# O USO DA TECNOLOGIA *BLOCKCHAIN* PARA ARQUIVAMENTO DE DOCUMENTOS ELETRÔNICOS E NEGÓCIOS PROBATÓRIOS SEGUNDO A LEI DE LIBERDADE ECONÔMICA

*Fredie Souza Didier Júnior*
*Rafael Alexandria de Oliveira*
Autores Convidados

# O USO DA TECNOLOGIA *BLOCKCHAIN* PARA ARQUIVAMENTO DE DOCUMENTOS ELETRÔNICOS E NEGÓCIOS PROBATÓRIOS SEGUNDO A LEI DE LIBERDADE ECONÔMICA[1]

## *THE USE OF BLOCKCHAIN TCHNOLOGIE TO DOCUMENT FILING AND PROBATIVE AGREEMENTS ACCORDING TO BRAZILIAN 'ECONOMIC FREEDOM' LAW*

*Fredie Souza Didier Júnior*
*Rafael Alexandria de Oliveira*

## RESUMO

Este artigo pretende demonstrar que a Lei n. 13.874/2019 (Lei de Liberdade Econômica) ampliou a possibilidade do uso de documentos eletrônicos, além de discutir questões relativas à segurança e confiabilidade desses documentos e identificar na legislação hipótese típica de negócio jurídico sobre prova. Por fim, apresenta a possibilidade do uso da tecnologia *blockchain* como forma de garantir a autenticidade, integridade e confidencialidade de documentos eletrônicos, sejam eles públicos ou particulares.

**PALAVRAS-CHAVE:** *BLOCKCHAIN*. DOCUMENTOS ELETRÔNICOS. LEI DE LIBERDADE ECONÔMICA.

## *ABSTRACT*

*This article aims to demonstrate that Law n. 13.874/2019 (Economic Freedom Act) expanded the possibility of using electronic documents, and to discussing issues related to the security and reliability of these documents and identifying in the legislation typical hypothesis of agreement on evidence. Finally, it presents the possibility of*

*using blockchain technology as a way to guarantee the authenticity, integrity and confidentiality of electronic documents, whether public or private.*

***KEYWORDS:*** *BLOCKCHAIN. ELECTRONIC DOCUMENTS. ECONOMIC FREEDOM ACT.*

SUMÁRIO: 1. Introdução. 2. A Lei de Liberdade Econômica e a ampliação do uso do documento eletrônico: armazenamento em meio eletrônico de documentos públicos ou privados. 3. Documento eletrônico: a questão da segurança e da confiabilidade. 4. A presunção de autenticidade, integridade e confidencialidade do documento eletrônico certificado no padrão da ICP-Brasil. 5. A previsão de hipótese típica de negócio jurídico sobre prova. 6. *Blockchain* – 6.1. O que é *blockchain*; 6.2. Segurança e imutabilidade; 6.3. Transparência; 6.4. *Blockchain* como prova atípica; 6.5. *Blockchain* como forma de garantir a autoria, integridade e confidencialidade de documento eletrônico. 7. Conclusão. 8. Referências Bibliográficas.

## 1. INTRODUÇÃO

A Lei n. 13.874/2019 (Lei de Liberdade Econômica) ampliou a possibilidade de utilização do documento eletrônico de duas formas: *(i)* ao alterar a redação do art. 2º-A da Lei n. 12.682/2012, passou a autorizar o armazenamento, em meio eletrônico, óptico ou equivalente, de documentos privados e também de documentos públicos; *(ii)* equiparou a digitalização[2] ao próprio documento em suporte de papel, desde que atendidos a técnica e os requisitos estabelecidos em regulamento (art. 3º, X, Lei n. 13.874/2019[3]).

Essas alterações estão em conformidade com o movimento de desburocratização da Administração Pública que vem sendo implementado por sucessivos atos normativos – como, por exemplo, a Lei n. 13.460/2017, a Lei n. 13.726/2018 e a Lei 12.682/2012. Esse movimento abrange também os métodos de documentação, inclusive os métodos de documentação aplicáveis às relações entre particulares.

A consequência disso, no âmbito dos métodos de documentação, é uma crescente utilização dos documentos eletrônicos em substituição a outras formas de armazenamento de dados e de imagens, especialmente em substituição aos documentos em suporte de papel.

O propósito deste artigo é tratar da *blockchain* como meio atípico de comprovação da autoria, integridade e confidencialidade de documentos particulares ou públicos, a partir da hipótese típica de negócio jurídico sobre prova previsto no art. 18 da Lei n. 13.874/2019 c/c art. 10, §2º, da Medida Provisória n. 2.200-2/2001.

## 2. A LEI DE LIBERDADE ECONÔMICA E A AMPLIAÇÃO DO USO DO DOCUMENTO ELETRÔNICO: ARMAZENAMENTO EM MEIO ELETRÔNICO DE DOCUMENTOS PÚBLICOS OU PRIVADOS

A Medida Provisória n. 881, de 30 de abril de 2019, que instituiu a Declaração de Direitos de Liberdade Econômica (e foi a antecessora da Lei de Liberdade Econômica), já havia acrescentado o art. 2º-A à Lei n. 12.682/2012. No *caput* desse art. 2º-A, a MP 881 autorizava "o armazenamento, em meio eletrônico, óptico ou equivalente, *de documentos privados*, compostos por dados ou por imagens, observado o disposto nesta Lei, nas das demais legislações específicas e no regulamento" (acrescentamos o itálico).

O art. 10 da Lei de Liberdade Econômica alterou esse art. 2º-A acrescentado pela MP 881 à Lei n. 12.682/2012. Com a mudança, o *caput* passou a autorizar "o armazenamento, em meio eletrônico, óptico ou equivalente, *de documentos públicos ou privados*, compostos por dados ou por imagens, observado o disposto nesta Lei, nas legislações específicas e no regulamento" (acrescentamos o itálico).

A alteração é sensível: acrescentou-se a possibilidade de, para todos os fins, os documentos públicos serem, também eles, armazenados em meio eletrônico, óptico ou equivalente.

A distinção entre documento público e privado parte da análise de quem seja o autor do documento (DIDIER JR. et al, 2020): "será público quando o seu autor *imediato* for agente investido de função pública, e quando a formação do documento se der no exercício desta função […]. Será, ao contrário, particular o documento quando sua autoria *imediata* se dê por ação de um particular ou mesmo de um funcionário público (desde que este não se encontre no exercício de suas funções)" (MARINONI; ARENHART, 2005, p. 245-246).

A redação atual do *caput* do art. 2º-A da Lei n. 12.682/2012 harmoniza com o art. 3º, X, da Lei de Liberdade Econômica, que reconhece a toda pessoa, natural ou jurídica, o direito essencial de "arquivar *qualquer documento* por meio de microfilme ou por meio digital, conforme técnica e requisitos estabelecidos em regulamento, hipótese em que se equiparará a documento físico para todos os efeitos legais e para a comprovação de qualquer ato de direito público" (acrescentamos o itálico).

O armazenamento (ou arquivamento) em meio eletrônico de documento público ou privado é técnica que se aplica tanto aos documentos novos, criados já em formato de código digital, quanto aos documentos criados em suporte de papel cuja imagem venha a ser digitalizada e convertida para o formato de código digital (art. 1º, par. ún., Lei n. 12.682/2012).

