

The background is a solid blue color with a network of white lines connecting various circular icons. The icons include a calendar, a stack of coins with a dollar sign, a server rack, a Bitcoin symbol, a bar chart with an upward arrow, and a document with a checkmark. The main title is written in large, bold, yellow capital letters.

BLOCKCHAIN, INOVAÇÃO E PROTEÇÃO DE DADOS

LGPD ACADÊMICO

OBRA COLETIVA



Amanda Sousa Alencar

 amanda-sousa-alencar



Guilherme Sampaio

 melhergui



Maristela Marquiasfave

 maristela-marquiasfave-672a2a32

LGPD ACADÊMICO

Esse e-book foi desenvolvido a partir de uma iniciativa (sem fins lucrativos) que começou em agosto/2018, o grupo LGPD Acadêmico, o qual é composto por voluntários do Brasil inteiro, apaixonados pelo mundo da privacidade e com objetivo comum - aprender e compartilhar.

Por identificar uma necessidade direta da sociedade, organizações corporativas - independente do seu porte, profissionais, entre outros, por conta da Lei Geral de Proteção de Dados (Lei Nº. 13.709, de 14 de agosto de 2018) que entrará em vigor em 16 de agosto de 2020.

O LGPD Acadêmico decidiu reunir o conhecimento e experiência prática de cada autor neste material através de uma linguagem simples, evitando-se o famoso “juridiquês”, recorrendo a termos técnicos somente quando absolutamente necessário e claro, acessível a todos de maneira gratuita.

Todo material elaborado pelo LGPD Acadêmico é Licença Creative Commons - Atribuição 4.0 Internacional.

Boa Leitura!



LGDPacademicooficial.com.br



[LGDPacademicooficial](#)



[LGDPacademicooficial](#)

INTRODUÇÃO

A tecnologia blockchain, que está por trás da famosa criptomoeda Bitcoin, foi descrita por Naughton (2016) como: *"a mais importante invenção de TI da nossa era"*. Mougayar (2016) disse que *"está no mesmo nível da World Wide Web em termos de importância"*. Com essas duas afirmações e toda a propagação de notícias quanto à Bitcoin, outras criptomoedas e a constante divulgação de novos usos e inovações utilizando a tecnologia blockchain como base, podemos perceber que ainda que essas afirmações façam parte do "hype", como alguns dizem, precisamos estar de olho e acompanhar suas transformações.

Nesse e-book, abordaremos em quatro textos selecionados aspectos atuais sobre o uso da tecnologia blockchain como forma de ilustrar as transformações e inovações apresentadas para a sociedade, tratando dos conceitos fundamentais da tecnologia e seu funcionamento; sua relação com os smart contracts; sua relação com a indústria do entretenimento e suas principais incompatibilidades e perspectivas de adequação com a Lei Geral de Proteção de Dados (Lei nº. 13.709/2018), que entrará em vigor em agosto de 2020.

SUMÁRIO

O que é *blockchain*? _____ 5
Guilherme Sampaio

Aplicabilidade dos *smart contracts* _____ 12
Maristela Marquiafave

Blockchain e a indústria do entretenimento _____ 20
Guilherme Sampaio

Blockchain e proteção de dados: é possível uma
compatibilidade? _____ 23
Amanda Alencar

O QUE É BLOCKCHAIN?

Por Guilherme Sampaio

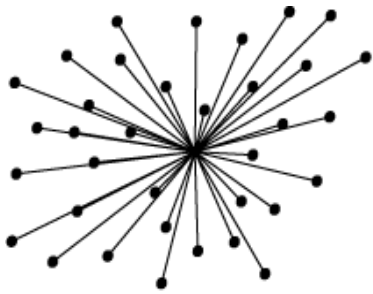
A tecnologia blockchain surgiu junto com a criptomoeda Bitcoin em meados de 2008 no artigo “*Bitcoin: A Peer-to-Peer Electronic Cash System*”, de Satoshi Nakamoto (uma figura mítica nessa história, pois ninguém sabe quem ele realmente é). Mas foi apenas em 2009 que tanto a Bitcoin quanto a tecnologia blockchain foram lançadas em código aberto para o público. Nesse momento, começaram a surgir os primeiros nós e mineradores, e a Bitcoin era abundante, ou seja, a quantidade de criptomoeda como recompensa pela mineração era muito maior.

A tecnologia blockchain foi pensada por Satoshi como uma forma segura para se transferir Bitcoins de uma pessoa para outra. A criptomoeda Bitcoin apenas aceita transferências de Bitcoins, mas a tecnologia blockchain utilizada para a criação da criptomoeda permite a transação de qualquer ativo, com um registro seguro.

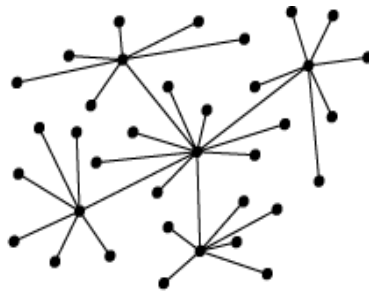
Hoje, quando fazemos transações de forma geral, precisamos de um intermediário confiável que assegure que essa transação seja concluída com sucesso. No caso das transferências monetárias, temos os bancos, que cobram altas taxas, e não funcionam de forma transparente, pois geram uma gama de cobranças e taxas que dificultam o acompanhamento fácil e ainda utilizam nossos recursos para aumentar os próprios.

Conceito

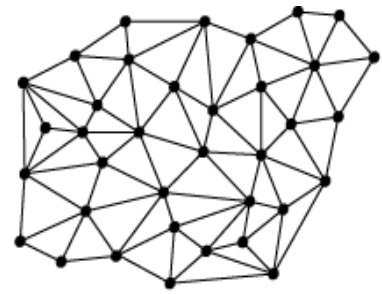
A blockchain é uma rede distribuída, na qual não existe um único intermediário para realizar e validar uma transação, muito menos alguém para cobrar altas taxas de operação. Basicamente, todos os computadores dentro dessa rede (também conhecidos como nós) precisam reconhecer a transação para ela se tornar válida.



