REVISTA ACADEMICA
Faculdade de Direito do Recife
Vol. 94 n. 02 – Anno CXXXI

BLOCKCHAIN COMO NOVO VEÍCULO DA PROVA DIGITAL, UMA EXPERIÊNCIA CHINESA

BLOCKCHAIN AS A NEW VEHICLE OF ELECTRONIC EVIDENCE, A CHINESE EXPERIENCE

Recebimento em 20/01/2022
Aceito em 28/10/2022

Xinkai Luo[1]
http://orcid.org/0000-0001-9984-6185
yc07209@umac.edu.mo

RESUMO

No presente trabalho, será abordada a extensão do conceito de prova digital na nova era da blockchain, bem como o significado da aplicação da blockchain na geração de provas digitais no ordenamento jurídico chinês. O artigocompreende uma explicação do papel fundamental da verificação da prova digital alicerçada na blockchain e uma análise do primeiro caso decidido na China com base na prova digital preservada pela tecnologia blockchain. Discute-se a possibilidade de que, em um futuro próximo, com vista a aumentar a credibilidade do sistema de geração de provas digitais e reforçar o processo de preservação da prova, a generalidade dos órgãos judiciais podem reconhecer o estatuto legal da prova digital preservada pela tecnologia blockchain.

Palavras-chave: Prova digital; blockchain; autenticidade e integridade de prova; Tribunal de Internet da China.

ABSTRACT

In this paper, it will be addressed the extension of the concept of digital evidence in the new era of blockchain, as well as the significance of the application of blockchain in generating digital evidence in the Chinese legal system. The article comprises an explanation of the fundamental role of the verification of digital evidence founded on blockchain and an analysis of the first case decided in China based on digital evidence preserved by blockchain technology. It will be discussed the possibility that in the coming future, while increasing the credibility of the digital evidence generation system and strengthening the evidence preservation process, the generality of judicial entities could recognize the legal status of digital evidence preserved by blockchain technology.

Keywords: electronic evidence; blockchain; authenticity and integrity of evidence; China's Internet Court.

[1] UNIVERSITY OF MACAU.

https://doi.org/10.51359/2448-2307.2022.253028

1 INTRODUÇÃO

Historicamente, o conceito de prova digital plasmou-se mais tarde face às demais tipologias de prova. Contudo, devido à evolução da tecnologia informática, a prova digital acabou por ser a modalidade que sofreu um maior alargamento da sua esfera (MESQUITA, 2010, p. 36). Há cada vez mais espécies de prova digital sendo consideradas como provas admissíveis, sendo a prova digital transmitida pela tecnologia blockchain um exemplo. A Chinaemitiuregras explícitas, admitindo a utilização de dados preservados através da tecnologia de blockchain (doravante designada como "TBC"), passando a ser reconhecidos como fonte de prova nos processos judiciais.Tal desenvolvimento foi originado pela sentença proferida por Tribunal de Internet, o qual é um tribunalde competência especializada visando a resolução dos litígios provindos da internet. Atualmente, são três os tribunais de Internet na China, criados em Hangzhou,Pequime Guangzhou[2].

Em 2015, o Supremo Tribunal Popular da China definiu,pela primeira vez,o conceito de prova digital nos artigos 116º da Interpretação sobre implementação da Lei Processual Civil[3] como: Os dados eletrônicos incluem: correio eletrônico, intercâmbio eletrônico de dados, blogue, *microblog, SMS*, assinaturas eletrônicas, domínios e outras informações formadas ou preservadas em meios eletrônico.[4]Para além disso,nosartigos 48º [5]da Lei Processual Penal, nos artigo 66º da

2 https://julaw.co.ao/conheca-os-tribunais-de-internet-da-china.
O primeiro Tribunal de Internet do país foi criado em Hangzhou, centro de comércio eletrónico, em agosto de 2017. O segundo em setembro de 2018, enquanto autoridades reforçam as medidas para proteger transações comerciais, informações pessoais e propriedade intelectual online. O terceiro foi aberto em Guangzhou, no sul da China, em setembro de 2018.

3 CHINA. Interpretação da Lei 2015 nº.5, Interpretação sobre implementação da Lei Processual Civil, Pequim, 18Dez.2014. Disponível em: https://www.spp.gov.cn/spp/flfg/sfjs/201502/t20150205_90222.shtml. Acesso em: 05,Fev.2015.
第一百一十六条视听资料包括录音资料和影像资料。电子数据是指通过电子邮件、电子数据交换、网上聊天记录、博客、微博、手机短信、电子签名、域名等形成或者存储在电子介质中的信息。

4 Artigo 75º da Interpretação Judicial da Lei Processual Penal da República Popular da China(2021), emitida pelo Supremo Tribunal Popular da China, adotou uma definição semelhante. CHINA. Interpretação da Lei 2021 nº.1, Interpretação sobre implementação da Lei Processual Penal, Pequim, 7 Dez.2020.Disponível em: https://www.court.gov.cn/fabu-xiangqing-286491.html. Acesso em: 01mar.2021.
第七十五条行政机关在行政执法和查办案件过程中收集的物证、书证、视听资料、电子数据等证据材料，经法庭查证属实，且收集程序符合有关法律、行政法规规定的，可以作为定案的根据。

5 Tradução do Artigo 48º do Lei Processual Penal da República Popular da China：
São provas todos os materiais que podem ser utilizados para provar os factos de um caso. Asprovas incluem:
(1) provas físicas;
(2) provas documentais;
(3) depoimentos de testemunhas;
(4) declarações da vítima;

https://doi.org/10.51359/2448-2307.2022.253028

Lei Processual Civil[6], inclusivamente o artigo 33º da Lei Administrativa[7],também se reconhecem no mesmo sentido de que, mesmo a legislação nada se prescreve a sua definição legal exata, a

(5) confissão e defesa do suspeito ou arguido;
(6) opinião de peritos
(7) transcrições da investigação da cena do crime, exame, identificação e encenação da investigação; e (8) gravações audiovisuais e dados eletrônicos. As provas devem ser autenticadas antes de serem utilizadas como base para decidir um caso.(Tradução original feita pelo autor)
CHINA. Artigo 75º do Lei Processual Penalda República Popular da China ,2021, Lei Processual Penal, Pequim,01 Mar.2021. Disponível em: http://www.gov.cn/flfg/2012-03/17/content_2094354.htm. Acessoem:15Jan.2022.
第四十八条可以用于证明案件事实的材料，都是证据。证据包括：
(一）物证；
（二）书证；
（三）证人证言；
（四）被害人陈述；
（五）犯罪嫌疑人、被告人供述和辩解；
（六）鉴定意见；
（七）勘验、检查、辨认、侦查实验等笔录；
（八）视听资料、电子数据。证据必须经过查证属实，才能作为定案的根据。

6 CHINA. Artigo 66º daLei Processual Civil da República Popular da China,2022,Pequim.22 Mar,2022.Disponívelem： http://www.dffyw.com/faguixiazai/ssf/200311/20031109201543.htm.Acesso em 20Mar.2022.
As provas incluem:
(1) declaração de uma das partes;
(2) provas documentais;
(3) provas físicas;
(4) gravações audiovisuais;
(5) dados eletrônicos;
(6) depoimentos de testemunhas;
(7) opinião de peritos; e
(8) transcrições do inquérito. As provas devem ser autenticadas antes de serem utilizadas como base para a decisão de um facto.(Tradução original feita pelo autor)
第六十六条　证据包括：
（一）当事人的陈述；
（二）书证；
（三）物证；
（四）视听资料；
（五）电子数据；
（六）证人证言；
（七）鉴定意见；
（八）勘验笔录。