A digitalização constitui, pois, uma forma de converter o documento em suporte de papel num documento eletrônico, a fim de que ele passe a ser armazenado (ou arquivado) em meio eletrônico.

Conforme visto, nos termos do art. 3º, X, da Lei de Liberdade Econômica, desde que atendidos técnica e requisitos estabelecidos em regulamento, o documento eletrônico produto da digitalização se equipara ao "documento físico para todos os efeitos legais e para a comprovação de qualquer ato de direito público"; isso vale "inclusive para atender ao poder fiscalizatório do Estado" (art. 2º-A, §2º, Lei n. 12.682/2012).

A eficácia desse art. 3º, X, está condicionada à regulamentação (art. 18, *caput*), mas alguns parâmetros já constam na Lei n. 12.682/2012, na Medida Provisória n. 2.200-2/2001 e também na própria Lei de Liberdade Econômica (art. 18, I e II).

O art. 18 da Lei de Liberdade Econômica prevê que: *(i)* se o documento digitalizado for particular, qualquer meio de comprovação da autoria, integridade e, se necessário, confidencialidade de documentos em forma eletrônica é válido, desde que escolhido de comum acordo pelas partes ou aceito pela pessoa a quem for oposto o documento; *(ii)* independentemente de aceitação, o processo de digitalização que empregar o uso da certificação no padrão da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) terá garantia de integralidade, autenticidade e confidencialidade para documentos públicos e privados.

Todos esses parâmetros precisam ser observados pelo regulamento.

Conforme o art. 2º-A, §1º, da Lei n. 12.682/2012, após a digitalização, constatada a integridade do documento digital nos termos estabelecidos no regulamento, o original poderá ser destruído, ressalvados os documentos de valor histórico, cuja preservação observará o disposto na legislação específica. Quanto aos documentos referentes a operações e transações realizadas no sistema financeiro nacional, a aferição de integridade do documento eletrônico e as hipóteses em que o documento original pode ser destruído devem ser regulamentadas em ato do Conselho Monetário Nacional (art. 2º-A, §6º, Lei n. 12.682/2012).

O dever de guarda dos documentos armazenados em meio eletrônico, tenham sido eles criados já como código digital ou sejam fruto de digitalização de documento em suporte de papel, termina com o exaurimento dos respectivos prazos de decadência ou de prescrição das situações jurídicas que deles emanam[4], momento em que se faculta sejam eles eliminados (art. 2º-A, §3º, Lei n. 12.682/2012).

## 3. DOCUMENTO ELETRÔNICO: A QUESTÃO DA SEGURANÇA E DA CONFIABILIDADE

A valorização do meio eletrônico para fins de documentação de fatos e declarações de vontade está em conformidade com o avanço tecnológico e com a forma pela qual as relações jurídicas vêm sendo constituídas atualmente. É crescente, por exemplo, o uso de aplicativos em dispositivos móveis para o registro de ideias e de manifestações de vontade (como os aplicativos de mensagem)[5], para a realização de transações financeiras (como os aplicativos de instituições financeiras) – em alguns casos, a senha pessoal é até substituída por recursos de biometria, como o reconhecimento facial – e para a celebração de *smart contracts* (como nos aplicativos de transporte, de aluguel de bicicletas ou patinetes, ou de *delivery* de comidas ou de compras feitas em ambiente *online* etc.).

Há, por isso mesmo, uma preocupação constante quanto ao grau de segurança e de certeza que se pode ter em relação à *autenticidade* dos documentos eletrônicos, que permite identificar a sua autoria, e à sua *integridade*, que permite garantir a inalterabilidade do seu conteúdo. Somente a certeza quanto a esses dados é que pode garantir a eficácia probatória desses documentos[6].

O problema é que, pelo seu próprio conceito (sequência de *bits* representativa de um fato), já se vê que a maior e melhor característica do documento eletrônico – que é a sua versatilidade, ou flexibilidade, na medida em que, em segundos, ele pode ser formado e utilizado, mediante envio pela Internet, em qualquer lugar do mundo – é também a porta para possíveis adulterações, o que infirma a sua integridade e, pois, a sua eficácia probatória.

Têm sido desenvolvidas técnicas que buscam dar maior segurança e confiabilidade aos documentos eletrônicos. Normalmente essas técnicas vinculam a garantia da autenticidade à integridade do conteúdo do documento, de modo que, alterado o seu conteúdo, desfaz-se a vinculação entre este novo conteúdo (alterado) e o autor do documento originário.

São várias as técnicas, que podem conferir maior ou menor segurança, a depender do tipo.

Tem-se, por exemplo (MARQUES, 2005): *(i)* a assinatura digitalizada (que não se confunde com a assinatura digital), que nada mais é que uma imagem da assinatura autógrafa, a qual pode ser lançada no documento para identificar a sua autoria; *(ii)* as firmas biométricas, que permitem reconhecer a autoria de uma declaração a partir das características físicas do seu emitente (o formato do rosto, a íris dos olhos, a impressão digital, o timbre de voz etc.), muito utilizadas por aplicativos instalados em *smartphones* com ferramentas de detecção de impressão digital ou de reconhecimento facial; *(iii)* as senhas pessoais, como o PIN (*Personal Identification Number* ou Número de Identificação Pessoal), a *Password* (palavra de aprovação) e a *Passphrase* (frase de passagem ou aprovação), comuns nos terminais bancários, nas transações eletrônicas etc.; *(iv)* a esteganografia, que transforma o documento em um código (espécie de criptografia) e lhe agrega um elemento marcante, semelhante a uma marca d'água; dentre outras.

A técnica mais segura de que hoje se tem conhecimento é a *criptografia*. Por essa técnica, a declaração (mensagem) é cifrada e transformada num código ininteligível àquele que não conhece o padrão para a decifração. O padrão utilizado para cifrar ou decifrar as mensagens é denominado de *chave*. Somente quem a conhece é que pode ter acesso ao conteúdo da mensagem[7].

Atualmente, a criptografia usa conceitos matemáticos extremamente complexos (os *algoritmos*) como chave para cifrar as mensagens. Essas chaves, no entanto, não codificam letras ou números, mas os próprios *bits* que compõem a sequência do documento eletrônico (MARQUES, 2005; LAGO JR., 2001).

Há duas formas de criptografia: a criptografia *simétrica* e a *assimétrica*.

Como ensina Antônio Lago Jr., "o uso da *criptografia simétrica*, também chamada de criptografia de chave privada, requer que o destinatário da mensagem conheça o algoritmo usado para cifrar o seu conteúdo, caso contrário, ficará impossibilitado de decifrar a mensagem, ou seja, o destinatário da mensagem deve ter acesso à chave utilizada pelo remetente" (LAGO JR., 2001, p. 35-36). Esse método é frágil em termos de segurança, na medida em que a chave utilizada para decifrar a mensagem é a mesma utilizada para cifrá-la. Assim, sendo ela conhecida pelo receptor, não se pode garantir que ele não venha utilizá-la para cifrar novas mensagens, fazendo-se passar pelo autor da mensagem originária. Isso infirmaria, como se pode ver, talvez não a autenticidade da mensagem recebida, mas de tantas outras que, a partir da chave conhecida, pudessem vir a ser formadas.