centralised

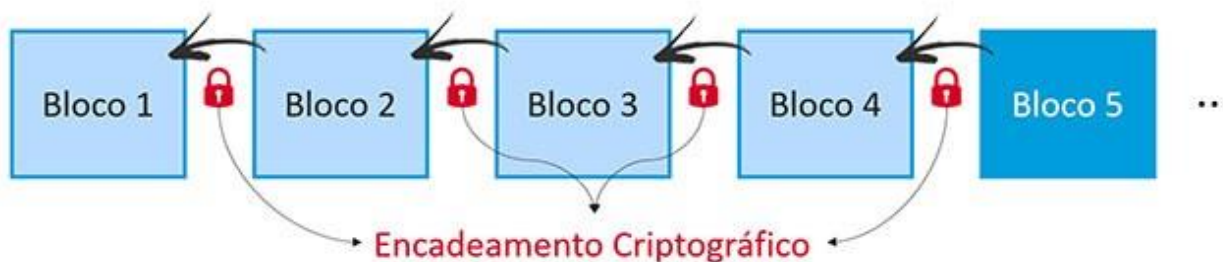


decentralised



distributed

- A unidade de informação numa blockchain é chamada de **transação**;
- Cada usuário e transação possui uma identificação própria (**endereço**);
- Dentro de uma blockchain essas transações serão agrupadas em formas de **blocos**;
- Para os blocos serem feitos é preciso respeitar algumas regras como: **um tamanho máximo de transações que um bloco pode comportar e conter apenas transações que sejam verificadas como válidas**;
- Enquanto as transações esperam para serem adicionadas em algum bloco, elas ficam temporariamente em uma estrutura chamada de **pool**;
- Os computadores da rede competem entre si para ver quem consegue encontrar um bloco válido primeiro dentro da pool (**mineração**);
- O computador que encontra um bloco válido avisa os demais para que se faça a checagem e que haja um consenso de validação;
- Quando um novo bloco válido é encontrado, o mesmo é enviado para a rede e o seu hash serve como prova de que o bloco é válido.
- O minerador é recompensado pelo seu trabalho através de incentivo financeiro;
- Após o bloco ser criado e validado pela rede, ele será adicionado a cadeia de blocos - também conhecido como **BLOCKCHAIN!**



Razões pelo hype

A razão pela qual a tecnologia blockchain ganhou tanta admiração é que:

- Não pertence a uma única entidade, por isso é descentralizada;
- Os endereços são armazenados criptograficamente dentro dela;
- A blockchain é imutável, então ninguém pode mexer com os dados que estão dentro da blockchain;
- A blockchain é transparente para que se possa rastrear os dados se eles quiserem.

Criptografia: O algoritmo de hash

O algoritmo de hash nada mais é uma função matemática que converte uma entrada de dados em uma saída que é única para aquela entrada. Ou seja, se você alterar 1 bit de informação, o hash gerado é completamente diferente, invalidando a transação.

Frase	Hash MD5
Marcos pagou 9.292,00 a Alx	6f9c6dc70406bf857b80b4e0638adab0
Marcos pagou 9.292,01 a Alx	b00da290d7d219141154dbedb1930b59

1º Passo: O registro de uma transação

O primeiro passo é o registro de uma transação. Digamos que Marcos Pianter deseje enviar dinheiro para Axl Rose. Ele envia essa requisição para a blockchain, deixando sua transação em um *pool* de transações que serão consumidas pelos mineradores para validarem as informações.

DE	PARA	VALOR
Marcos Pianter	Axl Rose	9.292,00
Jonas Matel	Marcos Bizi	123,23
Ricardo Dias	Fernanda Torres	1.040,33
Noberto Dias	Vitoria Dias	43,33
Bianca Silva	Pedro Richard	8.920,00
Mateus Cruz	Joao Dias	292,00
Marcelo Medeiros	João Franco Dias	20,00

2º Passo: Tornar a transação anônima

Assim que chega a hora de processar uma transação, tanto Marcos quanto Axl são anonimizados através de um algoritmo de hash.

ENDEREÇO DE	ENDEREÇO PARA	VALOR
dd0431de5ab97e280e	dcd2087624ef657423afb06	9.292,00
66a8279f8e7e306c9bf8	938f54e842bd99776d6ff2b	123,23
f543003c7b1e31864fe5	67c2d7ee38b7d58e8d1061	1.040,33
30257ff6a5a5c224b960	fadd731c3830d302ca98545	43,33
60268ef69af763756086	1f8861d10957458d4e4479	8.920,00
e158cdf32734343f65d5	93cc3da246e14fe49821cd4	292,00
1620063bbedce762615	5d129b9bd2151ea22f55f2	20,00

3º Passo: Tornar a transação “oficial”: O pool

Depois de anonimizadas as informações, a transação entra no pool de transações com o status de **pendente**.

ENDEREÇO DE	ENDEREÇO PARA	VALOR	STATUS
dd0431de5ab97e280e	dcd2087624ef657423afb06	9.292,00	Pendente
66a8279f8e7e306c9bf8	938f54e842bd99776d6ff2b	123,23	Pendente
f543003c7b1e31864fe5	67c2d7ee38b7d58e8d1061	1.040,33	Pendente
30257ff6a5a5c224b96c	fadd731c3830d302ca98545	43,33	Pendente
60268ef69af76375608e	1f8861d10957458d4e4479	8.920,00	Pendente
e158cdf32734343f65d5	93cc3da246e14fe49821cd4	292,00	Pendente
1620063bbedce762615	5d129b9bd2151ea22f55f2	20,00	Pendente

3º Passo: Tornar a transação “oficial”: assinatura

Para cada transação, é gerada uma assinatura através do algoritmo de hash utilizando os hash gerados anteriormente, ou seja, os endereços de quem enviou, de quem recebeu e o valor. Continuando no status pendente de processamento.

ENDEREÇO DE	ENDEREÇO PARA	VALOR	ASSINATURA	STATUS
dd0431de5ab97e280e	dcd2087624ef657423afb06	9.292,00	d991206573945515fecdd9776b6b8514	Pendente
66a8279f8e7e306c9bf8	938f54e842bd99776d6ff2b	123,23	155e4e1ca98a8bbab9708605349351e	Pendente
f543003c7b1e31864fe5	67c2d7ee38b7d58e8d1061	1.040,33	bc6a22c4f3892035665ab15e05ea2d3	Pendente
30257ff6a5a5c224b96c	fadd731c3830d302ca98545	43,33	4913e03e9f343d8f6a08610b92e356b	Pendente
60268ef69af76375608e	1f8861d10957458d4e4479	8.920,00	2f21a9bfda4d2e24137b3e80c7abe3c	Pendente
e158cdf32734343f65d5	93cc3da246e14fe49821cd4	292,00	8f23cb2da92cc58344b0523477985f65	Pendente
1620063bbedce762615	5d129b9bd2151ea22f55f2	20,00	81d16bd0172d2e021c101d3c553ab9f	Pendente

3º Passo: Tornar a transação “oficial”: Validação

Depois, é hora de validar a assinatura da transação com as informações contidas nela para descobrir se foi alterada de alguma forma. Caso não tenha sido, a transação ganha o status de OK, recebe uma data e hora de processamento e essas informações são utilizadas para gerar o ID da transação.