7 O órgão administrativo deve estabelecer e aperfeiçoar os sistemas pertinentes, a fim de promover a administração eletrônica pelo governo, anunciará as questões sob licença administrativa em página oficial de órgão administrativo, e facilitará a apresentação de pedidos de licenciamento administrativo por dados eletrônicos. O mesmo também partilha as informações relativas à licença administrativa com outros órgãos administrativos, de modo a aumentar a eficiência.(Tradução original feita pelo autor)CHINA.Artigo 33º daLei de Autorização Administrativa da República Popular da China,Pequim,
Disponível em: http://tfs.mofcom.gov.cn/article/ba/bg/201101/20110107347618.shtml.27Agu.2003. Acessoem:04Mar.2022.
《中华人民共和国行政许可法》第三十三条：
行政机关应当建立和完善有关制度，推行电子政务，在行政机关的网站上公布行政许可事项，方便申请人采取数据电文等方式提出行政许可申请；应当与其他行政机关共享有关行政许可信息，提高办事效率。.

https://doi.org/10.51359/2448-2307.2022.253028

admissibilidade dos chamados dados eletrônicos como prova. Aí estão previstos as informações e documentos eletrônicos que são considerados como os dados eletrônicos:

(1) Informações publicadas através de plataformas digitais tais como páginas de website, blogs, microblogs, capturas de tela do*Wechat* (JinLing, 2021). Compreendendo um serviço multiplataforma de mensagensinstantâneas desenvolvido pela *Tencent* na China, lançado originalmente em janeiro de 2011. É um dos maiores aplicativos de mensagens autônomas por usuários ativos mensais.

(2) Comunicações einformações em serviços de aplicação de rede, tais como *SMS*, correio eletrônico, mensagens instantâneas, e grupos de comunicação;

(3) Informações, incluindo informações de registro do utilizador, identidade, informações de autenticação, registros de comércio eletrônico, registros de comunicações e registros de acesso;

(4) Documentos eletrônicos, incluindo documentos escritos, imagens, registros de áudio e vídeo, certificados digitais, e programas informáticos;os depoimentos de testemunhas, os depoimentos de vítimas, os depoimentos e argumentos de suspeitos ou arguidos preservados em formato digital.

Na sequência de exemplificar as espécies dos dados eletrónicos, o Supremo Tribunal da China, para aperfeiçoar os equipamentos processuais e processos judiciais de tais novas espécies, emitiu em 16 de Junho de 2021, as Regras sobre os Processos *Online*para os Tribunais Populares, que entraram em vigor em 1 de agosto de 2021. As Regras contêm 39 artigos que abrangem a eficácia jurídica, os princípios fundamentais, o âmbito de aplicação e os pressupostos de aplicabilidade de processos *online*, fornecendo uma orientação concreta sobre o procedimento de processos *online*, incluindo a análise de autenticidade de prova eletrônica preservada pela TBC. Segundo tais regras, os tribunais, as partes e os demais participantes poderão contar com plataformas de processo eletrônico para realizar *online*, pela internet ou redes especializadas, para realizar totalmente ou parcialmente os atos processuais *online*, incluindo o ajuizamento, a mediação, a troca de provas, o inquérito, as audiências de julgamento e as notificações. Os atos praticados no âmbito de processos online e os atos praticados no âmbito de processos*offline* têm o mesmo efeito jurídico. O julgamento online é aplicável a todos os processos civis e administrativos. No que toca ao âmbito da aplicação dos processos, o julgamento online é aplicável a todos os processos civis e administrativos, mas só é aplicável aos processos criminais quando o caso seja julgado em processo sumário, no caso de comutação de pena e de concessão de liberdade

https://doi.org/10.51359/2448-2307.2022.253028

condicional, assim como os demais casos que forem considerados como não sendo adequados para o julgamento *offline* por outras razões específicas.

Em princípio, para conduzir um processo *online*, o tribunal deve sempre obter o consentimento das ambas das partes. No entanto, se apenas uma das partes optar pelo processo *online*, o tribunal pode ainda permitir que essa parte litigue *online* e a outra parte litigue pessoalmente, decidindo sobre a publicidade do julgamento *online*, uma vez que já tenha considerado o consentimento das partes, a idoneidade do caso, o impacto social consequente e as condições técnicas.Por sua vez, O julgamento *online* já não é admissível se todas as partes interessadas expressarem o seu desacordo, ou se uma das partes expressar desacordo, com razões plausíveis.

As Regras têm influência significante no sentido de que são permitidos os documentos eletrônicos sejam apreciados diretamente em processos após serem auditados pelos tribunais, a menos que os documentos originais sejam exigidos pelo tribunal em circunstâncias específicas (art.12º). As provas digitais preservadas por meio da TBC e tecnicamente verificadas como consistentes serão consideradas livres de adulteração após serem carregadas no bloco, a menos que haja prova contrária que seja suficiente para derrubar a presunção legal de inalterabilidade previamente estabelecida para as provas digitais preservadas pela TBC (art. 16º). Nos artigos 17º até 19º, as Regras de julgamento especificam ainda o método de autenticação das provas digitais preservadas pela TBC, incluindo a determinação se alguma prova eletrônica foi alterada antes de ser preservada no bloco pela TBC (artigos 17º-19º). É evidente que o Supremo Tribunal da China acredita que as provas digitais preservadas pela TBC trarão maior transparência, credibilidade, rastreabilidade e que promoverão maior eficiência para os processos online na China. Mundialmente, há mais jurisdições reagindo sobre essa tendência legislativa-operativa.

A Lei 269 do Senado de Vermont dos EUA, que especifica o valor das provas baseadas na TBC nos processos judiciais, permite que os tribunais confirmem diretamente a validade probatória da TBC sem ter homologação do Conservatório Federal ou Perícia Judicial. A Lei afirma no artigo 902º que um registro digital registrado eletronicamente em uma cadeia é autoautenticante se for acompanhado por uma declaração escrita de uma pessoa qualificada, feita sob juramento, declarando a qualificação da pessoa que faz tal certificação e a data e hora em que o registro entrou na cadeia de bloqueio; a data e hora em que o registro foi recebido pela TBC que o registro foi mantido na cadeia como uma atividade regularmente conduzida; e que o registro foi feito pela atividade regularmente conduzida como uma prática regular. Entretanto, a presunção não se estende à veracidade, validade ou estatuto legal do conteúdo do fato ou registro. Tal registro

https://doi.org/10.51359/2448-2307.2022.253028

digital é considerado como registro de atividade comercial regularmente conduzida, a menos que a fonte da informação, o método ou a circunstância careçam de confiabilidade. A lei também estabelece várias presunções legais: Em primeiro lugar, o registro é considerado autêntico. Além disso, a data e a hora do registro é a data e a hora em que o registro foi adicionado à aplicação da TBC. As pessoas duvidamque as provas preservadaspelas aplicaçõesda TBC podem contestar a autenticidade de tais registros,apresentando provas que demonstrem que o "fato presumido, registro, hora ou identidade não é autêntico como estabelecido na data adicionada à cadeia " (VERMONT, 2022).

Outro estado pioneiro como Washington, aprovou o Projeto de Lei do Senado 5638 em 26 de abril de 2019 e entrou em vigor em 28 de julho de 2019, sendo uma Lei "Relativa aoreconhecimento da validade da tecnologia de livros contábeis distribuídos"que define um registro eletrônico como "um registro gerado, comunicado, recebido ou preservado por meios eletrônicos para uso em um sistema de informação ou para transmissão de um sistema de informação para outro". Os registros eletrônicos não podem ter negadosseus efeitos legais, validade ou aplicabilidade com base no fato de serem gerados, comunicados, recebidos ou preservados por tecnologia de registro distribuído, mas reconheça comparativamente a sua eficácia legal como assinatura eletrônica e*smartcontract* (WASHINGTON, 2019).

