoais, condicionando ao consentimento expresso pelo titular dos dados (TEIXEIRA; ARMELIN, 2019).

De acordo com Ulrich (2014), é provável que nenhum país desenvolvido tenha avançado tanto a agenda contra a privacidade financeira como os Estados Unidos, tanto que tais normas têm feito bancos europeus e suíços em declinar de clientes americanos para não terem que se submeter a exigências do governo dos EUA, como as impostas pela legislação FATCA *(Foreign Account Tax Complience Act)*. Aprovada pelo congresso em 2010, a FATCA concede à Receita Federam dos EUA *(Internal Revenue Service ou IRS)* o poder de violar o direito de cidadãos que detenham investimentos ou contas bancárias no exterior.

Já no âmbito da saúde, os Estados Unidos possuem uma lei de proteção de dados própria para a área da saúde, a HIPAA (*Health Insurance Portability and Accountability Act*) criada em 1996 e amplamente aplicada no início dos anos 2000 sendo sua aplicação obrigatória pata planos de saúde, farmácia, médicos, seguros saúde e programas de saúde governamentais, definindo que dados pessoais não podem ser coletados ou utilizados sem autorização do paciente, sendo estes dados anonimizados métodos, definidos por Tanner (2016) como pouco confiáveis e com a possibilidade de acessarem estes dados sem serem cobertos pelas regras do HIPAA.

Segundo Teixeira e Armelin (2019), o cidadão brasileiro comum ainda não se incomoda em fornecer o seu número de CPF as empresas em troca de descontos e outros benefícios.

O Brasil está em processo de implementar a LGPD (Lei Geral de Proteção a Dados), defendida por Teixeira e Armelim (2019), como uma lei que definirá o fim da era do *Big Data* para o *Small* Data, já que os dados não serão coletados dados sem qualquer

evidência ou finalidade determinada previamente. Para que os dados sejam tutelados pela LGPD, basta que se encontre em território nacional no momento da coleta, considerando a extraterritorialidade das empresas.

Porém, existe uma brecha legal na qual dados anônimos, aqueles que não são possíveis de serem reidentificados por quaisquer meios razoavelmente possíveis, não são dados pessoais e não são tutelados por lei, já dados anonimizados, aqueles que através de técnicas possibilite sua reidentificação, estará sobre a tutela da lei, sendo considerados como pesudoanonimizados (TEIXEIRA; ARMELIN, 2019).

Monetização de dados pessoais: Caso Henrietta Lacks

Henrietta Lacks morreu em 1951 de um adenocarcinoma agressivo do colo do útero. Uma biópsia do tecido obtida para a avaliação diagnóstica rendeu o seqüenciamento das células retiradas sem o consentimento para o laboratório Johns Hopkins (Baltimore, Maryland). As células cancerosas, cresceram rapidamente na cultura celular e tornaram-o genoma HeLa. (SKLOOT, 2013)

Henrietta Lacks era uma agricultora de tabaco, negra e mãe de cinco, e embora ela tenha falecido em 1951, suas células foram utilizadas para ajudar a desenvolver vacinas, medicamentos para o câncer, fertilização *in vitro*, mapeamento de genes, clonagem, entre outros (SKLOOT, 2013).

De acordo com Guedes (2013), amostra de células cancerosas foram retiradas durante o tratamento e, mediante o consentimento do viúvo para uma autópsia, mais células foram retiradas após a morte de Henrietta, com a promessa de que tais células serviriam para a realização de testes com potencial de gerar benefícios futuros a seus descendentes.

Guedes (2013) também expõe que uma das maiores questões sobre a história de Henrietta é referente à ausência de consentimento para a retirada e utilização de suas células para fins de pesquisa. A autorização solicitada e assinada em vida por Henrietta constava a autorização da paciente apenas para a realização de

procedimentos cirúrgicos e anestésicos necessários para a evolução do tratamento da doença.

