XI CONGRESSO RECAJ-UFMG

ACESSO À JUSTIÇA E TECNOLOGIA

A174
Acesso à justiça e tecnologias do processo judicial [Recurso eletrônico on-line] organização XI Congresso RECAJ-UFMG: UFMG – Belo Horizonte;

Coordenadores: Edgar Gastón Jacobs Flores Filho, Caio Augusto Souza Lara e Lucas Jerônimo Ribeiro da Silva – Belo Horizonte: UFMG, 2020.

Inclui bibliografia
ISBN: 978-65-5648-253-8
Modo de acesso: www.conpedi.org.br em publicações
Tema: Desafios, travessias e potencialidades para o direito e o acesso à justiça face aos algoritmos, ao big data e à inteligência artificial.
1. Direito. 2. Tecnologia. 3. Acesso à justiça. I. XI Congresso RECAJ-UFMG (1:2020: Belo Horizonte, MG).

CDU: 34

XI CONGRESSO RECAJ-UFMG

ACESSO À JUSTIÇA E TECNOLOGIA

Apresentação

É com imensa satisfação que o Programa RECAJ-UFMG – Acesso à Justiça pela Via dos Direitos e Solução de Conflitos da Faculdade de Direito da Universidade Federal de Minas Gerais e o CONPEDI – Conselho Nacional de Pesquisa e Pós-graduação em Direito tornam público à comunidade científica o conjunto dos oito livros produzidos a partir dos Grupos de Trabalho do XI Congresso RECAJ-UFMG: Desafios, travessias e potencialidades para o Direito e o Acesso à Justiça face aos algoritmos, ao big data e à inteligência artificial. As discussões ocorreram em ambiente virtual ao longo dos dias 18, 19 e 20 de novembro de 2020, dentro da programação que contou com grandes nomes nacionais e internacionais da área, além de cento e sessenta e três pesquisadoras e pesquisadores inscritos no total, provenientes de quatorze Estados da federação (AC, AM, BA, CE, MG, PA, PE, PR, RJ, RO, RS, SC, SE e SP). Os livros compõem o produto deste congresso, que há mais de uma década tem lugar cativo no calendário científico nacional.

Trata-se de coletânea composta pelos cento e oito trabalhos aprovados e que atingiram nota mínima de aprovação, sendo que também foram submetidos ao processo denominado double blind peer review (dupla avaliação cega por pares) dentro da plataforma PublicaDireito, que é mantida pelo CONPEDI. Os oito grupos de trabalho geraram cerca de seiscentas páginas de produção científica relacionadas ao que há de mais novo e relevante em termos de discussão acadêmica sobre diversos temas jurídicos e sua relação com a tecnologia: Acesso à Justiça e tecnologias do processo judicial; Direito do Trabalho no século XXI; Estado, governança, democracia e virtualidades; tecnologias do Direito Ambiental e da sustentabilidade; formas de solução de conflitos, educação e tecnologia; Direitos Humanos, gênero e tecnologias da contemporaneidade; inteligência artificial, startups, lawtechs e legaltechs; e Criminologia e cybercrimes.

Os referidos Grupos de Trabalho contaram, ainda, com a contribuição de vinte e quatro proeminentes pesquisadores ligados a renomadas instituições de ensino superior do país, dentre eles alguns mestrandos e doutorandos do próprio Programa de Pós-graduação em Direito da UFMG, que indicaram os caminhos para o aperfeiçoamento dos trabalhos dos autores. Cada livro desta coletânea foi organizado, preparado e assinado pelos professores e pós-graduandos que coordenaram os trabalhos. Sem dúvida, houve uma troca intensa de saberes e a produção de conhecimento de alto nível foi, certamente, o grande legado do evento.