Já a *criptografia assimétrica* é uma das técnicas capazes de conferir maior segurança quanto à autenticidade e integridade do conteúdo do documento eletrônico. Como explica Augusto Marcacini:

> A criptografia assimétrica, ao contrário da convencional (que pede a mesma chave tanto para cifrar como para decifrar a mensagem), utiliza *duas* chaves, geradas pelo computador. Uma das chaves dizemos ser a *chave privada*, a ser mantida em sigilo pelo usuário, em seu exclusivo poder, e a outra, a *chave pública*, que, como sugere o nome, pode e deve ser livremente distribuída. Estas duas chaves são dois números que se relacionam de tal modo que uma desfaz o que a outra faz. Encriptando a mensagem com a chave pública, geramos uma mensagem cifrada *que não pode ser decifrada com a própria chave pública que a gerou*. Só com o uso da chave privada poderemos decifrar a mensagem que foi codificada com a chave

> pública. E o contrário também é verdadeiro: o que for encriptado com o uso da chave privada, só poderá ser decriptado com a chave pública. (MARCACINI, 1999)

A chave privada, utilizada por aquele que formou o documento eletrônico, gera uma assinatura digital, que permite a identificação do seu autor. Essa assinatura digital pode ser conferida a partir do uso da chave pública. Não se trata, contudo, de um sinal visível, como o é a assinatura manuscrita, mas de uma sequência numérica a que o programa de computador chega a partir de fórmulas matemáticas. A assinatura digital será diferente para cada documento gerado por uma determinada chave privada, mas sempre estará vinculado a ela, o que garante a prova da autenticidade do documento.

Além de essa chave privada poder atestar a autenticidade do documento, ela ficará vinculada ao seu conteúdo, de modo que qualquer alteração superveniente tornará, automaticamente, ineficaz a assinatura digital outrora lançada. Com isso, embora seja possível a alteração do conteúdo do documento guardado pela criptografia assimétrica, essa alteração não mais vinculará o seu autor originário (MARCACINI, 1999)[8]. Em outras palavras: a integridade do documento é garantida em relação ao seu autor; não sendo possível identificá-lo, tem-se aí um indício de que o documento foi alterado.

Como se viu, somente a chave pública distribuída por uma determinada pessoa pode ser utilizada para decifrar a mensagem codificada pelo titular da respectiva chave privada. Mas aí surge um novo problema: "qualquer um poderia gerar um par de chaves e atribuir-lhe o nome de qualquer pessoa, existente ou imaginária. A autenticidade do documento eletrônico é conferida sem dificuldade por qualquer usuário de computador, com o uso do programa de criptografia e de posse da chave pública do seu subscritor. Mas, e se a própria chave pública não for autêntica? Esta conferência o programa não tem como realizar. O que fazer, então, para contornar o problema?" (MARCACINI, 1999). Nesse caso, a assinatura digital apontaria, como autor do documento, uma determinada pessoa, distinta da que efetivamente formara o documento.

"Para evitar, então, essa fraude, instituiu-se a *certificação digital*, onde a identidade do proprietário das chaves é previamente verificada

por uma terceira entidade de confiança dos interlocutores, que terá a incumbência de certificar a ligação entre a chave pública e a pessoa que a emitiu, como também a sua validade" (MARQUES, 2005). Essa terceira entidade a que alude Antônio Terêncio Marques, responsável pela certificação digital da identidade do proprietário das chaves e pela divulgação ao público das chaves públicas válidas, é a chamada *autoridade certificadora*[9].

## 4. A PRESUNÇÃO DE AUTENTICIDADE, INTEGRIDADE E CONFIDENCIALIDADE DO DOCUMENTO ELETRÔNICO CERTIFICADO NO PADRÃO DA ICP-BRASIL

No intuito, dentre outras coisas, de garantir a autenticidade, a integridade e a validade jurídica dos documentos eletrônicos, a Medida Provisória n. 2.200-2/2001 instituiu a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil (art. 1º), composta por uma autoridade vinculada ao Comitê Gestor por ela criado e pela cadeia de autoridades certificadoras (art. 2º).

A regulamentação legal veio para viabilizar meios de tornar ainda mais segura a utilização dos documentos eletrônicos protegidos por criptografia assimétrica. A sua eficácia probatória, quando produzido com a utilização de processo de certificação disponibilizado pela ICP-Brasil, é a mesma dos documentos públicos e particulares, presumindo-se verdadeiros em relação aos signatários (art. 10, *caput* e § 1º, MP n. 2.200-2/2001).

Quando se trata de digitalização de documentos em papel, o art. 3º da Lei n. 12.682/2012 prescreve que o processo de digitalização deve ser realizado de forma a manter a integridade, a autenticidade e, se necessário, a confidencialidade do documento digital, com o emprego de certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Nesses mesmos termos, a Lei de Liberdade Econômica (Lei n. 13.874/2019) estabelece a presunção de que o processo de digitalização do documento de papel, público ou particular, que empregar o uso da certificação no padrão da ICP-Brasil terá garantia de integralidade, autenticidade e confidencialidade (art. 18, II).

## 5. A PREVISÃO DE HIPÓTESE TÍPICA DE NEGÓCIO JURÍDICO SOBRE PROVA

A certificação no padrão da ICP-Brasil pode ser substituída por outro método de certificação escolhido em comum acordo pelas partes ou aceito pela pessoa a quem for oposto o documento. Em linha de princípio, isso é expresso apenas em relação aos documentos particulares, conforme se vê no art. 18, I, da Lei de Liberdade Econômica: "*para documentos particulares*, qualquer meio de comprovação da autoria, integridade e, se necessário, confidencialidade de documentos em forma eletrônica é válido, desde que escolhido de comum acordo pelas partes ou aceito pela pessoa a quem for oposto o documento" (acrescentamos o itálico).

O art. 2º-A, §8º, da Lei n. 12.682/2012, acrescentado pela Lei n. 13.874/2019, prescreve que "para a garantia de preservação da integridade, da autenticidade e da confidencialidade de *documentos públicos* será usada certificação digital no padrão da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)".

Uma leitura apressada desse art. 2º-A, §8º, da Lei n. 12.682/2012 e do art. 18, I, da Lei n. 13.874/2019 poderia dar a entender que a certificação dos documentos públicos somente é possível se utilizado o padrão da ICP-Brasil.

Sucede que o art. 10, §2º, da MP n. 2.200-2/2001, responsável por instituir a ICP-Brasil, prescreve que, para todos os fins legais, os documentos eletrônicos tratados na Medida Provisória se consideram públicos ou particulares (art. 10, *caput*), a depender da sua autoria. Já o §2º estabelece que "o disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento".