Outro ponto abordado por Guedes (2013) era a segregação presente na época, na qual pessoas negras e em situações de vulnerabilidade costumavam ser inseridas em estudos científicos de maneira compulsória, indiferente ao consentimento ou consequências das pesquisas. Guedes (2013) ressalta também centros biomédicos de pesquisas, onde pessoas negras eram frequentemente utilizadas como cobaias em estudos, muitas vezes trazendo sérios prejuízos à integridade física, como uma pesquisa sobre sífilis que levou à morte muitos negros estadunidenses privados de assistência médica.

As publicações acerca das pesquisas relacionadas as células HeLa ganharam destaque e em 1973, a identidade de Henrietta como a doadora das células foi revelada de maneira não intencional a sua família. O acesso aos resultados de estudos em muitos países hoje são um direito reconhecido aos participantes, entretanto, na época de Henrietta, não existiam diretrizes ou legislações relacionadas à produção científica e ao compartilhamento de ganhos obtidos (GUEDES, 2013).

Atualmente, documentos e legislações internacionais preveem não só o direito das pessoas de serem questionadas quanto ao interesse em participar voluntariamente das pesquisas, assim como ao direito de conhecer e usufruir de possíveis benefícios originados por estudos. Em pesquisas biomédicas, por exemplo, a conclusão dos estudos, podem resultar à produção de medicamentos aos quais os participantes conseguem ter acesso. No caso das pesquisas qualitativas, os participantes têm direito a conhecer os resultados do estudo e usufruir de possíveis benefícios indiretos ou mesmo imprevisíveis, como ganhos financeiros resultantes de prêmios, produções de livros, filmes ou documentários (GUEDES, 2013).

Monetização por geração de conteúdo: STEEMIT

A STEEMIT foi criada como uma rede social que gira em torno do conceito de contribuição significativa de todos para a Comunidade, e que tais contribuições devem ser reconhecidas pelo valor que acrescenta (STEEM INC., 2018).

Uma das particulariedades a partir da aplicação do *blockchain*, são as distribuíções de moedas STEEM (tokens) para criadores de conteúdo, publicamente acessível e relevantes. O blockchain da STEEM oferece uma troca de tokens descentralizada, permitindo que os usuários negociem seus tokens de STEEM e de SBD através de um mercado peer-to-peer descentralizado e público. Os usuários podem colocar ordens de compra e venda, e a correspondência de pedidos é executada automaticamente pela *blockchain* (STEEM INC., 2017).

O desafio enfrentado pela STEEM é criar um algoritmo para marcar contribuições individuais que a maioria dos membros da Comunidade consideram ser uma avaliação justa do valor subjetivo de cada contribuição. Em um mundo perfeito, os membros da Comunidade cooperariam para avaliar a contribuição uns dos outros e obter uma compensação justa. No mundo real, os algoritmos devem ser projetados de tal forma que eles são resistentes à manipulação intencional para o lucro (STEEM INC., 2017).

3. Metodologia da pesquisa

A pesquisa realizada neste trabalho pode ser classificada como exploratória, isto porque, deve a pesquisa a uma abordagem direta por meio das bibliografias empregadas para a documentação, permitindo a descrição e investigação hipotético-dedutiva, caracterizada pela busca de autores para uma exploração mais abrangente.

O método hipotético-dedutivo foi definido por Karl Pooper em 1935, propõe ao pesquisador manter-se em atitude crítica permanente, com o objetivo de combater o erro, considerando-o tão importante quanto o objetivo de descobrir a verdade científica (GUIMARÃES, 2018).

O material documentado, bem como as respectivas análises, foram organizadas de maneira ordenada por hierarquia de necessidade para construir uma lógica com suas camadas de aplicação, pretendendo estruturar a viabilidade hipotética de uma aplicação da análise contida a seguir.

4. Análise de dados e resultados

A declaração universal dos direitos humanos prevê a igualdade entre todos os seres humanos, sem distinção de qualquer espécie, o que nos remetendo a proteção mais rigorosa dos dados, que se utilizados de maneira a extrapolar sua finalidade, podem causar alguma discriminação.