Nesta esteira, a coletânea que ora se apresenta é de inegável valor científico. Pretende-se, com esta publicação, contribuir com a ciência jurídica e com o aprofundamento da relação entre a graduação e a pós-graduação, seguindo as diretrizes oficiais da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES. Importante lembrar, ainda, da contribuição deste congresso com a formação de novos pesquisadores na seara interdisciplinar entre o Direito e a tecnologia, uma vez que o número de graduandos que apresentaram trabalhos de qualidade foi expressivo.

O Programa RECAJ-UFMG existe desde 2007 e foi criado poucos meses após o Conselho Nacional de Justiça ter iniciado o Movimento pela Conciliação. Durante a I Semana Nacional de Conciliação, em 2006, a Faculdade de Direito da UFMG, por meio de seu então diretor, Professor Doutor Joaquim Carlos Salgado, firmou o compromisso, em 4 de dezembro de 2006, de envidar esforços para incluir disciplina sobre as formas de solução de conflitos na grade curricular da faculdade.

De forma pioneira no país e observando a necessidade de estudo e aprofundamento dos temas do acesso à justiça e das formas de solução de conflitos complementares ao Poder Judiciário, a Professora Doutora Adriana Goulart de Sena Orsini passou a ofertar a disciplina “Formas de Resolução de Conflitos e Acesso à Justiça” no período de 2007-2017, em todos os seus semestres na Faculdade de Direito da UFMG.

Nesse contexto, o Programa RECAJ-UFMG atua desde o início em atividades de ensino, pesquisa e extensão em acesso a justiça pela via dos direitos e soluções de conflitos. Reúne grupos de alunos e ex-alunos da graduação e da pós-graduação stricto sensu que, sob orientação da Prof. Adriana, passaram a estudar de forma aprofundada os temas nucleares do Programa e aqueles que lhes são correlatos. Desenvolvendo uma série de projetos, tais como grupo de estudos, disciplinas optativas, seminários, pesquisas, cursos de formação, atividades de extensão, dentre outras, o Programa RECAJ-UFMG honra a sua vocação para ações variadas em seus temas de forma responsável, séria, atualizada, científica e contemporânea. No RECAJ-UFMG, a indissociabilidade entre o ensino, pesquisa e a extensão é uma marca distintiva.

Agradecemos ainda a todas as pesquisadoras e pesquisadores pela inestimável contribuição e desejamos a todos uma ótima e proveitosa leitura!

Belo Horizonte-MG, 26 de novembro de 2020.

Profª. Drª. Adriana Goulart de Sena Orsini - Coordenadora do Programa RECAJ-UFMG

Prof. Dr. Caio Augusto Souza Lara - SKEMA Business School/ESDHC/CONPEDI

Prof. Dr. José Eduardo Resende Chaves Júnior - SKEMA Business School/PUC Minas

BLOCKCHAIN: USO DA INFORMAÇÃO COMO MEIO DE PROVA NO PROCESSO CIVIL

BLOCKCHAIN: INFORMATION USE AS PROOF IN THE CIVIL PROCESS

Lusimábile Cassiano Koda [1]

Resumo

Este artigo busca como a informação construída e armazenada numa blockchain é confiável para ser usada como meio de prova no processo civil brasileiro. Explora o entendimento blockchain para o contexto jurídico – o que resulta na identificação de aspectos positivos e negativos. Analisa casos concretos que usaram provas registradas na blockchain. Apresenta a compreensão para autenticidade documental, prova documental e prova documentada. Aborda limitações probatórias e de rito processual para o bom manuseio das provas. Observa o tratamento processual legal da autenticidade. Identifica e analisa as mudanças legislativas recentes, a Estratégia do Governo Digital e a implantação do e-Notariado.

Palavras-chave: Autenticidade, Blockchain, E-notariado, Processo civil, Provas documentais

Abstract/Resumen/Résumé

This paper studies how the information in a blockchain is reliable in order to be used as evidence in the Brazilian civil process. It explores the understanding of blockchain for the legal context - which results in the identification of positive and negative aspects. It studies concrete cases have been used evidence registered in the blockchain. It analyzes the evidential and procedural rite limitations for the good handling of the evidence. Addresses notary use for authenticity. Observes the legal procedural treatment of authenticity. It identifies and analyzes the recent legislative changes, the Digital Government Strategy and the implementation of e-Notary.