ENDEREÇO DE	ENDEREÇO PARA	VALOR	ASSINATURA	STATUS	DATA-HORA	TRANSACTION ID
dd0431de5ab97e	dcd2087624ef657423a	9.292,00	d991206573945515fe	OK	2017-01-10 18:23:22	32b66448fed65314ce5d4c1eca917f6e
66a8279f8e7e306	938f54e842bd99776d6	123,23	155e4e1ca98a8bbab	OK	2017-01-10 18:23:22	b1d015975a200bbf0e4069932f89c5b9
f543003c7b1e318	67c2d7ee38b7d58e8d	1.040,33	bc6a22c4f389203566	OK	2017-01-10 18:23:22	b35f941bd0942ffa64bfaa47b50d4123
30257ff6a5a5c224	fadd731c3830d302ca9	43,33	4913e03e9f343d8f6a	OK	2017-01-10 18:23:22	b3758bc58ded77a199f4148259c72be9
60268ef69af7637	1f8861d10957458d4e4	8.920,00	2f21a9bfda4d2e2413	OK	2017-01-10 18:23:22	e3ca68c49f0e78acb7d8324202e85f4f
e158cdf32734343	93cc3da246e14fe4982	292,00	8f23cb2da92cc58344	OK	2017-01-10 18:23:22	4f5b7bb1d3f3e73121ff59538469d977
1620063bbedce7	5d129b9bd2151ea22f5	20,00	81d16bd0172d2e021	OK	2017-01-10 18:23:22	a637e27540bafcddee51ca225d35cb754

4º Passo: Tornar a transação imutável: O hash das transações

Ao chegar no tamanho máximo do bloco, é gerado um hash das transações que fazem parte daquele bloco. Além do ID das transações, é utilizado também o ID do novo bloco que está sendo gerado.


TRANSACTION ID	BLOCO	HASH DO TRANSAÇÕES
32b66448fed65314ce5d4c1eca917f6e	54	c33e8f2391c2e883dfd3a06f9030aad7
b1d015975a200bbf0e4069932f89c5b9	54	
b35f941bd0942ffa64bfaa47b50d4123	54	
b3758bc58ded77a199f4148259c72be9	54	
e3ca68c49f0e78acb7d8324202e85f4f	54	
4f5b7bb1d3f3e73121ff59538469d977	54	
a637e27540bafcddee51ca225d35cb754	54	

5º Passo: Tornar a transação imutável: O hash do bloco

Todos os blocos possuem o número do bloco, as transações, o hash das transações e o hash do bloco anterior, gerando assim o hash final daquele bloco que será utilizado

para conectar e validar o bloco na blockchain. O único bloco que não possui hash do bloco anterior é o bloco gênese, ou seja o primeiro bloco da blockchain.

TRANSACTION ID	BLOCO	HASH DO TRANSAÇÕES	HASH DO BLOCO ANTERIOR	HASH FINAL
148b2dfc47cf46be3840f80c826fea75	53			
84cd62a6425b38d228ef29869dfb0897	53			
aad6c875b15b126741c85c9fdd37a4f9	53			
fa59c2996d445ebce84710948aac288	53	bdc5ef6b47177f56b18109aeb2317625	3346c4e052de08901daf6151c188c640	000b7d7e471af96494565613141df45d
01b8bedfc29bc61608b89e1ef300345e	53			
fba9ca1450a5477e8de461f5e6fa2af2	53			
6ceda1ffaa097890088163d32bf1aea0	53			
32b66448fed65314ce5d4c1eca917f6e	54			
b1d015975a200bbf0e4069932f89c5b9	54			
b35f941bd0942ffa64bfaa47b50d4123	54			
b3758bc58ded77a199f4148259c72be9	54	c33e8f2391c2e883dfd3a06f9030aad7	000b7d7e471af96494565613141df45d	6c35b3e1e30a17ca14e997dc5ab11c16
e3ca68c49f0e78acb7d8324202e85f4f	54			
4f5b7bb1d3f3e73121ff59538469d977	54			
a637e27540bafcddee51ca225d35cb754	54			



Desta forma a tecnologia blockchain garante que:

- Absolutamente todos os registros do banco de dados estão entrelaçados. Logo, podemos analisar todo o histórico de mudanças e alterações nas informações sabendo exatamente quando, onde, e quem estava envolvido nestas operações;
- Mesmo que alguém consiga alterar uma cópia local para enganar a blockchain, jamais conseguiria oficializar isso frente as demais cópias do blockchain, pois, para enganar, teríamos que alterar todos os blocos anteriores para que os hashes estejam em conformidade;
- Para garantir que realmente um bloco está seguro, a blockchain pode ser programada para ter um limite, esperando que um bloco apenas é válido depois que mais N blocos sejam validados, validando a cadeia anterior ao bloco.

APLICABILIDADE DOS SMART CONTRACTS

Por Maristela Marquiafave

Atualmente experimentamos a chamada Revolução Industrial 4.0, que avança exponencialmente e que em menos de dez anos trouxe ao mundo uma inovação sem precedentes, transformando todos os setores da economia através do uso da tecnologia.

Sabemos, no entanto, que este não foi sempre o ritmo das mudanças. Mais de dois séculos foram necessários para que três grandes revoluções de forte impacto para o cenário socioeconômico global se desenvolvessem, diga-se de passagem, linearmente, e se concretizassem: a invenção da máquina a vapor, o advento da eletricidade e o desenvolvimento da computação.

Uma longa estrada foi percorrida para que definições até então desconhecidas, como blockchain, criptoativos, inteligência artificial, robótica, internet das coisas, pudessem ser hoje debatidos em larga escala e compreendidos por nossa geração, o que comprova estarmos diante de um caminho inovador sem volta. E em meio a tamanha inovação, modificam-se exponencialmente também as relações humanas e a forma como as partes de uma relação contratual adquirem direitos e assumem obrigações, surgindo espaço para o uso dos *smart contracts* (ou contratos inteligentes).

Smart contracts: como essa ideia surgiu?

Não podemos falar de *smart contracts* sem antes citar o cientista da computação americano Nick Szabo, que instituiu o referido termo em 1994, ao afirmar que: “*A smart contract is a computerized transaction protocol that executes the terms of a contract*”, o que em livre tradução define um *smart contract* como nada mais que um protocolo de transação informatizado que executa os termos de um contrato.