Indivíduos em situações de opressão ou emergência podem ser beneficiados da privacidade possível com a aplicação da *blockchain* proporciona, assim como pessoas que buscam privacidade financeira, como esposas fugindo de parceiros abusivos, pessoas procurando serviços de saúde controversos, empregadores que conseguem julgar suas decisões, expatriados, entre outros.

Uma maneira possível de alcançar justiça e atribuir responsabilidade as partes que manuseiam dados pessoais de saúde é a utilização de contratos, com as partes interessadas se comprometendo a pagar uma penalidade caso se comporte desonestamente, podendo eliminar a dependência de uma autoridade central para escrever esses contratos.

Dados de saúde físicos podem ser considerados uma propriedade inteligente, não sendo produto digital, mas um objeto que se tornou “inteligente” através de uma ligação explícita ou implícita com um *blockchain*, ligando sua assinatura criptográfica ao seu conteúdo (MOUGAYAR, 2017).

Mougayar (2017) relata que a utilização da blockchain possibilita diversas abordagens direcionadas à segurança pessoal e de identidade, incluindo acesso a dados e serviços. Algumas necessitam de novas soluções de hardware, outras são baseadas em software, outras se integram com soluções de negócio a negócio.

As aplicações que utilizara *Hardware* incluem, por exemplo, um cartão similar a um passaporte, que dá acesso a viagens ou nos autoriza a dirigir, podendo combinar dados biométricos a outras autenticações, enquanto aplicações relacionadas a utilização de softwares incluem identificações que são realizadas na *web* ao entrar em sites (MOUGAYAR, 2017).

Mougayar (2017), dá um exemplo de aplicação de *blockchain* na área da saúde, o *Guardtime* realizado pelo governo estoniano, que utiliza dados de saúde desbloqueados em conjunto com um registro distribuído, onde os cidadãos obtêm uma credencial que desbloqueia o acesso a seus registros em tempo real. Para Agraal et al. (2017) Essa abordagem garante que os dados dentro dos registros eletrônicos de saúde contenham uma trilha de auditoria imutável, com logs também imutáveis e com carimbo de tempo. Qualquer atualização no banco de dados, como agendamento de compromissos, é atribuída um carimbo de data/hora e assinado criptograficamente em um bloco.

Uma segunda implementação relacionada a registros de saúde é a MedRec, um projeto iniciado entre o MIT Media Lab e o Beth Israel Deaconess Medical Center. Esta plataforma oferece uma abordagem descentralizada para o gerenciamento de permissões, autorização e compartilhamento de dados entre sistemas de saúde com o uso de blockchain. Esta aplicação destina-se a dar aos pacientes a capacidade de ter conhecimento de quem pode acessar seus dados de saúde, mesmo que os dados de saúde não sejam armazenados no blockchain (ANGRAAL et al., 2017).

Outros usos para área da saúde podem ser combinação de processos multiassinaturas e *QR codes* para dar acesso específico de registros médicos ou partes dele a profissionais de saúde autorizados, reduzir fraudes de convênios em procedimentos ou verificar conformidades em serviços prestados e até compartilhar dados de pacientes de maneira agregada garantindo sua privacidade (MOUGAYAR, 2017).

Boulos et al. (2018), também pontua que a gestão da cadeia de abastecimento de saúde e sua gestão podem utilizar a *blockchain* para rastrear os materiais originados para fabricação, o próprio processo de fabricação e a distribuição dos produtos fabricados, reduzindo o número de perdas, falsificações e atestando sua qualidade.

Podemos considerar que o estudo da aplicabilidade da *blockchain* em áreas de saúde foi iniciada, porém, seu leque de aplicações não foi aproveitado em sua totalidade, tornando essa área ainda pouco explorada.