Keywords/Palabras-claves/Mots-clés: Authenticity, Blockchain, E-notary, Civil process, Documentary evidence

[1] Bacharel em Direito pela UniMetrocamp, especialista em Gestão Estratégica de Projetos pela FGV-SP com atuação em projetos de gestão empresarial e TI.

1 INTRODUÇÃO

Numa sociedade que vive a era da informação, com evolução constante e impactos nas mais diversas esferas, a possibilidade de aceitação do uso de novas tecnologias na formação dos meios de prova no processo civil entende-se como benéfica para a busca da verdade judicial.

Por conta da pandemia mundial de coronavírus, a resistência do poder judiciário em adoção de tecnologias tem sido revista até para continuidade de seus trabalhos. A *blockchain*, com o reconhecimento gradual de seu valor pelos países e corporações, é algo que merece entrar o quanto antes no radar das instituições brasileiras.

Em que consiste tal tecnologia *blockchain*? Tal tecnologia seria confiável? Há aplicações em uso no país para fins documentais e, portanto, judiciais? O ordenamento jurídico brasileiro possibilita ou dificulta a adoção das informações formadas nesta tecnologia como meios de prova?

Diante da incipiência do tema no processo civil e, por conseguinte, de sua presença nos julgados do país, valeu-se de uma pesquisa exploratória com uma pluralidade de fontes de pesquisa, tais como: a jurisprudência sobre provas atípicas e documento eletrônico, notícias de imprensa, material produzido por centros de pesquisa tecnológicos e juristas que abordam a temática do direito probatório, como Carnelutti, Marinoni e Arenhart.

2 BLOCKCHAIN: ORIGENS E CONCEITOS

O tema blockchain tem sua origem na Ciência da Computação associada ao campo da Criptografia[1]. Ao contrário do que muitos possam pensar, a ideia não é propriamente inovadora. Watternhofer[2] (2017) registra que na década de 70 tem-se os fundamentos desta tecnologia. Nos anos 90, da discussão em um grupo resultou um texto[3] que explorara pontos que estariam presentes numa tecnologia apresentada 15 anos depois, a *blockchain*.

Numa *blockchain* o elemento transacionado não se resume a criptomoedas, pode ser um valor, conforme explica Tapscott (2016), uma ação, um título, pontos de fidelidade,

[1] A Criptografia é o braço da Matemática que nos permite criar provas matemáticas que conferem altos níveis de segurança. O comércio eletrônico e o internet banking beneficiam-se da criptografia (Bitcoin Project 2009-2020). Dito de outra forma, é um método prático para proteger a informação transmitida e armanezada eletronicamente. Utiliza-se de técnicas da matemática para cifrar os dados deixando-os ininteligíveis e, portanto, mantendo-os privados.

[2] Professor de computação do Instituto Federal de Tecnologia da Suíça em entrevista ao documentário "The Blockchain and Us" de Manuel Stagars.

[3] "A Cypherpunk's Manifesto" foi assinado pelo matemático Eric Hughes em março de 1993 e está disponível em https://www.activism.net/cypherpunk/manifesto.html

propriedade intelectual, música, arte, voto, crédito de carbono, entre outros bens. Danziger (2018), declarou que é o maior legado por trás das criptomoedas com "potencial para melhorar as relações econômicas e sociais de nossa sociedade inserindo alto grau de confiança".

Uma aplicação que use *blockchain* transacionará um valor entre duas partes. E cada transação (fato) é, necessariamente, validada[4]. Após a validação, um conjunto de várias transações é inserido e encerrado num bloco de informações. Não é possível estornar ou alterar a transação depois.