Fica muito claro, portanto, que o sistema normativo não estabelece a certificação digital no padrão da ICP-Brasil como *método exclusivo* para garantir a preservação da integridade, da autenticidade e da confidencialidade dos documentos eletrônicos. Apenas há, como já visto no item anterior, uma *presunção* de que o uso da certificação no padrão

da ICP-Brasil implica esse tipo de garantia para documentos públicos e privados (art. 18, II, Lei n. 13.874/2019), bem como que, *a princípio*, quanto aos documentos públicos, essa garantia decorre da certificação digital no padrão da ICP-Brasil (art. 2º-A, §8º, da Lei n. 12.682/2012).

É possível, porém, que outros meios de comprovação de autoria, de integridade e de confidencialidade de documentos eletrônicos sejam utilizados para essa finalidade, desde que isso seja "admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento". O §2º do art. 10 da MP n. 2.200-2/2001 não diferencia entre documentos públicos e particulares; o *caput* do art. 10 prescreve, inclusive, e como visto, que os documentos eletrônicos tanto podem ser públicos como particulares.

Conjugando-se, pois, o art. 18, I, da Lei n. 13.874/2019 com o art. 10, §2º, da MP n. 2.200-2/2001, temos que o sistema normativo contém hipótese típica de negócio jurídico sobre prova, consistente no acordo quanto ao método de certificação da autoria, integridade e confidencialidade do documento eletrônico, seja ele público ou particular.

Nesse cenário, nada impede que se convencione, por exemplo, o uso da *blockchain* como método de certificação da autoria, integridade e confidencialidade do documento eletrônico.

## 6. *BLOCKCHAIN*

### 6.1. O que é *blockchain*

*Blockchain* é palavra em língua inglesa que significa *cadeia de blocos*.

Esse é o nome usado, ao mesmo tempo, para *(i)* designar uma *base de dados distribuída* e também para *(ii)* designar a *tecnologia que mantém as múltiplas cópias dessa base de dados operando em sincronia umas com as outras*, de modo que estejam sempre atualizadas (informação verbal)[10]. Vejamos.

*Blockchain* é uma base de dados distribuída.

Quando pretendemos obter informação sobre determinado imóvel, nós buscamos essa informação no Registro de Imóveis da cidade – o Registro de Imóveis centraliza as informações sobre imóveis existentes em determinada região. Quando pretendemos obter informação sobre antecedentes criminais de determinado sujeito, nós buscamos essa informação no Setor de Distribuição das Justiças Estadual e Federal – o Setor de Distribuição centraliza as informações sobre processos pendentes. Quando pretendemos obter informação sobre o nosso saldo na conta bancária, nós acessamos o sistema eletrônico do banco – o nosso banco centraliza as informações sobre a nossa conta bancária. Por fim, quando pretendemos obter informação sobre um determinado assunto que seja do nosso interesse, é comum procurarmos essa informação no *site* do *Google* – o *Google* é uma ferramenta que centraliza muitas informações sobre assuntos variados cujo acesso está disponível na *internet*.

Todos esses são exemplos de bases de dados concentradas, não distribuídas, que dependem sempre de um servidor ou de um intermediário para que possam ser acessadas. Se houver um incêndio na sede do Registro de Imóveis, perdem-se os registros ali arquivados; se for feriado, provavelmente não será possível obter a certidão de antecedentes criminais no Setor de Distribuição das Justiças Estadual e Federal; se houver um ataque de *hackers*, podemos ter problemas com as informações contidas no sistema bancário; se o grupo de pessoas que comanda o *Google* resolvesse desligar seus servidores, perderíamos o acesso a essa importante ferramenta de consulta à base de dados da *internet*.

A ideia subjacente à *blockchain* é a de que a informação deve ser registrada em *múltiplos servidores*, de modo que é desnecessário existir um intermediário – o Registro de Imóveis, o Setor de Distribuição, o banco, o *Google* – para que possamos acessar essa informação. Essa ideia se concretiza por meio do *compartilhamento* (distribuição) da informação – também chamada de *consenso distribuído*.

Uma informação registrada na *blockchain* não fica em apenas um lugar, nem depende de um intermediário para ser acessada. Ela é distribuída entre os inúmeros computadores que compõem a rede (denominados "nós"), de modo que fica registrada em todos eles.

Isso assegura a plena acessibilidade das informações registradas na *blockchain*, que podem ser consultadas 24 horas por dia, 365 dias por ano. Se um "nó" (computador da rede) estiver desligado ou tiver problemas porque sofreu um ataque *hacker*, haverá outro funcionando e a informação estará lá.

A ideia por trás da *blockchain* é a descentralização do controle, registro e gestão. No sistema tradicional, isso fica na mão de um intermediário (o banco, por exemplo); no sistema *blockchain*, fica na mão de todos.

Mas não basta distribuir a informação como forma de mantê-la acessível; é preciso mantê-la acessível e *atualizada*.

A *blockchain* é, como dito, não apenas uma base de dados distribuída como também uma tecnologia que permite que toda a informação distribuída se mantenha atualizada e em sincronia.

A *blockchain* é uma espécie de Diário[11], onde as informações são lançadas e vão sendo atualizadas a cada período de tempo. A cada momento – em média, a cada dez minutos –, uma nova página é acrescentada a esse Diário, contendo novas e atualizadas informações; a essa nova página se dá o nome de "bloco" (*block*). A rede vai sendo periodicamente atualizada e cada nova página (*block*) deve ser reconhecida como verdadeira pela base de usuários (chamados "nós"), que vai guardando registro dessa nova realidade.

Para que a informação seja registrada na rede, a *blockchain* exige que um determinado desafio matemático seja resolvido pelo usuário. Ou seja, o usuário só consegue registrar essa nova página do Diário (*block*) se resolver um problema matemático. A solução desse desafio requer muito esforço computacional, de modo que o caminho mais fácil é o computador ficar arriscando números aleatórios como resposta. A partir do momento em que acerta a resposta, ele adquire o direito de propagar para toda a rede uma base de informações.

Esse esforço computacional para vencer o desafio matemático e registrar um novo bloco de informações na rede é considerado um *serviço* e é recompensado com pagamento em *Bitcoin* – a essa atividade se deu

o nome de *mineração*[12]. Minerador é, pois, o usuário da *blockchain* que põe a sua capacidade de processamento (seus computadores, ou "nós") a serviço da rede, registrando novos blocos de informações. Se você não tem capacidade de processamento para lançar tais registros, pode contratar quem o tenha e suas informações serão registradas na *blockchain*.

A partir do momento em que uma nova página é adicionada ao "Diário" – continuemos com a nossa metáfora –, há uma sincronização de dados e validação de conteúdo, de forma que toda a base de dados distribuída passa a exibir os mesmos registros – é como se todos pudessem ter a chance de ser oficial do Registro de Imóveis e pudessem, vencendo o desafio matemático, registrar a venda de um determinado imóvel, lançando-a no "Diário" que é a *blockchain* e que está distribuído entre os inúmeros "nós" que compõem a rede.

A *blockchain* não é uma rede única.

É possível que haja várias redes baseadas na tecnologia *blockchain* – a rede usada para o registro de transações em *Bitcoins* é um exemplo de rede baseada em tecnologia *blockchain*. Nada impede que se construa uma rede *blockchain* para que os funcionários de uma determinada empresa multinacional compartilhem documentos de trabalho. Também é possível a construção de uma rede *blockchain* para que membros de determinado partido ou associação votem em candidatos a determinados cargos.