Em 1997, através de um artigo¹ publicado na revista acadêmica *First Monday*, Szabo trouxe à tona uma nova forma de pensar os tradicionais contratos através de

¹ <https://firstmonday.org/ojs/index.php/fm/article/view/548>

códigos computacionais, buscando maior segurança e proteção para as partes. A tradução livre do resumo de seu artigo assim detalha o centro de suas ideias: *“Smart contracts combinam protocolos com interfaces de usuários para formalizar e assegurar as relações em redes de computadores. Objetivos e princípios para o design desses sistemas são derivados dos princípios legais, teoria econômica e teorias de protocolos confiáveis e seguros. Similaridades e diferenças entre os smart contracts e os procedimentos de negócios tradicionais baseados em contratos escritos, controles e formulários estáticos são discutidas. O uso de criptografia e outros mecanismos de segurança podem trazer proteção a muitas relações especificadas por algoritmos contra violações de princípios e de interceptação ou interferência maliciosa de terceiros, até considerações de tempo, interface do usuário e integridade da especificação algorítmica”*.

Essa teoria teria sido pensada através da análise das *vending machines*, pois se traçarmos um paralelo, estamos “contratando” com referidas máquinas ao compramos um refrigerante, por exemplo, mediante várias cláusulas pré-estabelecidas: (i) escolha do produto; (ii) depósito do valor estabelecido na máquina para aquisição daquele produto; (iii) liberação do produto pela máquina mediante pagamento do valor correto; (iv) devolução de troco devido a eventual depósito de valor a maior. Com isso, resta adimplida e executada a transação, sem a intervenção de terceiros.

É nítido, pois, que Szabo vislumbrou um aperfeiçoamento deste tipo de transação, buscando uma forma mais segura (com o uso de criptografia) e rápida de se contratar, imutável, autoexecutável e sem a necessidade de intermediários. A dificuldade neste aperfeiçoamento estaria apenas no fato de que de que à época ainda não se falava em blockchain, tampouco em criptomoedas, razão pela qual a efetiva viabilização da ideia viria a acontecer apenas alguns anos mais tarde.

Satoshi Nakamoto e o Bitcoin

Somente em 2009, com a divulgação do *paper* de Satoshi Nakamoto (em teoria o pseudônimo de uma pessoa ou de um grupo de pessoas) denominado *“Bitcoin: A Peer-*

to-Peer Electronic Cash System”² é que surge o criptoativo *Bitcoin* (BTC) e a tecnologia blockchain, trazendo finalmente as condições necessárias para o desenvolvimento dos *smart contracts* em seu formato atual.

Um grande avanço a ser atribuído ao BTC foi a solução do problema do “gasto duplo”, não sendo possível simplesmente “copiar” o dinheiro digital e usá-lo mais de uma vez, como ocorre com o envio de uma fotografia digital, pois as transações se dão em sua rede pública descentralizada, auditável e com código fonte aberto, sem a necessidade de um terceiro controlador, graças à confiança criptográfica embasada no consenso entre os membros da rede, apta a validar as transações e os saldos das contas de seus usuários.

Essa solução do problema do “gasto duplo” conferiu à rede do BTC a confiabilidade de tal sistema monetário e a segurança tão debatida por Nick Szabo, o que muito nos importa para o tema dos *smart contracts*.

Ainda, vale dizer que a blockchain do BTC (assim como as demais), é uma camada de tecnologia que roda em cima da internet, assim como a nossa velha conhecida *www* (*World Wide Web*) e mantém uma transparência sem igual via *ledger* de transações (uma espécie de “livro-razão”) com todas as operações registradas com horário e por ordem cronológica, desde o início de sua operação.

Isso possibilita que a blockchain prove algo que realmente aconteceu, representando um novo paradigma para implementação da confiança nas transações, computada por máquinas.

Vitalik Buterin e o Ethereum

Em 2013, o programador russo Vitalik Buterin, então com 19 anos de idade, sob o argumento de que a rede do *Bitcoin* precisava de uma linguagem mais generalizada, apresenta o *white paper* da rede *Ethereum*, rede descentralizada e capaz de executar *smart contracts*, também com código fonte aberto³, tendo sido o projeto financiado através de *crowdfunding*, com lançamento efetivo em 2015.

² <https://bitcoin.org/bitcoin.pdf>

³ <https://github.com/ethereum/wiki/wiki/White-Paper>

Como na blockchain do *Bitcoin*, as características principais da rede *Ethereum* são similares, sendo que ela também armazena as transações numa espécie de planilha pública, distribuída e criptografada, validadas pelos próprios usuários da rede. No entanto, contratos inteligentes formalizados na blockchain do Ethereum não são pagos em *Bitcoins*, mas sim em *Ether*, a “moeda” da rede.

Definição e conceitos dos smart contracts

Muito se discute sobre a nomenclatura dos *smart contracts*, pois na prática, podemos dizer que os mesmos não são contratos e nem são inteligentes, eis que se referem a meras linhas de código de programação, prévia e objetivamente definidas, não sendo capazes de “aprenderem” nem executarem tarefas de forma autônoma, mas apenas darem cumprimento aos comandos de quem os programou.

Logicamente podemos considerá-los inteligentes quando confrontados com os tradicionais padrões de contratos, mas ao avaliarmos juridicamente o seu conceito, vamos chegar à rápida conclusão de que a mudança causada pelos *smart contracts* na verdade representam apenas o momento final da negociação, mais precisamente o seu *enforcement*.

Uma boa definição para os *smart contracts* seria: **códigos de programação publicados em uma rede blockchain, com capacidade de automatizar e auto executar suas negociações desde que cumpridas as condições impostas, de forma imutável, segura, transparente e sem intervenção humana.**

Com relação à estrutura e funcionamento dos *smart contracts*, a blockchain do Ethereum é a mais utilizada e um dos projetos mais famosos no setor de contratos inteligentes, trazendo condições especiais para seu desenvolvimento e execução, criando uma espécie de “máquina virtual” em que as partes podem desenvolver e aplicar suas regras.

O ponto que diferencia de fato o *Ethereum* dos demais *altcoins* (criptoativos alternativos ao *Bitcoin*) é que o mesmo busca difundir a tecnologia do blockchain e a adoção de contratos inteligentes para “qualquer situação a ser programada”.

A linguagem de programação mais utilizada é o *Solidity*, sendo o *Remix* a melhor ferramenta para redigir e publicar os contratos. O *Ether* é o “combustível” da plataforma, apto a possibilitar que as transações se realizem e que o contrato se implemente.