A União Europeia tinha financiado o projeto *LOCARD* (ATHINA-EREVNITIKO, 2022), visando adquirir uma plataforma abrangente que permita a preservação de dados de provas digitais e assegure a apropriada cadeia da custódia adquiridano processo. A *LOCARD* empregará um "Ambiente de Execução Confiável" para garantir a privacidade e fornecer acesso a uma gama de provas digitais. O objetivo da *LOCARD* é fornecer uma plataforma holística para garantia da cadeia de custódia ao longo do fluxo de trabalho forense, uma plataforma distribuída confiável que permite a preservação de provas digitais pela TBC. Tal projeto finalizarápelo final de julho de 2022.Cada bloco da *LOCARD* pode definir independentemente suas próprias políticas de permissão e compartilhar seletivamente o acesso à evidência digital com outros nós quando considerado necessário e mediante autorização adequada através de políticas de granulaçãofina. A modularidade da *LOCARD* também permitirá que diversos atores adaptem a plataforma às suas necessidades e papéis específicos no fluxo de trabalho forense digital, desde a preparação e prontidão, até a coleta, análise e relatórios. A *LOCARD* terá um módulo de fonte de multidões para coletar relatórios de violações selecionadas, um rastreador para correlacionar comportamentos desviantes online,e ferramentas para investigadores que os auxiliará na coleta de provas *online* e *offline*.

https://doi.org/10.51359/2448-2307.2022.253028

Isto será alimentado por preservação imutável e um sistema de gerenciamento de identidade que protegerá a privacidade e tratará o acesso aos dados de prova, usando um ambiente de execução confiável. A tecnologia *Blockchain* não só garantirá que as informações sobre as provas não possam ser adulteradas, mas permitirá também a interoperabilidade sem a necessidade de confiar em terceiro.

Basicamente, as jurisdições comparadas forneceram três modalidade de respostas interessantes à admissibilidade de registros como provas baseadas no uso da TBC, em áreas como governança do mercado de valores mobiliários, regulamentação de conformidade de transações, compensação ou liquidação de transações: Certas jurisdições promulgaram novas leis que reconhecem o valor probatório das provas de TBC, outras emendaram leis probatórias existentes, enquanto outras emitiram declarações esclarecendo as leis existentes (POLLACO, 2020). À altura que os desenvolvimentos legislativos estabelecem a base para a admissibilidade de provas da TBC, na maioria das jurisdições os tribunais ainda não deram aplicação prática a estas disposições.Porque o sistema de prova eletrônica carece de infraestrutura informática, compreendendo um sistema partilhado pelos órgãos judiciais,visando a preservação de provas digitais e a consequente submissão à cadeia suportada pela TBC, podemos dizer assim, a maior barreira impeditiva não consiste no seio legislativo,nem por uma rutura cognitiva,mas sim por razão tecnológica. A dificuldade de construção de um sistema fiável de tramitação eletrônica do processo judicial, conjuntamente com as provas adquiridas é que decide a aplicabilidade eventual dasprovas oriundas da TBC. Os EUA., a China e a UE deram um passo mais a frente nesta corrida.

2 A PROVA DIGITAL CONVENCIONAL DIANTE PROVA DA TBC

2.1 A COMPARAÇÃO ENTRE PROVA DIGITAL CONVENCIONAL E PROVA DE TBC:

No fundo, a prova digital convencional não é*self-authenticating*como a prova oriunda da TBC, o qual permiteaos órgãos judiciais confiarem na sua autenticidade a todo o tempo. Para saber o porquê da mesma conveniência não acontecer com a prova digital convencional, importa-nos descortinar a questão daautenticidade da prova digital.Neste contexto, independentemente quão difusas as interpretações dadas pelas jurisdições diferentes, o significado de autenticidade de prova digital tem de se desdobrar minimamente emdois níveis:

1. A autenticidade do próprio veículo de prova digital: Compreende-se, por exemplo, a mesma célula com que o arguido mandou o SMS, ou seja, o computador portátil com que um criminoso pesquisou a consequência de crime antes de o cometer.

https://doi.org/10.51359/2448-2307.2022.253028

2. A autenticidade do fato contido na prova. Se pensarmos no exemplo do SMS enviado por arguido, para validar a mensagem como prova, o conteúdo abrangido no SMS tem que dizer respeito a situação apresentada no processo, se verifique com os restantes fatosjá apurados do processo, não podendoser um fato controverso, nem pode ser um fato falsificado.

No exemplo do SMS,a prova digital não está simplesmente preservada no celular, na verdade está preservada na memória do celular,quesãodoissujeitos individuais ecompletamente desmontáveis, alteráveis e separáveisdo veículo original—celular. Isto é,sãoseparáveis o meio de preservação da prova digital e a prova digital em si,sendo isto a maior diferença que distingue a prova digital das demais espécies de prova.Devido a divisibilidade entre o veículo de prova digital e a prova em si,nos é exigido uma dupla autenticação antes de lhes adotar:Por um lado, temos sempre que verificar a originalidade, complementaridade e identidade do próprio veículo onde se encontre preservado os dados eletrônicos, e por outro lado a originalidade, complementaridade e identidade dos dados transmitidos pelo veículo de prova digital, tais dados têm de ser originais, não podem sermodificados,apagados ou adicionados no decurso do processo.

A originalidade, complementaridade e identidade são justamente três momentos fundamentaisde autenticidade da prova digital, tais momentos estão intimamente interligados ese verificam mutuamente. Àpartida, a autenticidade doveículo de prova digital não garante necessariamente a autenticidade do conteúdo da prova digital, aqui não temos uma presunção lógica automaticamente probatória. Mas em certa medida,a autenticidade do veículo de prova digital é uma garantia externa daautenticidade da prova digital. A originalidade significa o estado original tanto da prova em si comodo veículo que a transmite. Enquanto aprecia o valor da prova digital, o juiz deve sempre averiguarseguindouma linha lógica de originalidade contínua, quer dizer, a originalidade dos três momentos consecutivos e inteiros, sendo eles:

a)A originalidade do veículo da prova (por via da qual a prova é transmitida, pode ser a memória do computador, por exemplo);

b)A originalidade da prova em si;

c) A originalidade do conteúdo da prova.

No caso de SMS enviado pelo celular do arguido, imaginemos que o arguido confessou nele detalhadamente o crime. A confissão deste está enquadrada com os indícios apurados. Mesmo assim,o juiz não pode valer a presente prova como válida, mas deve,antes de mais,elucidar setal telefone é a própria ferramenta mandante do*SMS*. Não bastaexistir a mesmamassagem confessória na máquina para constituira relatividade, porque a mensagem pode ter sidoinserida por umsegundo aparelhoatravés da instalação da memória do telefone original.Não sendo o verdadeiro gerador da

https://doi.org/10.51359/2448-2307.2022.253028

mensagem original,então está quebrada a cadeia de custódia. Sendo assim, a prova não é válida sem ter sido provada a identidade entre o veículo de prova (no caso em apreço, a memória de telefone) e a prova digital em si. A colheita há de ser completa, e, se no decurso da coleta da prova digital, o veículo transmitente da prova sofrer dano ou modificaçãoartificial, prejudicaria necessariamente a complementaridade da prova.

Como podemos observar, é o caráter de volatilidade da prova digital que nos é requeridadupla autenticação não autossuficiente e não *self-authenticating*da prova digital convencional. Isto já não aconteceria com as demais tipologias de prova, por exemplo,se tratamos de uma prova documental, basta averiguar a veracidade dodocumento por si só,estandoescusadode provar a relatividade entre documento eosfatos nele contidos, isso também não aconteceria com as provas da TBC.