Braga (2017, p.12) elencou alguns benefícios decorrentes das propriedades técnicas da *blockchain*: a) a imutabilidade dos registros; b) a atualidade, devido à atualização constante e periódica da base de dados distribuída; c) a irrefutabilidade, pois uma transação replicada para os nós da rede não pode ser negada pelo seu autor; d) prevenção contra duplicação de transações; e) transparência, pois todos os nós e softwares clientes visualizam as transações registradas; f) descentralização, pois todo nó é coproprietário do ledger, nenhum nó tem controle absoluto e ninguém pode reivindicar sua propriedade; g) desintermediação, no sentido de eliminar "intermediários artificiais entre sistemas", o que torna os processos mais simples.

Fazendo-se um paralelo entre aspectos técnicos da *blockchain* e os atributos dos dados coletados nela, para fins de atividade probatória no ambiente processual, tem-se o quadro seguinte.

ASPECTO TÉCNICO	**ATRIBUTO INFORMACIONAL**
IMUTABILIDADE DOS REGISTROS	CONFIABILIDADE-SEGURANÇA - INTEGRIDADE – RASTREABILIDADE - AUDITABILIDADE
ATUALIDADE	AGILIDADE - DISPONIBILIDADE
IRREFUTABILIDADE	CONFIABILIDADE
PREVENÇÃO CONTRA DUPLICAÇÃO	UNICIDADE - CONFIABILIDADE-SEGURANÇA
TRANSPARÊNCIA	CONFIABILIDADE – SEGURANÇA
DESCENTRALIZAÇÃO	SEGURANÇA – DISPONIBILIDADE
DESINSTERMEDIAÇÃO	AGILIDADE – SIMPLIFICAÇÃO

Fonte: Autoria própria, 2020.

3 QUESTÕES PRÁTICAS SOBRE *BLOCKCHAIN*

A evolução é da essência da ciência computacional. Assim, soluções em uso atual podem se tornar obsoletas. Em termos de *blockchain*, o que se abordará nas exposições

[4] A validação é a chamada mineração, um processo de recompensa em criptomoeda para o minerador que resolve o desafio matemático.

seguintes é o que se tem visto na arquitetura corrente da tecnologia.

Em termos processuais, várias questões práticas podem se apresentar. Diante disso, abordam-se algumas na sequência e de que modo os dados coletados numa *blockchain* seriam ou não de auxílio à questão probatória do processo civil.

3.1 COMO SE DÁ O ACESSO AOS DADOS GRAVADOS NUMA REDE *BLOCKCHAIN*?

Tendo-se em vista a amplitude do conceito de dados e o objeto da presente pesquisa, convém significar dados nesta abordagem como os registros que possibilitam extrair informações das transações com relevância jurídica. A transação pode ser, por exemplo, uma compra de criptomoeda, um contrato criado, a letra de uma música, a autencidade de um documento.

Delimitação feita, observa-se que há diversos tipos de usuários[5] numa *blockchain*, cada tipo com papel próprio a desempenhar. É congruente, o que conferiria maior imparcialidade, pensar em dois tipos de usuários: a) alguém que não transaciona valores e não é participante da rede, ou seja, alguém que fará somente consultas; b) alguém que transaciona valores, o *business user*. Em se tratando do autor ou réu da ação, não é raro observar ações judiciais em que um ou ambos são usuários de negócios, cujo papel é somente vender ou comprar valores na rede.

Para abordagem probatória, o relevante é a consulta à *ledger*, cujo acesso é público ou privado. A *ledger*, como já definido anteriormente, consiste na base de dados, o local onde estão registradas todas as transações de valor, seus detalhes e os blocos que encerram essas transações, funcionando como um genuíno livro contábil de registros.

Feito uma ressalva às diferenças, como o acesso a um *smartphone* e aos aplicativos contidos nele, uma blockchain pode ser concebida de modo que os acessos e as ações dentro dela sejam controlados ou livres. Desse modo, há as *blockchain*s de acesso permissionado e acesso não permissionado (GUPTA, 2020, p. 15; FORMIGONI, BRAGA, LEAL, 2016, p. 8).