O passo a passo para o funcionamento e aplicabilidade dos smart contracts

A fim de melhor compreender o funcionamento dos *smart contracts*, importante apresentarmos alguns detalhes de sua figura:

1 - **Programação:** é recomendado que programador e advogados representantes das partes trabalhem juntos e programem com muita cautela o encadeamento exato, bem como a lógica das funções a serem realizadas, não devendo restar brechas para qualquer tipo de dúvida no ato da execução do contrato, pois a partir do momento em que todas as cláusulas forem adimplidas, a função nele descrita será executada.

Podemos pensar como exemplo no cenário do *e-commerce*, que é um grande potencial para o uso de contratos inteligentes e possui um processo bastante simples. Pensemos na comercialização de um sapato feita por um indiano a um brasileiro. Em razão da demora no frete e na possibilidade da não concretização deste negócio, seria possível a efetivação de um *smart contract* previamente programado e validado, com o rastreio dos Correios ou transportadora envolvida, sendo que, havendo a confirmação do recebimento dos produtos pelo consumidor, dar-se-ia automaticamente a execução do contrato e a transferência do pagamento.

Esta é apenas uma possibilidade, sendo que o mercado de seguros, financeiro, registros societários, métodos de votação, mobilidade, hospedagem, serviços cartorários, dentre inúmeros outros, podem envolver a formalização de contratos inteligentes.

Logicamente, a etapa de discussão da minuta do documento e o estabelecimento de suas cláusulas, bem como regras e consequências exatas da relação jurídica (direitos, deveres, penalidades em caso de descumprimento etc.) ainda exigem

formalização via modelos tradicionais, o que possibilitará o *self-enforcement* preciso do *smart contracts*.

2 - Implementação: após sua programação, será feito o *deployment* do contrato na plataforma de computação (rede distribuída) baseada em blockchain público, uma espécie de *upload* do documento, o que permitirá sua execução em uma única máquina virtual descentralizada denominada EVM - *Ethereum Virtual Machine*, no caso da rede *Ethereum*.

Seria, em outras palavras, a transcrição de todas as cláusulas do contrato, através de uma plataforma computacional, para que as condições possam estar claramente estabelecidas e serem oportunamente implementadas e satisfeitas.

3 - Concretização: a rede distribuída possui seu próprio criptoativo (neste caso específico, o *Ether*), que funciona como o “combustível” que o contrato precisa para ser “minerado” e executado. O adimplemento dessa transação se dá mediante o envio de criptoativos da carteira de uma parte para outra e essa transação deverá ser validada pelos nós da rede, no chamado mecanismo de consenso, o que se dá através do processo de mineração e prova de trabalho - *Proof of Work* (PoW).

4 - Mineração: este processo é uma espécie de “tentativa e erro”, no qual os “mineradores” espalhados pelo mundo participam de um “jogo” de decodificação criptográfica e buscam acertar a hash (sequência de caracteres - números e letras aleatórios, por exemplo, ‘344dcc402944e2b3’) de validação daquela transação e, ao acertarem, são responsáveis por aquele específico registro no próximo bloco de dados e na rede blockchain, o livro-razão coletivo. Todo bloco sucessivo conterá o hash do bloco anterior, para que não se quebre a cadeia de confiabilidade e segurança da rede. O uso da tecnologia de criptografia garante a não modificação, minimizando o risco de perdas.

Logicamente quanto mais potentes as redes computacionais destes mineradores (ou *pool* de mineradores), maior a probabilidade de acerto, pois o processo envolve manter os computadores pensando, calculando e procurando hashes até desvendar um bloco, validá-lo e receber a recompensa tarifada pela respectiva rede.

5 - **Autoexecução:** findo este processo de negociação, *deployment*, validação e registro pela rede, estando as condições do contrato adimplidas, ocorrerá o seu *enforcement* e, conseqüentemente, a satisfação das partes envolvidas.

A disseminação dos smart contracts no futuro

Diante desse contexto, podemos concluir que temos vivenciado uma excitante jornada disruptiva e de inovação sem precedentes, sendo possível atrelar as relações humanas e, neste particular o Direito, ao ramo da Tecnologia.

Imaginemos um futuro de amplas relações *peer-to-peer*, sem grandes empresas dos principais setores intermediárias e detentoras do poder, mas sim com códigos abertos e gratuitos, de interfaces simples, seguros e autoexecutáveis, perpetuados de forma imutável em uma cadeia de blocos assegurada pelos seus próprios nós validadores, podendo prever variados tipos de serviços, logicamente pensados dentro dos padrões adequados ao mundo jurídico vigente.

O objetivo central das pessoas que hoje detêm o conhecimento e estão à frente deste cenário é justamente buscar o protagonismo e a mudança gradativa do *mindset* comum e dos antigos modelos sócio-político-econômicos, abolindo os pontos de atrito do sistema tradicional, em busca de economia de tempo e recursos.

Necessário também que as barreiras legais e regulatórias sejam superadas e ajustadas aos poucos, sempre na busca do equilíbrio entre a evolução do mercado e o controle dos gargalos existentes.

Para os profissionais do Direito, é importante disseminar este conhecimento e a viabilidade cada vez maior para o uso dos *smart contracts*, rompendo a ideia de que este modelo será prejudicial à função do advogado e fomentando as inúmeras novas possibilidades de negócios que podem surgir neste ambiente. Lembremos as palavras do próprio idealizador do conceito, Nick Szabo, que ao discursar em 2016 num simpósio em Nova Iorque, afirmou que os contratos inteligentes não irão tomar o lugar dos advogados, mas sim “possibilitar coisas novas que não foram ainda realizadas anteriormente”.

É importante que tenhamos passado a ideia de que hoje não estamos mais diante da era da internet da informação, mas sim da internet do valor, em que transações precisam ocorrer de forma *online*, com rapidez, segurança e transparência, sendo as redes blockchain e os contratos inteligentes os grandes responsáveis por essa concretização, em busca da modernização do cenário até então praticado e da adaptação dos novos modelos econômicos e sociais a um cenário jurídico confiável.

Para corroborar esse pensamento e essa ânsia por mudanças, enumeramos cinco grandes vantagens dos *smart contracts*: (i) **segurança** (criptografia); (ii) **redução de custos** (menor intervenção humana); (iii) **velocidade** (ações rápidas e em tempo real); (iv) **precisão** (100% programados por códigos); e (v) **transparência** (auditáveis).

É notório, pois, que o futuro nos reserva grandes oportunidades no contexto da inovação tecnológica em todos os âmbitos, avançando-se a disrupção através das novas empresas, segmentos e comportamentos, bem como dos novos padrões dentro das empresas e negócios já existentes, todavia, ameaçados diante do atual cenário.