As dificuldades resumidas *supra* acabam por afetar a taxa de admissibilidade da prova digital convencional nos processos judiciais, resultando em uma taxa de recolhimento significativamente mais baixa em comparação com as demais espécies de prova e dando azo ao fenómeno que fica conhecido como “desperdício da prova digital"(TIAN, 2021). O pioneiro do estudo de direito probatório chinês, ProfessorPinxinLiu (LIU, 2017)realizou um estudo, no qual analisou 8095 sentenças domésticas chinesas relacionadas com "provas digitais" e "dados eletrônicos", extraídas da página oficial de documentos judiciais da China[8], entre as quais constam 2702 sentenças cíveis, 5295 sentenças criminais e 98 sentenças administrativas. A análise estatística feita mostra que na grande maioria dos casos, o tribunal não se pronunciou explicitamente sobre a admissibilidade da prova eletrônica, correspondendo a 92,8% dos casos atendidos; apenas em um pequeno número de casos o tribunal se pronunciou explicitamente sobre a admissibilidade, representando 7,2%. Esta última situação pode ser tripartida em três tipos de posições: Totalmente admissível, parcialmente admissível e inadmissível (não considerada probatória), representando respetivamente 29,2%, 2,0% e 68,8% dos casos admitidos.

2.2 A CLASSIFICAÇÃO DA PROVA TBC:

É muito ambíguo sem distinguir claramente as tipologias da prova da TBC, segue procederemos a uma divisão conceitual dentro do seu chamamento geral,quetêm substancialmente 3 modalidade.

2.2.1 As provas digitais oriundas da TBC:

[8] Disponível em: http://wenshu.court.gov.cn/

https://doi.org/10.51359/2448-2307.2022.253028

Crimes realizados através de uma plataforma digital, tendo essência técnica descentralizada, estamos a dizer, possivelmente a prática de crime de sequestro, branqueamento de capital, fraude, crime de danos ao sistema informático, crime contra os dados pessoais de um cidadão etc.Como as condutas de prática são registradas na próprio plataforma, então todas as provas recolhidas são extraídas originalmente dessa mesma plataforma em formato TBC, e cabem nelas provar todo o processo de prática do crime:Por exemplo, o recorde de transferênciatransfronteiriça de X quantidade de*dogecoin* que equivale a YReais, operando com o intuito de colmatar o crime de branqueamento de capital, e tal transferência fosse viabilizada por plataforma *silkroad*.Esseregistro de transferência de propriedade virtual consiste um exemplo de provas eletrônicas oriundas da TBC.

2.2.2 As provas digitais preservadas pela TBC:

Por exemplo uma captura do ecrã de uma página no *Facebook* que contém conteúdo preservado pela aplicação de preservação judicial, não sofrerão mudanças mesmo se apágina for posteriormente eliminada, estando salvaguardado o conteúdo exato no momento em que foi preservado,vê-se garantida a sua originalidade porque se encontrapreservada pela TBC e tal modo garante a sua inalterabilidade.

2.2.3 As provas digitais autenticadas pela TBC:

As autenticações de provas digitais realizam-se através da verificação comparativa entre os valores de *hash*[9] dos respetivos dados informáticos anteriormente preservados e os dados posteriormente recolhidos, uma comparação permite-nos acertar a originalidade da prova mostrada na fase de investigação no tribunal.

Tabela 1 análise de autenticidade de prova após submetido à aplicação descentralizada baseada na TBC

	As provas digitais oriundas da TBC.	**As provas digitais preservadas pela TBC.**	**As provas digitais autenticadas pela TBC.**
Pontos comuns de garantia de autenticidade de prova	Verificação por valor de hash,carimbo de tempo, verificação por cálculo de bloco etc. São os principais meios anti modificativos por fatores humanos.		
Momento em que a prova é submetida a cadeia	Momento de formação da prova	Quando adquirir a prova ou depois da aquisição	Após adquirir a prova

9 *Hash* nada mais é que uma sequência de dados de comprimento fixo (ou seja, de mesmo número de caracteres) obtida por meio de tratamento de determinado conjunto de informações a um algoritmo (a grosso modo, sequência de instruções que determinará a conversão das informações em um hash).

https://doi.org/10.51359/2448-2307.2022.253028

Momentos antimodificativos	A submissão da prova à cadeia e o efeito de garantia de autenticidade	Uma garantia de autenticidade universal que cobre as fases inteiras	Uma garantia de autenticidade total ou parcial de provas submetidas a cadeia	Uma garantia de autenticidade apenas de certas fases durante o processo

Como todos os dados eletrônicossupra-mencionados são passíveis de submissão e preservação individual em plataformas digitais, a mera diferença entre o meio de geração, o método de preservação, e a maneira de autenticação diferencia o valor dos dados eletrônicos em causa, uma vez que as plataformas suportadas pela TBC garantem efetivamente a originalidade da prova digital, a qual é momentaneamente verificável

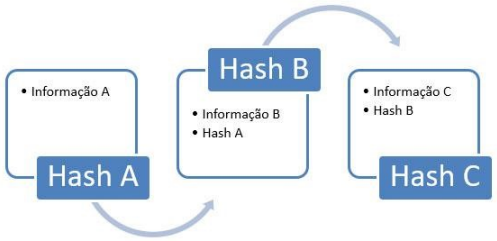
3 O MECANISMO DE GARANTIA DA VERACIDADE DA TBC

A *Blockchain* foi descrita pela primeira vez num artigo publicado por um indivíduo (ou um grupo de indivíduos) anônimo,usando o pseudônimo*SatoshiNakamoto*. A popularidade desta tecnologia liga-se, em grande parte, com a crise financeira mundial de 2008 na qual grandes operadores financeiros ficaram à beira da falência. A blockchain caracteriza-se descentralização, que não sóproporciona confiança nas transações, mas também enfraquece o tradicional mecanismo centralizado de confiança no Estado ou organizações intermediárias. Desde a sua origem, a blockchain tem sido considerada como a substituição de um centro de confiança tradicional com a característica de estar "desprovida de confiança" (FAIRFIELD, 2014, p. 36) Visto muitas vezes como uma “máquina de confiança” (PRIMAVERA; MANNAN; REIJERS, 2020, p. 17), o desenvolvimento contínuo e a aplicação generalizada da tecnologia blockchain têm fortificado tal tendência. A blockchain estendeu-se da indústria financeira para os demais setores comerciais e até começou a desafiar a estrutura de confiança centrada no poder público.A blockchain é, de fato, uma conta-livro de distribuição aberta. Funciona emfeixe (*cluster*) de computadores (*P2P*), do qual qualquer pessoa pode participar e está aberto ao público. Ao importar o mecanismo de prova de trabalho (*PoW –Proofofwork*), a blockchain pode proteger os dados contra a adulteração arbitrária (NOGUCHI, 2018, p. 13). O mecanismo *PoW* não pode ser compreendido separadamente do algoritmo de *hash*, *digests*ou*checksums*, que são produtos de algoritmos capazes de reduzir grandes quantidades de dados a uma sequência menor, usualmente de tamanho determinado, alcançada de modo unidirecional. O funcionamento se baseia nas funções de mão única (*hash*), carimbo do tempo, assinatura digital, rede descentralizada *peer-to-peer* e mecanismo de geração de um novo bloco. A primeira transação tem o respectivo valor *hash*calculado; em seguida, a próxima transação

https://doi.org/10.51359/2448-2307.2022.253028

em conjunto com o *hash* da transação anterior também tem seu valor *hash* calculado e este processo continua até a última transação. Adicionado ao *hash* das transações, é calculado o valor do novo bloco e do bloco anterior. Desta forma o bloco anterior está ligado ao novo bloco, e assim sucessivamente (LUCENA; HENRIQUES, 2016)

Tabela2*modus operandi* de transação de informaçãoporvalor *hash*



O "valor *hash*", tem as duas características seguintes:

Primeiramente, se mudar os dados originais, obterá um valor *hash*completamente diferente. Em segundo lugar, mesmo que o valor *hash* seja conhecido, os valores originais do hash não podem ser deduzidos por uma regra aritmética (NOGUCHI, 2018, p. 19).A preservação pela TBC funciona como um banco de dados, onde são preservadas transações em caráter permanente. Cada bloco de informações possui referência ao bloco anterior (daí o termo “cadeia de blocos”) e, por isso, nenhum bloco anterior pode ser alterado sem que modifiquem os blocos posteriores: primeiramente, é essencial mostrar o seu arquivo (qualquer tipo) ao website que preste o serviço, e este converterá o conteúdo do ficheiro em um bloco encriptado ou valor *hash*. O algoritmo pode criar um bloco ou uma cadeia encriptada para representar os dados. Não é possívelexistir dois resumos exatamente idênticos,a não ser que sejam calculados a partir do mesmo documento.