5. Considerações finais

A internet é composta de versões públicas e privadas, e os caminhos das aplicações da blockchain tendem a seguir o mesmo caminho. Sua principal diferença será o propósito, porém a funcionalidade tenderá a seguir o propósito de transparência e integridade das informações

No Brasil, legalmente, o princípio da preservação física do indivíduo vem frente a preservação da privacidade, portando a utilização da interoperabilidade de sistema de saúde pode e deve ser utilizada para manter e facilitar o acesso de pessoas autorizadas à registros médicos em emergências, facilitando processos e, possivelmente, salvando vidas.

Já existem normas nas quais os pacientes e participantes têm direito a conhecer os resultados do estudo e usufruir de possíveis benefícios indiretos ou ganhos monetários de pesquisas e consultas médicas, porém muitas camadas que recolhem, armazenam ou trabalham com estes dados, não solicitam o aceite do usuário sobre o uso.

As maneiras de dados de saúde serem verificados, auditados e analisados na forma que são armazenados hoje é praticamente impossível pelo público comum, restringindo técnicas como o *Business Intelligence* as decisões internas e objetivadas a ganhos empresariais.

O *Business Intelligence*, como conceito e não ferramenta, pode ser uma maneira de dar acesso a um grupo de usuários capacitados, um meio de auditar e acompanhar o que empresas realizam – e ganham – com nossos dados.

Clientes gostam de utilizar cartões de crédito por seus benefícios, por exemplo, então por que é possível receber pelo compartilhamento e utilização dos nossos dados? Este poderia ser um benefício atrelado a um serviço ou produto, da mesma forma que é

entendido o *cashback* ou proteção de crédito, como valor agregado e este nada mais é do que uma versão simplificada de um ativo digital.

Não só o blockchain protege a propriedade de dados, como também pode facilitar o compartilhamento de forma segura enquanto recebe benefícios ou pagamentos. Os dados de saúde podem ser utilizados para a coleta de exames ensaios clínicos, podem ser rentabilizados, e compartilhados com outros profissionais de saúde em formato de registos eletrônicos.

É possível e viável atrelar a interoperabilidade necessária nos sistemas de saúde, a transparência da *blockchain*, fazendo do uso de ideias de tokenização, como proposto pela Steemit, um meio democratizar o entendimento da utilização e monetização dos nossos dados.

Se os dados são considerados minas de ouro, os usuários devem ter o poder de decidir sobre seu anonimato, e se for sua vontade, devem ganhar uma parte deste prêmio.

6. Referências bibliográficas

ÁMASON, Gardar; ÁMASON, Vilhjálmur. Informed Democratic Consent? The Case Of The Iceland Database. **TRAMES**, Estonia, 2004.

ANGRAAL, Suveen *et al*. Blockchain Technology: Applications in Health Care. **Cardiovascular Perspective, Yale New Haven Hospital**, New Haven, CT, 2017.

AZZOLINI, Damiano *et al*. Modeling Bitcoin Protocols with Probabilistic Logic Programming. **CEUR**, Ferrara, Italy, v. 2219, 2018.

BARBIERI, Carlos. **BI2 Business Intelligence. Modelagem e Qualidade**. [*S. l.*]: Elisever, 2011.

BIG Data Now. [*S. l.*]: O'Reilley Media Inc., 2012.

BOTOS, Horia. Bitcoin Intelligence: Business Intelligence meets Crypto Currency. **CES Working Paper**, Romenia, 2017.

BOULOS, Maged N. K. *et al*. Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare. **International Journal of Health Geographics**, [*s. l.*], 2018.

EDCHAIN. A Comparison Between 5 Major Blockchain Protocols. **Medium**, [*s. l.*], 2018. Disponível em: https://medium.com/edchain/a-comparison-between-5-major-blockchain-protocols-b8a6a46f8b1f. Acesso em: 30 set. 2019.

ELGER, Bernice S.; CAPLAN, Arthur L. Consent and anonymization in research involving biobanks. **Science e Society**, [*s. l.*], ano 7, v. 7, 2006.

FILHO, Marcio Barbosa de O. **Utilizando o protocolo Bitcoin para condução de computações multilaterais seguras e justas**. Orientador: Anjolina Grisi de Oliveira. 2016. Tese (Mestrado em Ciência da Computação) - Universidade Federal de Pernambuco, Recife, 2016.