Cabe a nós, atores desta transformação, o atingimento consciente e responsável das novas práticas, buscando o casamento perfeito entre Tecnologia e Direito, sem nos esquecer que por trás dos *smart contracts* e de todo o futuro tecnológico que desponta, os relacionamentos interpessoais e valores pessoais serão as ferramentas de maior importância, aptas a nos diferenciar das máquinas no mercado daqui em diante.

BLOCKCHAIN E A INDÚSTRIA DO ENTRETENIMENTO

Por Guilherme Sampaio

A indústria de mídia e entretenimento é baseada em contratos que valorizam a proteção da propriedade intelectual. A blockchain tem o potencial de aumentar os lucros para criadores de conteúdo e empresas de mídia e fornecer preços baseados em consumo em tempo real. À medida que a tecnologia blockchain amadurece, os executivos de mídia e entretenimento devem estar aprendendo sobre a tecnologia e os possíveis casos de uso para seus negócios.

Entender como o blockchain atua na estratégia mais ampla da empresa, quais são as prioridades da empresa e se o modelo de negócios pode ser significativamente impactado pela tecnologia será essencial. Embora a tecnologia ainda seja nova, ela tem aplicativos para toda a indústria com o potencial de transformar a maneira como o conteúdo é criado, consumido e protegido. Além disso, é importante começar a pensar nos possíveis benefícios e desafios da adoção agora.

As principais disrupções que podem ser causadas pela união da indústria do entretenimento e a blockchain são: a eliminação de intermediários, distribuição de royalties, compartilhamento de ativos e vendas consumidor-consumidor.

Eliminação de intermediários

A estrutura descentralizada da blockchain poderia permitir que os criadores de conteúdo - como músicos ou escritores - distribuíssem diretamente seu trabalho para os consumidores, ignorando os canais de distribuição tradicionais e deixando uma parcela maior de receita para os próprios criadores de conteúdo. Isso poderia impactar todos, desde grandes meios de comunicação até “blogueiros” independentes, ajudando os artistas a formar um relacionamento direto com os consumidores.

Distribuição de royalties

A coleta e distribuição de pagamentos de royalties no setor musical se tornou ainda mais complexa com o crescimento dos serviços de *streaming* de música. Cada

vez que uma música é transmitida online ou reproduzida em segundo plano de um programa de TV, por exemplo, o distribuidor deve compensar o detentor dos direitos autorais da música, mas podem surgir controvérsias sobre a precisão e as taxas de compensação desses royalties.

Contratos inteligentes construídos em uma blockchain e anexados a uma determinada peça musical podem adicionar precisão, velocidade e confiança ao processo, executando termos de contrato automaticamente entre as partes elegíveis. Isso permitiria um rastreamento mais preciso do uso de uma música, pagamentos mais rápidos de royalties e mais transparência sobre os termos do contrato e a divisão da receita entre artistas e outras partes interessadas. É provável que também interrompa ou elimine o papel das associações de cobrança de direitos autorais, que atualmente atuam como intermediários centralizados na coleta de pagamentos para detentores de direitos.

Vendas consumidor-consumidor

Assim como o acompanhamento aprimorado do uso de músicas, o uso de blockchain poderia capacitar outros tipos de proprietários de conteúdo a manter uma melhor supervisão de seu material protegido por direitos autorais. O compartilhamento de arquivos *peer-to-peer* ilegal de programas de TV, filmes ou outros conteúdos já é comum, mas o compartilhamento de arquivos pode se tornar uma prática legítima que pode ser controlada e monetizada. Quando os consumidores compram ou assinam conteúdo hospedado por blockchain e o compartilham com um amigo, os proprietários do conteúdo podem acompanhar e cobrar uma taxa por essa distribuição. Isso criaria um fluxo de receita adicional para os criadores de conteúdo e forneceria uma melhor transparência sobre como os recursos protegidos por direitos autorais são consumidos e compartilhados.

Micro vendas de ativos

Uma tendência crescente que têm origens no *crowdfunding* e que pode ajudar muito a todos os profissionais e empresas do mercado é a micro venda de ativos. Hoje temos pinturas famosas como de Picasso que foram transformadas em milhões de micro

ações e vendidas por valores menores por conta da quantidade, abrindo caminho para micro investidores ou pequenos mecenas.

Essa transformação pode ser feita com qualquer ativo, principalmente os criados pela indústria do entretenimento, onde a maioria dos produtos é virtual. E não é só com produtos lançados que essa estratégia artística pode ser implementada, ela serve para qualquer ideia! Ou seja, um artista poderia usá-la como um *crowdfunding* para seu próximo álbum! E imagine se além de conseguir o valor para produzir seu novo álbum, ele se torne um sucesso e todos os fãs que lhe ajudaram no começo, que hoje são seus sócios em seu álbum de sucesso, estarão compartilhando não só da alegria de um projeto bem sucedido, mas também de seus lucros!

Conclusão

A blockchain pode criar fluxos de receita adicionais para conteúdo novo e existente e maior proteção da propriedade intelectual do conteúdo para os proprietários do conteúdo. Mas a tecnologia ainda não está madura e essas aplicações ainda estão sendo desenvolvidas. Os primeiros adeptos devem estar cientes dos desafios e custos potenciais. O uso de blockchain atualmente não é regulamentado, e padrões comuns para utilizar a tecnologia para criar valor ainda precisam ser criados. *“Para qualquer caso de uso adequado de blockchain que exija a participação de múltiplos constituintes, é necessário que haja uma condução de padrões entre esses participantes”*, diz Moy.

Além disso, alcançar todos os benefícios da blockchain pode exigir a substituição da tecnologia atual em certos casos. Integrar a tecnologia em processos existentes - e construir, testar e garantir a segurança - levará tempo. Há também a questão de onde toda essa propriedade intelectual será armazenada. As quantidades massivas de dados de transações precisarão ser armazenadas com terceiros e, nesse caso, quem é o proprietário desses imóveis? Enfrentar essas questões e encontrar um terreno comum levará tempo. É importante que os participantes da indústria de mídia trabalhem no desenvolvimento de padrões para aplicar blockchain e identificar áreas nas quais a tecnologia poderia beneficiar os principais participantes do setor, de criadores de conteúdo a agregadores de conteúdo e distribuidores.

BLOCKCHAIN E PROTEÇÃO DE DADOS: É POSSÍVEL UMA COMPATIBILIDADE?