Portanto, o valor *hash* pode então representar precisamente o conteúdo do documento. Depois de inserido o valor *hash* criptografado do documento em uma transação e o registo da transação em um bloco, o carimbo de tempo da blockchain passa a ser o carimbo de tempo do documento, para que o conteúdo do documento seja codificado na blockchain. Quando o mesmo arquivo é submetido mais uma vez, o valor *hash* pode ser criado da mesma forma para verificar se os dois arquivos são completamente consistentes. Por conseguinte, se forem feitas quaisquer alterações ao ficheiro, o valor *hash*recentemente obtido não corresponderá ao valor incorporado na blockchain nessa altura. É assim que o sistema completa o documento no processo de verificação (SWAM, 2018, p. 104).

Como há vários algoritmos, há várias estruturas de *hash* conhecidas. Para termos uma noção mais concreta do assunto, falamos de *hashes* SHA-1 (uma das muitas espécies

https://doi.org/10.51359/2448-2307.2022.253028

de *hash* disponíveis) a partir de textos aleatórios que escritos na página destinada a este fim. O algoritmo de *hash*criptografado é utilizado para provar a integridade de um arquivo, mas o problema é que este não é conhecido quando o arquivo foi criado até a blockchain fornecer um mecanismo para adicionar carimbos de tempo de segurança. O método fornece carimbos de tempo e dados de uma forma imutável e, ao mesmo tempo, assegura que o conteúdo dos dados não é divulgado.

Tabela 3 exemplos de *Hash* SHA-1

Texto digitado por mim	***Hash* SHA-1 correspondente**
CPC	eba32f8c03f6f2ed98d68a24b024bf9c98e8074e
CPCa	ae3a530e11a8ae6f5f708f21fa2d1ff3614ffbb6
Socorro alguém me explique o que é esse *blockchain*	c6e85ba73d25c1f74edec41d26c97513d8cf7afc

O *hash* tem sempre o mesmo número de caracteres (ainda que a informação original tenha extensões muito diferentes) e pode se alterar completamente com uma simples letrinha a mais adicionada na informação original. Basta comparar a linha "CPC" com a "CPCa" para perceberque se produziram *hashes* totalmente distintos.

Para cada bloco é produzido um *hash*, e aqui está a vinculação – no bloco seguinte é armazenada a "Informação B" e também o *hash* do bloco anterior ("*hash* A"). A partir desse conjunto é extraído o *hash* desse segundo bloco ("*hash* B") e assim por diante.

Mínimas alterações na informação original, como visto na tabela acima, modificam completamente o *hash*. Assim, se alguém tentar adulterar a informação armazenada no bloco A, isso irá modificar o *hash* A, que é gravado no bloco B, de maneira que toda a cadeia de informações nos blocos subsequentes se tornará inconsistente.

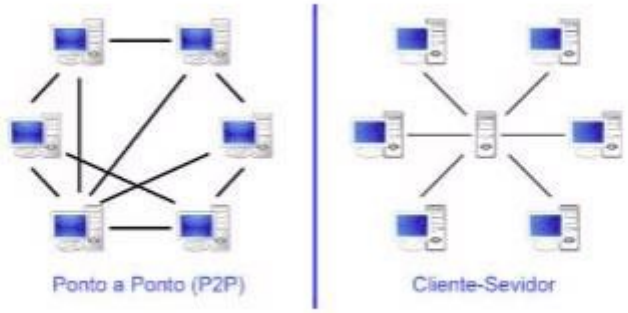
Esse não é o único fator de segurança da blockchain. Além da formação de cadeia de blocos, a informaçãoé armazenada de maneira descentralizada em várias máquinas ao mesmo tempo. Não existe um servidor que possa ser desligado ou de alguma forma adulterado. Trata-se, ao invés, de uma rede "ponto a ponto" (ou rede *P2P*).

Isso quer dizer que todos os computadores conectados nessa rede compartilham tarefas, com iguais privilégios e influência – em vez de uma influência dominante de um servidor. Se um dos computadores (chamados de "nós") é retirado da rede *P2P*, esta continuará funcionando normalmente, porque há cópias das informações nos demais "nós" da rede. Se um novo

https://doi.org/10.51359/2448-2307.2022.253028

computador (ou “nó”) se liga à rede, os “nós” originais compartilharão as informações para que esse novo membro da rede também as armazene.O diagrama abaixo ilustra a diferença entre uma rede cliente-servidor (como é o caso de redes sociais ou páginas da internet) e uma rede *P2P*:

Tabela4 A diferença entre uma rede cliente-servidor e uma rede *P2P*



Deste modo, a prova digital convencional é alterável e restaurável, as modificações realizadas em provas digitais não deixarão necessariamente registro de operações inapagáveis, sendo,por isso, possível a modificação integral da cadeira da prova sob intervenção de meio técnico. Por seu turno, como acabamos de ver, a prova digital preservada pela tecnologia blockchain, dado como um novo estado de existência de prova digital, é relativamente inalterável, salvo no caso em que ocorra um ataque de 51% contra uma rede em funcionamento (SAYEED; MARCO-GISBERT, 2019). Por isso esta beneficiará de uma presunção de autenticidade inerente assegurada pela essência da tecnologia per si (YLI-HUUMO; KO; CHOI; PARK; SMOLANDER, 2016, p. 77). Isto é, uma vez em que a respetiva prova digital é preservada pela TBC, é assegurada para sempre a sua autenticidade e tal prova digital estará imuneaposteriores alterações ou falsificaçõeshumanas.Esta capacidade de "congelar" dados, prevenindo a sua alteração, associada ao compartilhamento das informações, permitiram a aplicação da TBC em criptomoedas, gestão conjunta de dados, garantia de integridade e anterioridade de dados.

4 UM CASO PRÀTICO DA APLICAÇÃO JUDICIAL DA TBC

Foi proferida em 2018 a primeira sentença cuja preservação de prova é sustentada pela aplicação judicial da tecnologia de blockchain, quando o Tribunal de Internet de Hangzhoureconheceu *ex-novo* o estatutolegal de prova digital preservada e apresentada pela tecnologia blockchain. Na decisão, datada de 27 de junho de 2018, recaiu sobre o caso*HangzhouHuataiYimeiCulture Media* Co., Ltd. ("Huatai") v. Shenzhen

https://doi.org/10.51359/2448-2307.2022.253028

DaotongTechnologyDevelopment Co., Ltd. ("Daotong").[10]Trata-se de um caso deviolação de direitos de autor. A sociedade por quotasHuatai, na qualidade de autor de ação alegousertitular dos direitos de autor de um artigo ("artigo A") e que a Daotong publicou o artigo A na sua página oficial sem ter autorização prévia daquele, infringindo, assim, os direitos da Huatai.