Uma *blockchain* de *ledger* pública disponibiliza a consulta direta dos dados pela internet através dos chamados exploradores de bloco. Por eles ao usuário é possível examinar os blocos e as transações. São alguns exemplos: Block Explorer, Blockchain.com, Blockchair, BlockCypher, CoinMarketCap e Tokenview.

A *blockchain* de *ledger* privada é a do tipo permissionado. Quem precisar dos dados como material probatório e for um *business user*, em tese, não terá grandes dificuldades para

[5]Segundo Manav Gupta (2020, p. 18), há diversos tipos de usuários presentes na operação de uma rede *blockchain*: usuário de negócios, regulador, desenvolvedor, operador de rede, autoridade de certificado. Observa-se que não são todas *blockchains* que possuem mineradores.

obtê-lo. O quê não ocorrerá com um não participante desta rede que, para obter informação dela, terá que usar o expediente judicial se o caminho administrativo não for suficiente.

3.2 O DADO REGISTRADO NUMA *BLOCKCHAIN* É CONFIÁVEL?

Os aspectos técnicos abordados antes como a imutabilidade de registros, a descentralização e a transparência dificultam em alto grau a atividade de nós mal intencionados na rede. Assim, supor uma tentativa de fraudar transações dentro do bloco, deverá ter como premissa um ataque simultâneo em todos os nós da rede, ou seja, em todos os computadores e locais de armazenamento daquela *blockchain* no mundo – o que exige imenso esforço computacional. Ao se tratar de um ataque a uma *blockchain* não pública, além dos esforços citados, haverá um obstáculo adicional: penetrar em tal rede.

O próprio modo de funcionar da *blockchain* usa criptografia dentro de criptografia. A alteração de qualquer dado dentro do bloco não passa desapercebida.

3.3 COMO SABER A IDENTIDADE DAS PARTES ENVOLVIDAS NUMA TRANSAÇÃO NUMA *BLOCKCHAIN*?

Observa-se que as *blockchain*s de acesso permissionado à rede, as *blockchain*s privadas, tratam a identificação do usuário de modo mais tradicional, pois cada usuário da rede tem uma *única* identidade que, por sua vez, tem sua gestão e controle centralizados em um administrador e com suas próprias regras de identificação. Esse administrador pode estar, por exemplo, dentro um órgão público, como a RIK[6], ou dentro de um departamento de uma empresa, como é o caso da IBM, Mastercard e da BMW.

Não é suficiente saber que existe uma identidade, essa precisa ser consultada no contexto da transação de valor para fins de produção da prova documental. Como abordado na primeira questão, o que é determinante para isto é o acesso à *ledger*. Isso, em se tratando de *blockchain*s privadas, pode ser apoiado por um novo instrumento jurídico.

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei 13.709/2018[7], é uma norma

[6]Sigla da agência estatal do Ministério da Justiça da Estônia (Centro de Registros e Sistemas de Informação), cujo site é https://www.rik.ee/en/agency .

[7]Sob a justificação do Ministro da Economia Paulo Guedes, com receio da sociedade não conseguir se adequar para a aplicação ordenada da LGPD por conta dos impactos "da crise provocada pela pandemia do coronavírus", a lei teve sua entrada em vigor adiada para 03/05/2021 (Medida Provisória nº 959/2020). Mas se a MP 959 caducar, devido à aprovação do PL 1.179/20, a LGPD deve entrar em vigor em agosto de 2020.

que poderá dar um norte a tal tarefa dentro de uma tecnologia complexa como é a *blockchain*.

Embora se identificam certas não-aderências no modo de funcionamento da *blockchain* com a LGPD, o que é relevante para a questão investigatória e probatória são as aderências à lei. Desse modo, a LGPD consiste um relevante instrumento ao acesso de identificação das partes pelo fato de ser aderente a este contexto em várias disposições.