A plataforma *Ethereum*[13], por exemplo, permite que várias aplicações sejam construídas com base na tecnologia *blockchain*. Trata-se de grande aliado do uso da *blockchain* para o registro de informações que vão além de transações com *Bitcoins*. Essa rede se atualiza de modo ainda mais rápido que a *blockchain* do *Bitcoin* – a cada 12 segundos (MELO, 2018), e não a cada 10 minutos – e assegura o mesmo grau de confiabilidade.

### 6.2. Segurança e imutabilidade

A informação registrada na *blockchain* é considerada imutável e segura, porque, embora não seja imune à fraude, é muito custoso adulterá-la e, em certo ponto, a fraude passa a ser tecnicamente impossível para

os padrões computacionais de hoje. Isso se dá porque cada nova página (*block*) que se acrescenta ao Diário contém informações sobre as páginas anteriores, às quais se liga de forma encadeada. Assim, sempre que um novo bloco é validado consensualmente na rede, é como se todos os blocos que o antecedem fossem novamente validados.

É exatamente daí que vem o nome *blockchain*: cadeia de blocos.

Para que alguém consiga inserir uma informação falsa na rede *blockchain* é preciso que esse alguém detenha um poder de processamento computacional maior que 50% dos computadores ligados à rede. A questão aí é de probabilidade matemática: quanto menor o poder de processamento de dados, menor a chance de vencer o desafio matemático proposto e, portanto, menor a chance de ser o registrador da vez. O problema é que, segundo estimativa, para alcançar esse poder de processamento computacional maior que 50% dos computadores ligados à rede, seria necessário que o sujeito fraudador tivesse uma capacidade de processamento igual a cerca de 50 vezes a capacidade de processamento do *Google* (informação verbal)[14]. Ainda que existisse um servidor, ou conjunto de servidores, com uma capacidade de processamento tão expressiva, é difícil acreditar que ele seria colocado a serviço desse tipo de fraude.

Por outro lado, é também improvável que alguém consiga alterar informações já inseridas na *blockchain*. Para fazer isso, precisaria não apenas alterar o registro do bloco (página) em que a informação estivesse inserida, como também alterar o registro de todos os blocos subsequentes a ela, já que eles guardam e validam a informação dos blocos precedentes.

Se o bloco atual é, por exemplo, o 243 (p. ex., a página 243 do "Diário") e o sujeito quer alterar uma informação contida no bloco 157 (p. ex., na página 157 do "Diário"), ele vai precisar resolver o desafio matemático para alterar o bloco 157, o bloco 158, o bloco 159... e assim sucessivamente, até o bloco atual (informação verbal)[15]. É como alguém que pretende inserir um documento num processo em autos físicos e precisa renumerar todas as folhas subsequentes sem deixar rastros.

Sucede que, se já é difícil vencer o desafio matemático para registrar *um bloco*, ainda mais difícil é vencer sucessivos desafios

matemáticos, um na sequência do outro, a ponto de conseguir registrar todos os blocos fraudados.

Segundo análise de segurança feita por Satoshi Nakamoto, aquele que é considerado o inventor do *bitcoin*, é tecnicamente inviável, segundo os padrões tecnológicos atuais, que alguém consiga alterar *seis blocos* em sequência (informação verbal)[16] – o que significa que as informações registradas há mais de seis blocos (ou páginas) se tornam tecnicamente imutáveis; ou, sob a perspectiva de tempo, considerando que a cada dez minutos um novo bloco é registrado na rede, a informação registrada na rede há mais de uma hora já se torna tecnicamente imutável.

Um dos motivos invocados pelo Tribunal de Justiça de São Paulo (TJSP) no Agravo de Instrumento n. 2222371-76.2019.8.26.0000 para negar pedido de urgência para resgate imediato de *bitcoin* foi justamente a imutabilidade dos dados registrados na *blockchain*. Segundo se decidiu, "a moeda em questão é baseada na tecnologia de registro denominada 'blockchain' o que significa que, caso haja a inserção de algum dado em algum ponto de tal rede de registro, esta informação será replicada por todos os dispositivos dela integrantes - essa é a forma pela qual se atribui segurança e confiabilidade às operações. E, por esta razão, o eventual deferimento de uma medida que autorize o saque da moeda virtual tem natureza irreversível já que, realizada a transferência dos ativos almejados e confirmada a transação na rede correspondente, seria inviável a de devolução dos valores que somente poderá ser efetuada com a colaboração do autor e, quiçá, de terceiros que sejam os destinatários de tais valores" (BRASIL, 2019, p.4).

### 6.3. Transparência

Além da acessibilidade, da segurança e da imutabilidade, a transparência é outra marca da *blockchain*.

As informações são registradas publicamente, como parte da própria essência dessa tecnologia, que se utiliza do consenso distribuído como mecanismo de registro e de validação de informações. Isso, contudo, não significa que haja perda de privacidade. As pessoas que se vinculam à

rede são ali representadas por números (endereços). É possível saber, por exemplo, que o usuário 23xy4ab transferiu uma soma X de moeda para o usuário 45td94zk, mas não é possível, a princípio, saber *quem são* essas pessoas.

Há diversas formas de configuração dessa transparência. Por padrão, as informações são públicas e as identidades, privadas. Mas é possível que as informações sejam privadas e as identidades, públicas; ou que sejam ambas privadas, ou ambas públicas.

A transparência como são tratados os dados registrados na rede *blockchain* – sem que haja, necessariamente, perda de privacidade – reforça a possibilidade de uso dessa tecnologia como meio de prova no processo jurisdicional.

### 6.4. *Blockchain* como prova atípica

A tecnologia *blockchain* está umbilicalmente atrelada ao *bitcoin*, uma vez que as transações com essa moeda são realizadas e registradas numa rede *blockchain*.

Aliás, a *blockchain* é justamente um dos motivos pelos quais o *bitcoin* se revela como algo tão inovador. Isso se dá em razão de as transações com essa moeda prescindirem completamente de um intermediário – como o Governo de um país ou um banco – e poderem ser realizadas diretamente entre pessoas (*peer-to-peer*). As operações de crédito e débito feitas com *bitcoin* são registradas nesse Livro-Razão (*ledger*) distribuído que é a *blockchain* e vão sendo atualizadas a cada período de tempo.

Mas a *blockchain* pode ser mais que uma base de dados para registro de transações com *bitcoins*. Embora esses termos estejam vinculados em sua gênese, isso não significa que a tecnologia *blockchain* só possa ser aplicada para as transações com *bitcoins* (ALEIXO, 2018)[17]. Já se vem falando na tecnologia *blockchain* como algo que pode ser de grande utilidade, por sua confiabilidade e segurança, como método de documentação de informações veiculadas na internet (ROQUE, 2018)[18] e como prova atípica de maneira geral – art. 369, CPC (MELO, 2018).