Por Amanda Alencar

A tecnologia blockchain vem causando ao longo dos últimos anos uma verdadeira revolução, com soluções bastante inovadoras sendo experimentadas, que vão muito além das criptomoedas. Entretanto, em meio a exaltação quanto aos diferentes usos da tecnologia, ecoam questionamentos e debates acerca da sua compatibilidade quanto a outro tema bastante destacado nos últimos anos: a proteção de dados pessoais. Isso porque a tecnologia blockchain, da forma como foi originalmente pensada por Satoshi Nakamoto, se caracteriza por ser uma base de dados descentralizada, com total transparência e publicidade das informações inseridas, as quais são armazenadas de maneira imutável, sem a possibilidade de qualquer alteração posterior. Tais características, em uma primeira análise, parecem ser inconciliáveis com os principais critérios relacionados à proteção de dados pessoais, o que gera várias discussões acerca da compatibilidade e viabilidade da tecnologia quanto às normas de proteção de dados hoje aplicáveis.

Considerando esse contexto, abordaremos as características dessa classe de tecnologia no intuito de analisar se a mesma pode ser compatível com as principais disposições e princípios da Lei de Geral Proteção de Dados brasileira (LGPD), Lei nº. 13.709/2018, bem como do General Data Protection Regulation (GDPR), o Regulamento de proteção de dados da União Europeia, considerando o uso de dados pessoais, as características técnicas dos tipos de blockchain existentes e o exercício dos direitos do titular de dados, abordando, por fim, as possíveis soluções para uma desejável compatibilidade.

O uso de dados pessoais e a anonimização de dados em blockchains

O primeiro aspecto a ser enfrentado diz respeito ao uso de dados pessoais numa blockchain. Nos termos da Lei de Geral Proteção de Dados brasileira (LGPD), bem como

do General Data Protection Regulation (GDPR), o conceito de dados pessoais é bastante amplo, sendo considerado um dado pessoal aquele que possa tornar um indivíduo identificado ou identificável. Aqui reside a primeira observação e um dos principais problemas em relação aos dados pessoais e as blockchains: ainda que seja inserido um dado que não possa identificar diretamente um indivíduo, o seu uso recorrente ou a sua associação com outras informações torna o indivíduo identificável, o que fará incidir a aplicação das leis de proteção dos dados.

Um exemplo bastante comum é o endereço utilizado por um usuário numa blockchain, o qual representa um código criptográfico gerado por sua chave pública e que, conseqüentemente, não permite que o titular de dados seja identificado de forma direta. Entretanto, o uso recorrente do mesmo endereço, juntamente com outras informações que podem ser relacionadas com a chave pública, torna o titular de dados identificável, o que faz com que tanto o endereço quanto a chave pública correspondam a um dado pessoal. Tal situação é especialmente fácil de ser apresentada em uma blockchain pública, pois todas as transações do endereço podem ser visualizadas livremente, facilitando a rastreabilidade de informações.

Outra importante discussão seria quanto a possibilidade de anonimização dos dados. Tanto a LGPD, quanto o GDPR não se aplicam a dados anonimizados, que são dados que passaram por um processo em que perdem a possibilidade de associação ao titular. O procedimento pode ser uma solução em termos de proteção de dados em uma blockchain, no entanto, os requisitos técnicos que fazem corresponder uma anonimização de dados de forma efetiva podem ser rigorosos. De acordo com o Article 29 Working Party⁴ (Opinion 05/2014⁵), a técnica de anonimização deve ser suficientemente boa para que não seja possível haver reversão ou mesmo a associação com os dados pessoais originais a partir de outras informações disponíveis, o que, do contrário, tornará o titular de dados identificável. Assim, ainda que os dados sejam criptografados, há a possibilidade de reversão (uso da chave) e ainda o risco de associação a partir de outras informações, o que os tornará, portanto, apenas pseudoanonimizados.

⁴ Órgão europeu consultivo para proteção de dados anterior a vigência do GDPR.

⁵ Article 29 Working Party, “Opinion 05/2014 on Anonymisation Techniques”.

Importante lembrar que os mais diversos tipos de blockchains têm em comum a larga utilização da chamada função hash criptográfica, que é utilizada principalmente para encadear de forma bastante segura os blocos de informações um ao outro e na qual não é possível haver reversão. A função hash é usualmente comparada a uma impressão digital de um bloco de informações, pois o resultado gerado é único, de forma que a mínima alteração, seja de um bit sequer, no bloco de informações corresponderá a um resultado da função hash completamente diferente.

Mesmo considerando a característica de irreversibilidade da função hash, a discussão é ainda bastante controversa quando se trata de dado pessoal que foi “hasheado” antes de ser inserido numa blockchain. Como ressaltado no relatório do European Union Blockchain Observatory and Forum⁶, se o tamanho da informação for conhecido e for relativamente pequeno (um número de CPF, por exemplo), existe a possibilidade de ataque de força bruta, utilizando as possibilidades disponíveis e comparando-as com o resultado pretendido para se chegar ao dado original.

Há ainda o risco de vinculação ao titular de dados. Como já mencionado, os registros em uma blockchain ficam disponíveis de forma bastante transparente, tornando possível a rastreabilidade e agrupamento de outras informações e, conseqüentemente, facilitando a associação com o titular de dados, sendo esse um dos principais riscos de identificação do titular, ainda que não tenha sido inserido os seus dados pessoais diretamente numa blockchain. Na última seção, veremos quais as possibilidades para mitigar estes riscos.

Os diferentes tipos de blockchain e a responsabilidade pelo tratamento de dados pessoais

Além das discussões a respeito da inserção de dados pessoais, também a característica da descentralização de registro torna muito mais difícil a interpretação das normas de proteção de dados em blockchains. Isso porque a descentralização torna difícil a indicação do controlador responsável em blockchains e essa definição também pode variar bastante a depender do tipo de blockchain utilizada. O controlador, nos termos na Lei Geral de Proteção de Dados (artigo 5º, VI), é aquele a quem competem as decisões

⁶ European Union Blockchain Observatory and Forum, “Blockchain and the GDPR”.

referentes ao tratamento de dados pessoais. A definição do controlador é essencial em termos de responsabilização, mas se mostra particularmente desafiadora quando se trata de um sistema que tem múltiplos participantes, com uma base de dados descentralizada.

Em blockchains privadas e permissionadas, que são geralmente formadas por consórcios de empresas, é mais fácil aplicar a definição de controlador, pois os participantes (os “nós”) são conhecidos, inseridos de forma controlada, além de geralmente existir uma relação pré-contratual que permite a definição das responsabilidades de cada participante. Entretanto, as blockchains permissionadas também possuem desafios, uma vez que todos os participantes da rede precisam ter acesso às informações inseridas nos blocos e, como consequência, terão acesso aos dados pessoais. Além disso, de acordo com as normas de proteção de dados, é preciso definir corretamente a base legal que autorizará o tratamento de dados de acordo com as finalidades estabelecidas por todos os nós participantes.