Em apertada síntese, menciona-se: a) sua disposição geral; b) alguns de seus fundamentos; c) os casos de aplicabilidade; d) o conceito de coleta em solo nacional; e) o conceito de agentes de tratamento; f) o conceito de tratamento de dados; g) a previsão do exercício de direitos em processo judicial, administrativo ou arbitral; h) o acesso facilitado às informações como um direito do titular dos dados; i) os direitos do titular dos dados; j) o exercício em juízo dos direitos do titular; k) a divulgação pública do responsável pela adminstração dos dados; l) a obrigação de reparação; m) a inversão do ônus da prova a favor do titular para fins de produção de prova; n) as sanções aplicáveis aos infratores.

Uma vez entendida como se dá a identificação do usuário na *blockchain* privada, nas atuais *blockchain*s públicas o modo de identificação do usuário não é o mesmo que aquela. Convém saber que não há um padrão único na forma de identificação entre as *blockchain*s públicas, contudo existem semelhanças[8] em vários aspectos entre a Bitcoin *blockchain* e as que surgiram depois. O que não significa um compromisso de modelo a ser adotado pelas comunidades de desenvolvedores que mantêm as *blockchain*s.

Para abordagem das identidades numa *blockchain* pública, tomar-se-á o exemplo da Bitcoin *blockchain* por sua dominância[9] e influência nas demais *blockchain*s.

Devido às versões controversas sobre o anonimato nas *blockchain*s, menciona-se que há possibilidade de ser ou não ser anônimo na rede – o que dependerá da interpretação que será dada a anonimato. De um modo direto, se o dado da parte envolvida na transação permitir que se identifique a parte, não há anonimato, mas, se a identificação não for possível, há anonimato (NARAYANAN *et al*, 2016) e, assim, a confidencialidade estará preservada.

Far-se-á uma analogia com o e-mail para compreensão. Sabe-se que João Pedro Silva pode fazer uso de uma conta joapedrosilva@dominio.com.br, mas também pode usar várias outras para se comunicar, por exemplo, a conta silva_89@dominio.net. Se quem receber uma mensagem da última conta, não conseguir identificar que é João Pedro Silva o remetente, há

[8]É observável que outras criptomoedas emprestam vários conceitos da Bitcoin como, por exemplo, seu código-base para serem usados em suas *blockchains* (NARAYANAN *et al*, p. 454, 2016).

[9]Segundo consulta de 21/05/2020, em https://blockchair.com/compare, a Bitcoin tem participação de 66% no mercado de criptomoedas.

anonimato; caso contrário, se a identificação é feita, a conta não é anônima.

Por esta razão é que mencionam que a *blockchain* não garante o anonimato, não preserva a confidencialidade ou mesmo que há um pseudo-anonimato (NARAYANAN *et al*, p. 278, 2016; BRAGA, p. 25, 2017; PIRES, p. 34, 2016). Narayanan (2015) cita em sua aula que o "Bitcoin won´t hide you from NSA´s prying eyes"[10].

Diante disto, se pelo pseudônimo do usuário envolvido na transação conseguir-se identificar a parte que se deseja na transação, esse registro na *blockchain* poderá ser constituído como prova no processo. Prova, conforme disserta Marinoni (2015, p. 69), no sentido de ser um instrumento do qual "se serve o magistrado para o conhecimento dos fatos submetidos à sua análise" ou "ainda o resultado da atividade lógica do conhecimento."

Assim, como no e-mail, "a identidade real da pessoa não é requerida" para transferir valores na rede *blockchain*. "Qualquer usuário pode criar qualquer número de pares de chave a qualquer momento" (NARAYANAN *et al*, p. 123, 2016). Pares de chave? Sim, numa Bitcoin *blockchain*[11], ao invés do uso de uma identidade pessoal real, há um "endereço" (Bitcoin address) por trás da identidade que é uma chave pública[12] , cujo formato é de um código alfanumérico. Por exemplo, bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq, sendo que chave pública (*public key*) quer significar o mesmo que endereço público (*public address*).