De fato, em razão da confiabilidade e da segurança desse tipo de tecnologia, a *blockchain* pode ser utilizada em substituição a métodos tradicionais de atestação de existência e conteúdo de certos dados, como *(i)* o reconhecimento de assinatura num determinado documento; *(ii)* a confecção de diploma eletrônico que confirma a graduação num certo curso; *(iii)* a receita médica prescrevendo determinado medicamento de uso controlado, que tem validade definida e só pode ser usada uma vez pelo paciente; *(iv)* a constatação de que determinada fotografia ou notícia jornalística foi veiculada, em certo momento, numa dada rede social; *(v)* o registro de determinada criação intelectual, com identificação de autoria, gerando prova de existência e precedência dessa criação (MELO, 2018); *(vi)* a utilização da rede para registro de manifestação de vontade, dispensando a assinatura de próprio punho num instrumento contratual (MELO, 2018); *(vii)* a divulgação de dados obtidos a partir de auditoria em órgãos públicos, como forma de garantir transparência na gestão pública; (*viii*) cadeia logística, como datas de envio e entrega de produtos, para fins de vigilância sanitária; *(ix)*

Outra aplicação possível da *blockchain* como forma de documentação de fatos e manifestações de vontade está ligada à ideia dos *smart contracts*, ou contratos inteligentes[19]. Nesse tipo de contrato, os termos do acordo são convertidos em código por meio de linguagem de programação de computador; uma vez em movimento, seus termos são executados tal como foram programados (DE FILIPPI; WRIGHT, 2018)[20]. Os *smart contracts* já são uma realidade atualmente; eles estão nas compras *online* e nos aplicativos de *streaming*, como Spotify e Netflix, com que lidamos diariamente; estão também nas licenças de uso de *softwares*, como o Microsoft 365 e os produtos da Adobe, em aplicativos de leitura, como o Kindle Unlimited, e nos aplicativos de transporte, como o Uber, o Cabify e o 99[21].

Além disso, a tecnologia *blockchain* pode ser usada para a documentação da cadeia de custódia referida na Lei n. 13.964/2019 (denominada de Pacote Anticrime), que acrescentou ao Código de Processo Penal os arts. 158-A a 158-F[22-23]. Esses dispositivos regulam

detalhadamente todo o fluxo do tratamento a ser dado aos vestígios de determinado fato[24]. Trata-se de meio de preservação e garantia da integridade de determinada fonte de prova, algo que se relaciona com o direito a um processo devido e com a garantia constitucional que proíbe o uso da prova ilícita, uma vez que visa a "assegurar a fiabilidade do elemento probatório, ao colocá-lo sob proteção de interferências capazes de falsificar o resultado da atividade probatória" (PRADO, 2014, p. 82-86).

Embora regulamentada no Código de Processo Penal, nada impede que a cadeia de custódia seja ela utilizada como método de coleta, manutenção e documentação da história cronológica dos vestígios também no processo civil (DIDIER JR.; BRAGA et al., 2020). E nada impede seja ela documentada por meio da tecnologia *blockchain*.

### 6.5. *Blockchain* como forma de garantir a autoria, integridade e confidencialidade de documento eletrônico

Por fim, as partes podem convencionar que a comprovação da autoria, integridade ou confidencialidade de determinado documento eletrônico seja feita por meio da tecnologia *blockchain*. Os termos de uso de determinado *site* ou aplicativo podem estabelecer, por exemplo, que o usuário consente que toda informação trocada eletronicamente seja documentada numa plataforma *blockchain*, e consente que essa forma de documentação impede, numa futura disputa, qualquer discussão acerca da autoria, integridade ou confidencialidade do documento – uma presunção semelhante àquela erigida pelo legislador quanto à certificação no padrão da ICP-Brasil, só que baseada numa norma convencional.

Conhecer e considerar essa possibilidade é algo importante porque, além de ela consistir numa alternativa à certificação pelo padrão da ICP-Brasil, a revolução propiciada pela tecnologia *blockchain* vem sendo comparada àquela proporcionada pela introdução do *software* de código aberto no âmbito de tecnologia da informação (MAGNUS, 2017), a ponto de muitas pessoas e organizações estarem dedicadas ao estudo e experimentação de novas formas de aplicação dessa tecnologia, que se reputa capaz de gerar redução de custos operacionais e aperfeiçoamento dos mecanismos de controle interno (DE FILIPPI; WRIGHT, 2018).

Diversas atividades típicas da vida corporativa podem ser facilitadas pelo uso da tecnologia *blockchain* como método de documentação – desde, por exemplo, a utilização de livros contábeis eletrônicos em lugar da escrituração contábil tradicional (MAGNUS, 2017) até a realização de votações para eleição de comitês executivos, com resultados mais confiáveis e transparentes (DE FILIPPI; WRIGHT, 2018).

Imagine, então, que os atos constitutivos de determinada sociedade contemplem negócio jurídico no qual os cotistas ou acionistas tenham convencionado a presunção de autoria e integridade dos livros contábeis documentados em plataforma com tecnologia *blockchain* ou ainda do processo eletivo realizado com o uso dessa tecnologia (art. 18, I, Lei n. 13.874/2019) – essa presunção convencional afastaria a chance de discussão da autenticidade e da integridade dos documentos eletrônicos numa eventual disputa, em benefício do tempo e do custo de tramitação do processo.

## 7. CONCLUSÃO

O ensaio não tem intenção de exaurir o tema, que é complexo e abrange diversas áreas do conhecimento. A ideia é realmente a de provocar a reflexão sobre as questões aqui propostas.

Como conclusão, entendemos que a Lei de Liberdade Econômica veio para incentivar ainda mais o uso dos documentos eletrônicos, na medida em que autoriza o armazenamento (ou arquivamento) de documentos públicos e privados em meio eletrônico, bem como equipara a digitalização dos documentos em suporte de papel aos documentos originais, uma vez atendidos certos requisitos estabelecidos em regulamento.

A Lei de Liberdade Econômica estabelece, ainda, a presunção de que o processo de digitalização do documento de papel, público ou particular, que empregar o uso da certificação no padrão da ICP-Brasil tem garantia de integralidade, autenticidade e confidencialidade (art. 18, II). De resto, isso se aplica não apenas ao processo de digitalização como também ao armazenamento (ou arquivamento) de documentos em meio eletrônico com uso do padrão da ICP-Brasil.

Por outro lado, o art. 18, I, da mesma Lei n. 13.874/2019 e o art. 10, §2º, da MP n. 2.200-2/2001 inseriram no sistema normativo

uma hipótese típica de negócio jurídico processual sobre prova, consistente no acordo quanto ao método de certificação da autoria, integridade e confidencialidade do documento eletrônico, seja ele público ou particular.

Nesse cenário, nada impede que se convencione, por exemplo, o uso da *blockchain* como método de certificação da autoria, integridade e confidencialidade do documento eletrônico, criando-se, convencionalmente, a presunção de que os documentos eletrônicos armazenados em plataforma que opera com tecnologia *blockchain* têm sua autoria, integridade e confidencialidade asseguradas.

## NOTAS

1 Este artigo é também resultado do grupo de pesquisa "Transformações nas teorias sobre o processo e o Direito processual", vinculado à Universidade Federal da Bahia, cadastrado no Diretório Nacional de Grupos de Pesquisa do CNPq respectivamente nos endereços dgp.cnpq.br/dgp/espelhogrupo/7958378616800053. O grupo é membro fundador da "ProcNet – Rede Internacional de Pesquisa sobre Justiça Civil e Processo contemporâneo" (http://laprocon.ufes.br/rede-de-pesquisa).