Para obter as provas da alegada infração, o autor da ação utilizou-sedos recursos da *Baoquan Net*, uma empresa doméstica fundada em 2016 que foi pioneira nos serviços de preservação de dados baseados na TBC e geradora de uma plataforma dedicada à conservação de prova digital. Desempenhando a sua função na qualidade de terceiro imparcial,a*Baoquan Net* utilizava um programa de código aberto concebido pelo Google que se chama Puppeteer para fazer capturas de ecrã da página da Datong e, mais tarde, utilizava outra ferramenta de transferência de dados de código aberto chamada Curl e obtinha os códigos originais da página da Datong. Após adquirir, do modo acabado de descrever, a captura da página onde constava o artigo copiado e os códigos originais da mesma página, equiparava-as com o histórico das operações efetuadas. Registrava,aliás,a hora concreta em que o registro acima referido era consultado e extraído.

Finalmente, a Baoquan submetia todas as informaçõesem um arquivo comprimido ao sistema FACTOM[11]e ao Bitcoin Blockchain a fim de proceder à devida preservação comparável. No processo, a *Baoquan* transferiu o localizador uniforme de recursos (URL)da páginapara o tribunal, de modo aelucidar os factos perante este.

Considerando oraciocínio apresentado, calcula-se e comparam-se os valores de *hash* SHA25 dos dados contidos no ficheiro comprimido, podendo-se provar a autenticidade e integridade da prova adquirida, uma vez que os valores de *hash*são iguais entre o que foi submetido à plataforma FACTOM e o quefora preservado no Bitcoin Blockchain. Como os valores de *hash* são irrepetíveis e irreversíveis quando se representa um mesmo objeto, é evidente que, na hora em que os dados foram recolhidos, as matérias (entre as quais a cópia do Artigo A) eram exatamente como se mostrava na captura de tela.

O Tribunal da Internet de Hangzhouacedeu à plataforma-preservadora da *Baoquan Net*através da conta dada pelo autor da açãoe baixouo ficheiro que continha os dados comprovativos da violação do direito de autor:A captura de tela preservada mostrou que um Artigo semelhante ao Artigo A foi publicado na página.Os conteúdos dos dois artigos referidos eram

[10][Hangzhou HuataiYimei Culture Media Co., Ltd. v. Shenzhen Daotong Technology Development Co., Ltd.] (Hangzhou Internet Ct. 0192 Min Chu.No.81, 2018) (China).

[11] O Factom Blockchain é um protocolo de publicação descentralizada para a construção de sistemas de registos que são imutáveis e verificáveis de forma independente. Ele permite o armazenamento seguro de provas digitais para a proveniência dos dados e soluções de integridade, sem revelar dados privados ou exigir intermediários confiáveis. Informações disponíveis em: https://www.factom.com.

https://doi.org/10.51359/2448-2307.2022.253028

extremamente idênticos. Através da consulta dos códigos-fonte de operação desta página chegou-se à conclusão de que a Daotong era a entidade a título de quem a página estavaregistada e era também a verdadeira titular da página objetodessa violação dos direitos de autor.

A fim de determinar a validade e a força das provas digitais obtidas e preservadas pela TBC, o Tribunal invocou o artigo 8º da Lei de Assinatura Eletrônica da China (Emenda de 2019), que estabelece: "Os seguintes fatores devem ser tidos em consideração ao fazer o exame da veracidade de qualquer dado quesirva como prova:

1. A fiabilidade dos métodos de criação, armazenamento ou transmissão de mensagens de dados;
2. A fiabilidade dos métodos de manutençãoda integralidade do conteúdo;
3. A fiabilidade dos métodos de identificaçãodo remetente;
4. Outros fatores relevantes.

Por conseguinte, o Tribunal examinou três questões principais:

4.1 A NEUTRALIDADE E QUALIFICAÇÕES DA PLATAFORMA DE TERCEIROS:

Após um inquérito, o Tribunal considerou que a *Baoquan Net* estava qualificada para realizar as conservações de provas relevantes, considerando as certificações relevantes a nível nacional com as quais tinha sido equipada, incluindo a Certificação de Segurança de Nível 1 do Website emitida conjuntamente pelo Terceiro Instituto de Investigação do Ministério da Segurança Pública e pelo Centro Nacional de Supervisão e Inspeção da Qualidade dos Produtos de Segurança de Redes e Sistemas de Informação, e a prova de registo para o terceiro nível de proteção de segurança do sistema de informação emitida pelo Ministério da Segurança Pública. O Tribunal também considerou a Baoquan Net como um verdadeiro terceiro imparcial, dado que as empresas bem como os respectivos sócios/acionistas não são relacionadas entre si e, por isso, gozam de imparcialidade e neutralidade.

4.2 A FIABILIDADE DOS MEIOS TÉCNICOS ENVOLVIDOS PARA A OBTENÇÃO DE PROVASDIGITAIS:

O Tribunal concluiu que a *Baoquan Net* foi implantada na*AlibabaCloud*, uma plataforma universal de nuvem que podia, em circunstâncias normais, garantir que o servidor não fosse comprometido por vírus de software. Além disso, a Baoquan Net possuía as certificações de segurança relevantes para que os seus ambientes fossem considerados seguros para o armazenamento de dados eletrônicos, salvo que existissem provas em contrário. Além disso, o Tribunal defendeu a credibilidade dos meios técnicos envolvidos – nomeadamente, oPuppeteer e

https://doi.org/10.51359/2448-2307.2022.253028

o Curl,considerandonão só a sua natureza aberta e o funcionamento automático dos seus procedimentos pré-definidos, sendo, assim, considerados como "menos suscetíveis de serem adulterados", mas também o relatório de autenticação emitido pela instituição judicial Qianmai Centro.

4.3 A INTEGRIDADE DA PRESERVAÇÃO DE PROVAS DIGITAIS NA BLOCKCHAIN

Como primeiro passo, o Tribunal reconheceu que a blockchain tem a característica de "ser difícil de manipular ou de apagar", sendo que, por isso, "a blockchain é um método fiável para manter a integridade do conteúdo que lhe é carregado".

Adicionalmente, o tribunal buscou responder a duas questões:

a) Se os dados eletrônicos em questão foram efetivamente carregados;

b) Se os dados eletrônicos carregados eram os dados relevantes para o processo.

Para a pergunta (a), o Tribunal pesquisou o valor do *hash* e a altura do bloco fornecidos por Huatai na FACTOM e depois revisou o conteúdo armazenado no *hash*da transação e o seu tempo de geração. Comparado com o tempo registrado nos registros de chamadas relativos à utilização do "Puppeteer" e "Curl" para adquirir as imagens e códigos-fonte acima mencionados, o Tribunal considerou que o tempo de carregamento do conteúdo era razoável e o tempo de geração da altura do bloco cumpriu as lógicas de tempo entre o tempo de geração do registro de chamadas e as regras de embalagem do FACTOM. Depois, de acordo com o valor de *hash*da altura do bloco ancorado à cadeia de blocos Bitcoin, o Tribunal considerou que o valor de *hash* do conteúdo localizado no nó correspondente da cadeia de blocos Bitcoin era consistente com o valor de *hash* do conteúdo armazenado na cadeia de blocos FACTOM. Portanto, o Tribunal considerou que a *Baoquan Net* tinha efetivamente carregado as provas digitais tanto para o FACTOM blockchain como para o Bitcoin blockchain.

Para responder à pergunta (b), o Tribunal calculou o valor de *hash* das capturas de tela, códigos-fonte e registros de chamadas descarregados da *Baoquan Net*, e comparou-o com o valor de *hash* da blockchain eletrônica.

Tendo em conta todas essas questões, o Tribunal determinou que os dados eletrônicos em causa foram efetivamente carregados em FACTOM e Bitcoin, e que foram preservados na integridade sem qualquer modificação.