Entretanto, quando se trata de criptomoedas, como na atividade bancária, busca-se a manutenção do sigilo. A questão da *privacidade e da segurança nas criptomoedas repercute no anonimato do usuário*. Como exposto, há transparência na *blockchain*, isto é, qualquer um pode procurar uma transação de um "endereço" na rede. Uma vez que você informa o "endereço" para receber o depósito a privacidade está comprometida. Uma das razões que é recomendado e incentivado que se crie um "endereço" a cada nova remessa de criptomoeda.

3.4 POSSO PEDIR A PENHORA OU BLOQUEIO NO PROCESSO?

Considerando a característica de uma *blockchain* como a descentralização, no presente, para as atuais redes de criptomoedas isto não é possível. O que faz da rede um destino seguro para o resultado das vendas de entorpecentes, lavagem de dinheiro, sequestro de dados.

[10]Bitcoin não vai te esconder dos olhares indiscretos da NSA [tradução nossa].

[11]Observável também em diversas outras *blockchains* públicas como, por exemplo, Ethereum, Bitcoin cash, Litecoin.

[12]O segundo elemento do par é a chave privada (*private key*) que funciona como uma senha para efetuar a transação e somente o usuário tem acesso a ela.

Convém relembrar que as *blockchain*s de criptomoedas tratam-se de um tipo de construção contínua de transações validadas e imutáveis mediante consenso[13] e em nível global. Esta atual arquitetura de funcionamento, por si só, demandará uma nova concepção para que tal tipo de controle seja possível – o que exige uma agenda de intenções diversa da atual.

4 PROVA DOCUMENTAL E PROVA DOCUMENTADA COMO MEIO DE PROVA

Embora as expressões "prova documental" e "prova documentada" mostrem aparente proximidade, seus conceitos apresentam uma sutileza em sua distinção. Distinção essa que não é meramente acadêmica ou teórica.

Se o documento for apto a indicar *diretamente* um fato, constituirá prova documental, mas, se representar um fato de forma *indireta*, constituirá prova documentada (MARINONI, ARENHART, 2015, p. 611). Assim, a prova documental se basta para narrar o fato, ou melhor, narrar a afirmação do fato feita pelo autor da ação. A prova documentada é insuficiente, há um intermediário que usa sua compreensão do fato para narrá-lo.

As provas formadas - tendo como base a *blockchain* - podem ser de *ambos* os tipos dependendo do tipo de valor transacionado na rede e do caso concreto. A própria arquitetura de funcionamento da *blockchain* permite que as transações ali registradas funcionem como provas documentais - considerando-se que o objeto de prova tenha como fato alegado determinada transação.

Mesmo o direito à prova tendo status de norma constitucional, o legislador estabeleceu certas limitações à liberdade probatória, às provas judiciárias que a parte pode fazer uso. São elas: a retirada legal do juiz poder analisar livremente a prova colhida, a vedação do uso das provas consideradas ilícitas e a restrição do rito procedimental conforme o meio de prova específico disponível (VILAR FILHO, 2006, p. 175).

Ao presente capítulo interessa a última limitação, isto é, a restrição do procedimento conforme o meio de prova disponível que, longe de ser uma imposição inconstitucional[14], justifica-se por realizar o valor da efetividade ao processo. Tratam-se das limitações probatórias

[13] "Consenso distribuído é um termo da ciência da computação usado na disciplina de sistemas distribuídos e é um aspecto crítico do *Blockchain* e das criptomoedas. Consenso significa que quase todos (os envolvidos) concordam. Consenso é diferente de unanimidade, uma vez que nem todos tem que concordar, basta que a maioria concorde." (BRAGA, 2017, p. 5)

[14] José Eduardo Vilar Filho aborda em sua dissertação "Prova judiciária e verdade: enfoque constitucional" quais seriam os casos que levariam à inconstitucionalidade.