Por outro lado, a maior dificuldade reside em relação as blockchains públicas e não permissionadas, que hoje correspondem a grande maioria das blockchains em uso, como as blockchains de criptomoedas. Qualquer pessoa pode, sem nenhuma permissão necessária do sistema, atuar na rede como um nó validador ou apenas um nó participante (o qual possui uma cópia da base de dados). Assim, uma vez que não há controle dos participantes, como determinar quem seria o controlador e o operador nesses casos, segundo as normas de proteção de dados? O debate nesses casos ainda permanece inconclusivo, apesar de algumas opiniões já expressadas. A CNIL, autoridade francesa de proteção de dados, já apresentou relatório⁷ no qual considera, de maneira geral, os participantes de uma blockchain não permissionada como responsáveis pelo tratamento de dados pessoais. No entanto, o maior desafio não é definir essas responsabilidades e sim aplicá-las.

Quando há um controlador definido de forma mais clara, que faz a coleta dos dados de acordo com uma base legal definida, inclusive antes do início das atividades da blockchain, se mostra muito mais fácil identificar também, a partir daí, suas obrigações. Em outros casos, é necessária uma melhor orientação das autoridades de proteção de

⁷ CNIL, “Solutions for a responsible use of the blockchain in the context of personal data”.

dados, o que certamente levará a uma análise a ser desenvolvida caso a caso, a depender da configuração e características da blockchain e da forma de participação dos nós validadores.

O exercício dos direitos do titular de dados

Outro questionamento se dá sob a perspectiva do titular de dados, no qual é preciso analisar se o uso da tecnologia blockchain permite ao mesmo o exercício dos direitos resguardados nas leis de proteção de dados, especialmente os direitos de acesso, correção e eliminação dos dados.

Aqui reside outro grande desafio quanto à proteção de dados pessoais numa blockchain, que tem relação com uma de suas principais características: a imutabilidade. Como visto anteriormente, a alteração das informações contidas num bloco invalida o encadeamento de blocos, uma vez que a mínima alteração necessária altera também o código resultante da função hash, o principal responsável pela segurança do encadeamento. Assim, o cumprimento das obrigações de eliminação e correção de dados pessoais pode se tornar tecnicamente desafiador.

Segundo relatório da CNIL, determinadas técnicas de encriptação em conjunto com a destruição das chaves privadas podem ser consideradas como apagamento de dados. Assim, ainda que tecnicamente os dados não sejam apagados, a solução é que não se tenha mais possibilidade de acesso aos mesmos. No entanto, tal definição de forma conclusiva sobre o que pode ser considerado eliminação para o cumprimento das normas quanto a eliminação de dados pessoais ainda está em discussão e necessita também ser estabelecida pelas autoridades de proteção de dados pessoais.

Como visto anteriormente, no caso de blockchains públicas e não permissionadas se mostra especialmente complexo o cumprimento dessas obrigações, pois é difícil a definição do controlador e o consequente cumprimento das obrigações necessárias quanto aos direitos do titular de dados. Por isso, é de extrema importância colocar em prática soluções técnicas que possam eliminar o risco de acesso, que permitam a efetiva anonimização dos dados.

Considerações finais: quais as soluções possíveis?

Como ressaltado no recente relatório do Parlamento Europeu⁸, em primeiro lugar deve-se considerar que a tecnologia blockchain deve ser vista como uma classe de tecnologia, uma vez que não existe uma única versão disponível, com as mesmas características. Por este motivo, não há como definir uma única solução de adequação aos principais requisitos das leis de proteção de dados que possa ser utilizada de forma universal em diferentes tipos de blockchain. A análise de adequação deve ser realizada em cada caso particular e deve procurar observar os aspectos relacionados a estrutura técnica da blockchain utilizada, bem como a forma que se faz uso de dados pessoais. Isso deve ser feito sempre com apoio técnico avançado, e, quando possível, seguindo as diretrizes a serem estabelecidas pela Autoridade Nacional de Proteção de Dados.

No caso de ser absolutamente necessária a inserção de dado que possa identificar o seu titular, pode-se citar como exemplo de mitigação de riscos o uso da função hash (criptação não reversível) juntamente com técnicas como *salt* e *pepper*, as quais servem para agregar outras informações aleatórias no intuito de transformar os dados em tamanhos maiores de informações, o que possibilita mitigar os riscos de ataques de força bruta (tentativa e erro). Também é indicado coletar os dados *off chain*, possibilidade em que se grava os dados em um banco de dados tradicional e na blockchain apenas o hash que possibilita a autenticação de tais informações.

Existem outras soluções sendo atualmente implementadas e pesquisadas, como a chamada “prova de conhecimento zero” (*zero knowledge proof*). Esse tipo de validação de informação consiste em uma técnica na qual é possível alguém produzir prova de um requisito (no caso, um dado pessoal) sem de fato revelar o conteúdo da informação sujeita a prova. Com a implementação da prova de conhecimento zero numa rede, alguém poderia fazer prova de que é maior de 18 anos sem a necessidade de revelar sua idade, por exemplo.

Essa, como outras técnicas que estão sendo estudadas atualmente, precisam cumprir uma extensa lista de requisitos das leis de proteção dados, como visto nas seções

⁸ European Parliament, “Blockchain and the General Data Protection Regulation”.

anteriores. Por isso, o consenso hoje é que os riscos inerentes induzem quem procura implementar soluções em blockchain a evitar ao máximo o uso de dados pessoais, também em cumprimento ao indispensável princípio da necessidade, previsto no artigo 6º, inciso III da LGPD⁹ (ou minimização de dados, conforme o GDPR). Se é preciso utilizar dados pessoais, é necessário antes se certificar da utilização de técnicas atuais e eficazes por meio de ofuscação, encriptação e agregação objetivando a anonimização para que se possa mitigar os riscos do uso de dados pessoais numa blockchain.

⁹ Artigo 6º, III da LGPD: *“III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados”.*

Referências

Article 29 Working Party (2014). *Opinion 05/2014 on Anonymisation Techniques*. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>

CNIL (2018). *Solutions for a responsible use of the blockchain in the context of personal data*. Disponível em: <<https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf>>

European Parliament (2019). *Blockchain and the General Data Protection Regulation*. Disponível em: <[https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf)>

European Union Blockchain Observatory and Forum (2018). *Blockchain and the GDPR*. Disponível em: <<https://www.eublockchainforum.eu/sites/default/files/reports/a.pdf>>