Este é o primeiro caso na China em que se procedeu à determinaçãodo efeito legal da prova digital armazenada pela blockchain, fornecendo um método de análise e admissão deste novo tipo de prova eletrônica, detalhando os fatores de consideração e clarificando os critérios de

https://doi.org/10.51359/2448-2307.2022.253028

julgamento. O tribunal chinês que apreciou o caso forneceu, portanto, interpretações sem precedentes sobre a TBC, os princípios técnicos relevantes, e os métodos que podem ser utilizadospara avaliar a sua validade. Esta decisão está carregadade um elevado valor de referência para casos semelhantes que venham a surgir no futuro.

Em particular, o Tribunal salientou que deve ser mantido um ponto de vista neutro e independente em relação às provas da TBC.O Tribunal entendeu que, para os dados eletrônicos que sejam preservados pela adoção da blockchain ou outros meios técnicos, a análise deve ser conduzida com uma atitude aberta e neutra, caso a caso. Não devemos excluir nem aumentar a norma de admissão apenas porque a tecnologia, como a própria blockchain,é complicada, nem baixar anorma de admissão porque a tecnologia é difícil de manipular ou de apagar.

5 AVALIAÇÃO DE PROVAS PRESERVADAS PELA BLOCKCHAIN

A fim de assegurar a autenticidade e a integridade das provas preservadas na blockchain, é necessário implementar métodos e procedimentos de avaliação específicos (JINYOU, 2001). Alguns autores consideram a análise comparativa abrangente, o reconhecimento ea autenticação, como métodos principais de avaliação de provas. De acordo com as características dos dados eletrônicos, iremos abordar detalhadamente a questão-chave da autenticação. Se houver alguma dúvida sobre a veracidade de dados eletrônicos, estes devem ser autenticados.

Segundo artigo 93º de Interpretação do Supremo Tribunal Popular sobre a Aplicação da Lei de Processo Penal da República Popular da China,se houver alguma dúvida sobre as provas digitais, estas devem ser avaliadas ou verificadas.O artigo 11, parágrafo 3, das Disposições do Supremo Tribunal Popular sobre Certas Questões em Processos Judiciais na Internet estipula que: "As partes podem solicitar as opiniões de pessoas com conhecimentos especializados sobre questões técnicas de dados eletrônicos. Os tribunais na Internet podem, mediante requerimento das partes ou de acordo com a sua competência, levar a cabo a identificação da autenticidade dos dados eletrônicos ou investigar outras provas relevantes para verificação".

No primeiro julgamento sobre a preservação da blockchain, o Tribunal de Internet de Hangzhou fez uma apreciação judicial, com apoio de profissionais relevantes a fim de assegurar a fiabilidade da tecnologia. *Qianmai*, um Instituto de Autenticação confirmou a tecnicidade da utilização de programas paragestão de provas, por exemplo as capturas de tela da página oficial de Datong, e adquiriu o código-fonte. Por conseguinte, na ausência de provas em contrário, o tribunal considerou que o " *Baoquan*" era fiável na geração e preservação de mensagens de dados através

https://doi.org/10.51359/2448-2307.2022.253028

da utilização da versão pública do *crawler*de código aberto do Google para executar o domínio de resolução de nomes na página de destino.

5.1 UMA ANÁLISE COMPARATIVA E MÉTODOS DE VERIFICAÇÃO

Até à data, a implementação daTBCnos tribunais chineses não reflete muito o seu DNA revolucionário inato, como frequentemente se verifica nasblockchain públicas. A escolha da arquitetura técnica de blockchain (nomeadamente, um sistema relativamente fechado e mais pequeno) minimiza largamente o debate sobre descentralização, anarquismo, soberania digital, privacidade, etc. Em vez disso, a TBC está a ser utilizada de uma forma que não é contrária aos sistemas legais convencionais, mas está configurada para operar em parceria com eles. A contribuição mais proeminente da TBC tem sido a melhoria da eficiência judicial como um meio auxiliar de autenticação. Por outras palavras, a prova digital da TBC, por todos os seus méritos, não ultrapassou as fronteiras definidas em termos de lei e tecnologia; ou seja, tem de cumprir os requisitos legais para a prova em geral.A China limita prudentemente as implementações judiciais da TBC a alguns campos, nomeadamente o da prova de que os dados eletrônicos não foram adulterados depois de terem sido "encadeados". Contudo, a informação encadeada é, na melhor das hipóteses, uma parte integrante dos fatos de um caso e ainda precisa ser interpretada mais detalhadamente. Portanto, a fim de apresentar uma narrativa mais completa, a intervenção humana é inevitável. As preocupações permanecem no que respeita às lacunas no tempo entre as ocorrências específicas e quando foi "encadeada".

Isto não se deve necessariamente a uma desvantagem da TBC *per se*, mas está antes sujeito à popularidade da digitalização nesta fase. A China é um dos poucos países que gozam de facilidade técnica na cena da integração da TBC e do sistema judicial, e estabeleceu mais plataformas de TBC judicial do que qualquer outro país. No entanto, em comparação com o rápido desenvolvimento da TBC em geral, tais implementações judiciais ainda se encontram nas fases iniciais de utilização e estão principalmente preocupadas com a característica de resistência à manipulação da TBC. Mesmo como uma mera aplicação em fase inicial, quando se insere no contexto da vastidão da China ou do Brasil, a TBC já teve um impacto positivo e substancial na melhoria da eficiência do sistema judicial. Com o desenvolvimento futuroda digitalização e tecnologia (por exemplo, internet das coisas, 5G), muito mais pessoas estarão ligadas e mais comunicações e transações terão lugar diretamente "no bloco". Quando o fosso entre o que acontece fora e o que acontece dentro do bloco finalmente desaparecer, a TBC poderá desempenhar um papel mais substancial no sistema judiciário. Como salientou Kevin Werbach

https://doi.org/10.51359/2448-2307.2022.253028

(2018, p. 487), “Reguladores, legisladores e tribunais podem tomar a iniciativa de criar tanto espaços claros como explícitos para a experimentação", e "para encontrar um campo comum”. Ao permanecerem juntos desta forma, a integração sustentável do direito e da TBC pode realmente realizar-se, e servirá os interesses da sociedade como um todo.

5.2 COMENTÁRIOS E CRÍTICAS AO CASO

Aparentemente, a autenticidade dos dados eletrônicos é efetivamente garantida. Em primeiro lugar, graças à introdução do mecanismo *PoW* a preservação por blockchain pode proteger os dados contra arbitrariedades e alterações por algoritmo de *hash*. O carimbo de tempo é dado quando são geradas provas, e a integridade dos dados é verificada pela comparação dos valores de *hash* quando as provas eletrônicas são armazenadas. Durante a transmissão, a tecnologia de encriptação assimétrica é utilizada para encriptar as provas eletrônicas a fim de assegurar a segurança de transmissão, que garante plenamente a autenticidade das provas.

Em segundo lugar, a segurança do sistema de preservação é efetivamente salvaguardada (JIE, 2019, p.17).O armazenamento distribuído em cadeia por blocos determina que cada nó pode preservar os dados simultaneamente, daí que não se pode validamente modificar os dados da conta com um único nó. É também muito difícil para os hackers de rede atacarem todos os “nós” na blockchain ao mesmo tempo. Os danos em qualquer um dos “blocos” não interferem na preservação de dados na blockchain, pelo que os dados preservados em*hash* e blockchain podem reduzir efetivamente a capacidade de armazenamento de dados, e satisfazer também mais eficazmente os requisitos na era da*BigData*.