2 Conforme art. 1º, par. ún., da Lei n. 12.682/2012, "entende-se por digitalização a conversão da fiel imagem de um documento para código digital".

3 Art. 3º São direitos de toda pessoa, natural ou jurídica, essenciais para o desenvolvimento e o crescimento econômicos do País, observado o disposto no parágrafo único do art. 170 da Constituição Federal: [...] X - arquivar qualquer documento por meio de microfilme ou por meio digital, conforme técnica e requisitos estabelecidos em regulamento, hipótese em que se equiparará a documento físico para todos os efeitos legais e para a comprovação de qualquer ato de direito público.

4 Sobre o tema, o STJ já decidiu que "ocorrida a prescrição, não mais sobrevive o dever de guarda de documentos, sendo legítima a recusa fundada no transcurso do prazo prescricional. Pensar diferente seria impor à parte obrigação juridicamente impossível" (BRASIL, 2010).

5 Foi amplamente divulgada, em 2015, a notícia do primeiro acordo viabilizado por meio do aplicativo WhatsApp. O fato ocorreu num processo que tramitava perante a Justiça do Trabalho da 15ª Região, em Campinas/SP. A juíza e os advogados das partes iniciaram as tratativas por meio do aplicativo de mensagens e compareceram à audiência apenas para reduzi-lo a termo e assinar o documento físico. A despeito da preferência que se tenha dado ao documento de papel, é preciso ver que o diálogo entabulado por meio do WhatsApp, eletronicamente documentado, já consistia, por si só, numa exteriorização da vontade dos transatores; a juíza, no caso, optou por homologá-lo em audiência, mas poderia, sem qualquer prejuízo, tê-lo feito ali, no próprio grupo de WhatsApp, do qual também ela, juíza, participava, anexando posteriormente o documento eletrônico comprobatório da avença (e da sua homologação) aos autos do processo. A rigor, o documento

(eletrônico) surtiria o mesmo efeito que o documento de papel. A notícia reforça a ideia de que essas novas tecnologias estão e estarão cada vez mais acessíveis e a serviço do processo (processo n. 0010025-20.2015.5.15.0094; notícia disponível em < http://www.conjur.com.br/2015-jun-08/justica-trabalho-promove-acordo-entre-partes-via-whatsapp> Acesso em 27 dez. 2015).

[6] A propósito, o enunciado n. 297 das Jornadas de Direito Civil do Conselho da Justiça Federal: "O documento eletrônico tem valor probante, desde que seja apto a conservar a integridade de seu conteúdo e idôneo a apontar sua autoria, independentemente da tecnologia empregada".

[7] Júlio César, imperador romano, criou um eficiente sistema de envio de mensagens criptografadas para os seus centuriões no campo de batalha. Por meio dela, mandava substituir as letras do texto original sempre pela terceira letra que lhe sucedesse no alfabeto. Essa era, portanto, a chave para cifrar a mensagem. Quem a recebesse, precisaria valer-se desta mesma chave para decifrá-la, aplicando-a inversamente: as letras da mensagem recebida deveriam ser substituídas pela terceira letra que lhe antecedesse no alfabeto.

[8] O autor explica: "Se uma mínima modificação for feita ao abrir-se o arquivo, e for ele gravado em disco, o documento eletrônico ficará inutilizado, pois perderá o vínculo com a assinatura" (MARCACINI, 1999, p. 15).

[9] É uma espécie de "cibernotário", como sugere Augusto Tavares Rosa Marcacini (MARCACINI, 1999).

[10] Informação obtida em: ALEIXO, Gabriel. Aula 1: Blockchain e Direito. *Blockchain e seus aspectos jurídicos*. Curso online do ITS Rio, 1h06m35s, acesso em 23 de dezembro de 2018.

[11] A Blockchain compõe um sistema mais amplo, denominado Distributed Ledger Technology (DLT), ou Tecnologia do Livro-Razão Distribuído. Tecnicamente, a Blockchain é uma espécie de Livro-Razão, que é como um "Diário contábil", onde são lançados registros de operações financeiras de crédito e débito. Essa gênese está atrelada ao surgimento do Bitcoin, que foi o ecossistema onde floresceu a tecnologia Blockchain.

[12] "O propósito da mineração é frequentemente confundido com a criação de novas moedas. De fato, o processo de mineração gera novas moedas, porém esse artifício é usado como incentivo para que os participantes do sistema contribuam com o principal objetivo da mineração, que é validar as transações da rede sem a necessidade de uma autoridade central. Mesmo depois de uma nova transação ser propagada, o valor de saída somente pode ser gasto pelo destinatário após a transação ter sido verificada e incluída em um bloco através do processo chamado mineração. Quando a construção do bloco é finalizada, ele é adicionado à cadeia de blocos, e todas as transações nele contidas recebem uma 'confirmação'. Sempre que um novo bloco é minerado, todas as transações já presentes no registro da blockchain recebem uma nova confirmação, de forma que o número de confirmações representa a profundidade da transação na cadeia de blocos" (MARTINS, 2018, p. 34-35).

[13] https://www.ethereum.org.

[14] Informação colhida em ARAÚJO, Felipe. Aula 2: Ethereum. *Blockchain simplificada*. Curso online do ITS Rio, 16m45s, acesso em 22 de dezembro de 2018.

[15] Exemplo extraído de ALEIXO, Gabriel. Aula 1: Bitcoin: o começo de (quase) tudo. *Blockchain simplificada.* Curso online do ITS Rio, 1h06m48s, acesso em 22 de dezembro de 2018.

[16] Informação colhida em ARAÚJO, Felipe. Aula 2: Ethereum. *Blockchain simplificada*. Curso online do ITS Rio, 24m45s, acesso em 22 de dezembro de 2018.

[17] "O potencial da tecnologia blockchain reside em sua capacidade de oferecer serviços transparentes, livres de censura ou discriminação de uma maneira descentralizada para finalidades amplas; a partir do acesso mais equânime a um conjunto de instituições digitais (que permitem realizar votações, pagamentos, contratos, etc.)". (ALEIXO, 2018).

[18] André Roque chega a dizer que essa tecnologia pode superar o uso da ata notarial como método de documentação. (ROQUE, 2018).

[19] Nick Szabo falava dos smart contracts já na década de 1990, tratando-os como contratos cujos protocolos de controle (cláusulas capazes de atestar e validar o cumprimento das obrigações reciprocamente atribuídas) poderiam ser estabelecidos por meio de códigos de programação computacional (SZABO, 1997).

[20] Uma máquina de refrigerantes é uma espécie de ancestral dos smart contracts: inserido o meio de pagamento, o software gera um crédito que dá ao usuário o poder de compra de um dos produtos do display; basta que ele escolha o produto para que ele lhe seja entregue. Neste caso, os protocolos de controle (inserção de determinadas cédulas ou moedas; geração do crédito; escolha do produto; entrega do produto) estão determinados previamente, por meio de códigos de programação computacional (SZABO, 1997).