FRUNZA, Ana; SANDU, Antonio. Formalization of Informed Consent. From Ethical to Administreative Use. **Postmodern Openings**, [*s. l.*], v. 8, n. 3, p. 66-95, 2017.

GUEDES, Christiano. Uma mulher negra, suas células e alguns desafios da ética em pesquisa. **Fio Cruz**, Manguinhos, Rio de Janeiro, v. 20, p. 1413-1416, 2013.

GUIMARÃES, Gilberto de Lima *et al.* **Possibilidades de Avaliação Epistemológica dos Programas de Pós-Graduação em Enfermagem à Luz de Karl Popper.** Texto contexto – enferm. vol. 27. Nº 4. Florianópolis: 2018. ISSN 1980-265X

KISER, Mike. Know Your Transactions - KYT. **Fine Extra**, [*s. l.*], 2018. Disponível em: https://www.finextra.com/blogposting/16446/know-your-transactions---kyt. Acesso em: 30 set. 2019.

KORTS, Külliki; WEIDON, Sue; GUÔMUNDSDÓTTIR, Magrét. Consent and anonymization in research involving biobanks. **TRAMES**, [*s. l.*], ano Estonia, 2004.

KROLL, Joshua A.; DAVEY, Ian C.; FELTEN, Edward W. The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. **WEIS 2013, Princeton University**, Washington, DC, 2013.

KUO, Tsung-Ting *et al*. Blockchain Distributed ledger technologies for biomedical and health care applications. **Journal of the American Medical Informatic Association**, [*s. l.*], 2017.

MOUGAYAR, William. **Blockchain para negócios**: Promessa, Prática e Aplicação da Nova Tecnologia da Internet. 1. ed. Brasil: Alta Books Editora, 2017.

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Eletronic Cash System. **Bitcoin White Paper**, [*s. l.*], 2008. Disponível em: https://steem.com/steem-bluepaper.pdf. Acesso em: 30 set. 2019.

ROMANO, Rafaela. Blockchain, conteúdo e recompensa de usuários de redes sociais. **Blockmaster**, São Paulo, p. 1-10, 28 ago. 2019.

SILVA, João G. S. L.; MEIRELES, Fernando. O uso de bases de dados públicos por empresas em seus sistemas de Business Intelligence e seus benefícios para o negócio. **International Conference on Information Resources Management**, [*s. l.*], 2017.

SKLOOT, Rebecca. The Immortal Life of Henrietta Lacks, the Sequel. **The New York Times**, [*S. l.*], 23 mar. 2013. Opinion, p. 1-2.

STEEM INC. A protocol for enabling smart, social currency for publishers and content businesses across the internet. **STEEM Blue Paper**, [*s. l.*], 2017. Disponível em: https://steem.com/steem-bluepaper.pdf. Acesso em: 30 set. 2019.

STEEM INC. Steem: An incentivized, blockchain-based, public content platform. **Steem White Paper**, [*s. l.*], 2018. Disponível em: https://steem.com/steem-whitepaper.pdf. Acesso em: 30 set. 2019.

TANNER, Adam. **Our Bodies, our data**: How companies make billions selling our medical records. 1. ed. Boston: Beacon Press, 2016.

TEIXEIRA, Tarcisio; ARMELIN, Ruth. **Lei geral de proteção de dados pessoais**: Comentada artigo por artigo. 1. ed. [*S. l.*]: Editora JusPodivm, 2019.

TURBAN, Efrain; KING, David; ARONSON, Jay; SHARDA, Ramesh. **Business Intelligence: Um enfoque gerencial para a inteligência do negócio**. [*S. l.*]: Bookman, 2009. 253 p.

ULRICH, Fernando. **Bitcoin, A moeda na era digital**. 1. ed. Brasil: Mises Brasil, 2014.

VON MISES, Luwidg. **A Teoria da Moeda e dos Meios Fiduciários**. Austría: [*s. n.*], 1912.