[21] Tais contratos podem ajudar a "diminuir significativamente algumas possibilidades de falha humana, além de tornar menos custosos os protocolos de controle existentes em torno dos contratos, criados justamente para avaliar se determinadas cláusulas foram ou não cumpridas. Em um ambiente digital marcado por grande automação, procedimentos de controle como uma auditoria, por exemplo, demandariam muito menos tempo e recursos financeiros do que opções tradicionais" (ALEIXO, 2018).

[22] Conforme art. 158-A, Código de Processo Penal, cadeia de custódia é "o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte".

[23] O conceito legal é muito próximo daquele enunciado por Robert A. Doran: "The chain of custody is a process used to maintain and document the chronological history of physical evidence. This process should result in a product: the formal documentation of the process" (DORAN, 2005).

[24] O art. 158-B do CPP trata (i) do reconhecimento do elemento como de potencial interesse para a investigação; (ii) do seu isolamento para evitar que se altere o estado das coisas, configurando-se fraude processual a entrada em locais isolados bem como a remoção de quaisquer vestígios de locais de crime antes da liberação por parte do perito responsável (art. 158-C, §2º); (iii) da fixação, consistente na descrição detalhada do vestígio, inclusive com ilustração por fotografia ou outros meios de documentação; (iv) da coleta, que deve ser realizada preferencialmente por perito oficial

(art. 158-C), com preservação das suas características; (v) do acondicionamento, com registro dessas características específicas; (vi) do transporte; (vii) do recebimento, como ato formal de transferência da posse do vestígio; (viii) do processamento, consistente na manipulação do vestígio de acordo com a metodologia adequada às suas características biológicas, físicas e químicas, a fim de se obter o resultado desejado, que deve ser formalizado em laudo produzido por perito; (ix) do armazenamento, consistente na guarda, em condições adequadas, do material a ser processado, para realização de contraperícia; e (x) do descarte, procedimento referente à liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial.

## 8. REFERÊNCIAS BIBLIOGRÁFICAS

ALEIXO, Gabriel. Aula 1: Blockchain e Direito. *Blockchain e seus aspectos jurídicos*. Curso online do ITS Rio. Acesso em: 23 dez 2018.

_____. Aula 1: Bitcoin: o começo de (quase) tudo. *Blockchain simplificada*. Curso online do ITS Rio. Acesso em: 22 dez 2018.

_____. *Como o Bitcoin e os Smart Contracts Estão Transformando os Modelos de Negócios*. Disponível em: <https://medium.com/@gabrielaleixo/como-o-bitcoin-e-os-smart-contracts-estão-transformando-os-modelos-de-negócios-731025529e11> Acesso em: 23 dez 2018.

ARAÚJO, Felipe. Aula 2: Ethereum. *Blockchain simplificada*. Curso online do ITS Rio. Acesso em: 22 dez 2018.

BRASIL. Tribunal de Justiça de São Paulo, 31ª Câmara de Direito Privado, Agravo de Instrumento 2222371-76.2019.8.26.0000, rel. Des. José Augusto Genofre Martins, j. 07/11/2019, DJe 12/11/2019.

BRASIL. Superior Tribunal de Justiça, 4ª Turma, REsp 1046497/RJ, rel. Min. João Otávio de Noronha, j. 24/08/2010, DJe 09/11/2010.

DE FILIPPI, Primavera; WRIGHT, Aaron. *Blockchain and the Law: the rule of code.* Cambridge, Massachusetts: Harvard University Press, 2018, *ebook* Kindle.

DIDIER JR., Fredie; BRAGA, Paula Sarno; OLIVEIRA, Rafael Alexandria de. *Curso de direito processual civil*: teoria da prova, direito probatório, decisão, precedente, coisa julgada, processo estrutural e tutela provisória. 15ed. Salvador: Ed. Jus Podivm, 2020, v. 2.

DORAN, Robert A. *Exploring the links in the chain of custody*. Disponível em: <https://pt.scribd.com/document/66568187/Exploring-the-Links-in-the-Chain-of-Custody> Acesso em: 27 dez 2019.

LAGO Jr., Antônio. *Responsabilidade civil por atos ilícitos na internet*. São Paulo: LTr, 2001.

MAGNUS, Tiago. *Tudo que você precisa saber sobre o que é Blockchain e como funciona*. Disponível em: < https://transformacaodigital.com/tecnologia/o-que-e-blockchain/ >. Acesso em: 3 fev 2020.

MARCACINI, Augusto Tavares Rosa. *O documento eletrônico como meio de prova*. Obtido em: <http://www.advogado.com/internet/zip/tavares.htm>. Acesso em: 21 dez 2006.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. *Comentários ao Código de Processo Civil*. 2 ed. São Paulo: RT, 2005, v. 5, t. 2.

MARQUES, Antônio Terêncio G. L. *A prova documental na internet*. Curitiba: Juruá, 2005.

MARTINS, Thiago Fonseca. *Prova de existência de arquivos digitais utilizando a tecnologia blockchain do protocolo Bitcoin.* Monografia apresentada como requisito parcial para a obtenção do grau de Bacharel em Engenharia da Computação. Porto Alegre: Universidade Federal do Rio Grande do Sul (UFRGS), 2018.

MELO, Letícia Marcele do Nascimento. *Distributed Ledger Technology (DLT) como prova*: a atipicidade do blockchain, sua força probante e aplicações ao direito probatório. Monografia apresentada como requisito parcial para a obtenção do grau de Bacharel em Direito. Salvador: Universidade Federal da Bahia (UFBA), 2018.

PRADO, Geraldo. *Prova penal e sistema de controles epistêmicos*: a quebra da cadeia de custódia das provas obtidas por métodos ocultos. São Paulo: Marcial Pons, 2014.

ROQUE, André Vasconcelos. *A tecnologia blockchain como fonte de prova no processo civil*. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/novo-cpc/a-tecnologia-blockchain-como-fonte-de-prova-no-processo-civil-15102018> Acesso em: 23 out 2018.

SZABO, Nick. *Formalizing and Securing Relationships on Public Networks*. Disponível em: <https://nakamotoinstitute.org/formalizing-securing-relationships/> Acesso em: 23 dez 2018.

*Fredie Souza Didier Jr.*

Mestre em Direito pela UFBA.
Doutor em Direito pela PUC/SP.
Livre-docente pela USP.
Pós-doutorado pela Universidade de Lisboa.
Professor associado da Universidade Federal da Bahia, nos cursos de graduação, mestrado e doutorado.
Membro da Associação Internacional de Direito Processual, do Instituto Iberoamericano de Direito Processual, do Instituto Brasileiro de Direito Processual e da Associação Norte e Nordeste de Professores de Processo.
Advogado e consultor jurídico.

*Rafael Alexandria de Oliveira*

Mestre em Direito Público (UFBA).
Especialista em Direito Processual Civil (Fac. Jorge Amado/Juspodivm).
Professor do Programa de Pós-Graduação *Lato Sensu* da Faculdade Baiana de Direito.
Membro da Associação Norte e Nordeste de Professores de Processo (ANNEP).
Procurador do Município do Salvador/BA.
Advogado.