Em terceiro lugar,o sistema em si protege eficazmente o conteúdo dos dados da divulgação. O registro de um valor *hash*através da blockchain pode ser a prova de que o arquivo existia em um determinado momento. Além disso, como o valor do*hash* é registrado, o conteúdo não será exposto, o que pode ser considerado um método de ‘prova de zero conhecimento’ (MORAIS, 2019, p.76). Assim, a ‘prova de zero-conhecimento’ é uma forma de um certificador provar que possui a informação sem o fornecer à outra parte (NOGUCHI, 2018, p.120).

Com o surgimento da TBC, encontramos um método revolucionário de transação-preservação da prova digital. Há cada vez mais casos de acolhimento de provas digitais desse gênero (MINISTRY OF JUSTICE, 2017). A aplicação jurídica da blockchain não se cinge meramente à função do método de preservação de prova digital, mas também se conecta com a construção global do sistema de Tribunal Inteligente.

https://doi.org/10.51359/2448-2307.2022.253028

Apesar de tudo, no caso em apreço, o Tribunal não teve a oportunidade de tocar na essência da prova TBC, e algumas questões-chave ficaram por responder. Em primeiro lugar, no que diz respeito à questão acima referida da neutralidade da plataforma de terceiros, o âmbito independente das empresas e dos diferentes acionistas parece que não é suficiente para tirar a conclusão de neutralidade. A plataforma de terceiros *Baoquan Net*（*Baoquan* é a escrita de 保全, signifique providencia cautelarem Chinês）, afinal de contas, é uma empresa com fins lucrativos cujo principal meio de obter lucros é preservar as provas digitais. Nestas circunstâncias, resta saber como deve ser avaliada a neutralidade do terceiro. Nenhuma outra instrução foi dada pelo Tribunal. Isto não só porque o arguido não levantou quaisquer objeções que pudessem levar a mais explicações, mas também porque não havia normas ou critérios obrigatórios específicos já estabelecidos por lei.

Além disso, não é claro em que qualidade terceiros como a*Baoquan Net*estão participando no processo. Atualmente, o sistema processual chinês não esclarece o estatuto legal de terceiros como a *Baoquan Net* no processo. Tomemos como exemplo a atual Lei de Processo Civil da China. Entre os principais participantes no processo estipulados, por exemplo, as partes, os representantes dos litigantes e os inspetores, parece apropriado classificar uma terceira parte como a*Baoquan Net*como estando na posição de testemunha, que utilizou a TBC para incorporar, preservar, e transmitir as provas envolvidas no caso. Também neste caso, a neutralidade do terceiro deve ser avaliada, mas não existe uma lei específica que regule a respetiva matéria no ordenamento jurídico chinês, nem nos demais países referidos no presente artigo. Quanto à credibilidade dos meios técnicos envolvidos na obtenção de provas eletrônicas, a adoção da prova TBC pelo Tribunal não foi meramente pelo seu esmagador mérito, mas foi o resultado de considerações multifatoriais abrangentes. Por exemplo, o ambiente digital foi considerado seguro com base na tecnologia de nuvem fornecida pelo Grupo*Alibaba*[12].

*Puppeteer*e *Curl* foram tomados como fontes de dados eletrônicos credíveis; devido às suas características específicas, como o Tribunal observou que "estão abertos a todos, qualquer pessoa pode utilizá-los, e o processo de operação é automaticamente concluído desde que antecipadamente programado. Além disso, tendo em consideração o relatório fornecido pela instituição de autenticação judicial e a comparação de valores de *hash*, as provas carregadas em cadeias de bloco foram consideradas como autênticas.No período não negligenciável entre a recolha e o carregamento de provas (para o FACTOM ou Bitcoin), haverá sempre um intervalo de

[12] *Aliyun* é uma subsidiária do *Grupo Alibaba* voltada para o mercado de computação em nuvem.

https://doi.org/10.51359/2448-2307.2022.253028

tempo curto, durante o qual os dados podem ser adulterados. O desafio reside em descobrir como o trabalho conduzido por um terceiro centralizado pode ser tornado mais digno de confiança.

6 CONSIDERAÇÕES FINAIS

Desde a sua origem em 2008, a blockchain expandiu-se a partir setor financeiro para outras áreas. Sendo uma tecnologia descentralizada, parece ter um conflito essencial com a estrutura tradicional de confiança centralizada no poder estatal. Contudo, tal conflito técnico não significa necessariamente um conflito na realização da justiça. Isto é claramente demonstrado na aplicação da blockchain em sede de geração e preservação de provas digitais, que se trata, por sua vez, de uma fusão entre a tecnologia descentralizada e a estrutura tradicional alicerçada segundo o método centralizado.

A digitalização de provas consiste numa tendência irrefutável,quer no seio de contenciosos administrativos,quer quanto aos processos civis, bem assim no âmbito de investigações criminais, especialmente no que toca ao direito penal econômico, em que a prova digital trazida pela TBC será uma*conditio sine qua non* de descoberta da verdade material de determinados tipos de crime, como por exemplo o branqueamento de capitais transfronteiriço realizado mediante transação de criptomoeda. A aplicação da TBC nas áreas cruzadas com a ciência jurídico-processual colmatará as deficiências das atuais regras em matéria de provas e terá um impacto na estrutura de credibilidade dos tribunais, das instituições forenses, e das testemunhas especializadas.

É certo que, embora a ideia de tecnocracia deve conduzir a mudanças nas instituições jurídicas competentes, o papel da ciência e da tecnologia na governança social não significa que o papel do Estado é obliterado, mas indica uma integração de tecnocracia e governança democrática: Por exemplo, o sistema eletrônico de provas na era da blockchain. A essência da credibilidade da plataforma consiste na sua independência. Porém, há preocupações razoáveis que podem surgir com as facilidades quanto a este aspeto, nos casos em que as provas foram preservadas por plataformas criadas e mantidas por empresas privadas. E é neste sentido que a China promoveu a informatização do Tribunal de Internet e a sua própria plataforma de preservação de prova digital baseada na TBC, possibilitando deste modo a combinação e a compatibilidade do sistema atual de prova. Nessa medida, a fronteira entre a prova digital e os dados eletrônicos vê-se paulatinamente ofuscada e, consequentemente, surgirão cada vez mais subcategorias na esfera conceitual da prova digital, especialmente no que concerne à prova digital baseada da TBC, campo no qual formar-se-á eventualmente uma tipologia de prova legal misnova e verdadeiramente emergente.

https://doi.org/10.51359/2448-2307.2022.253028

REFERÊNCIAS

ATHINA-EREVNITIKO KENTRO. KAINOTOMIAS STIS TECHNOLOGIES TIS PLIROFORIAS, TON EPIKOINONION KAI TIS GNOSIS. Law ful evidence collecting and continuity plat form development. **CORDIS Revista Research**. Disponível em: https://cordis.europa.eu/project/id/832735/&https://locard.eu/project.reporting. Acesso em: 2 maio 2022.

BLOCKCHAIN, Noguchi Y. Revolution: **The Emergence of Distributed Self-Disciplined Society**. 2018. p. 120.

BLOCKCHAIN, Swan M. **New Economic Blueprint and Guide**. Beijing: New Star Press, 2018. p. 104.

EOGHAN,Casey. **Digital Evidence and Computer Crime**. London: Academic Press, 2000. 199 p.

FAIRFIELD, Joshua A.T. Smart Contracts, Bitcoin Bots, and Consumer Protection. **Washing and Lee Law Review Online**, v. 71, p. 35-50. Disponível em: https://scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss2/3. Acesso em: 20 abr. 2022.

FILIPPI, Primavera de; MANNAN, Morshed ; REIJERS, Wessel. **Blockchain as a confidence machine**: The problem of trust & challenges of governance, Technology in Society, 2020.

JINYOU, L. **Evidence Law**. 1. ed. China: University of Political Science and Law Press; 2001. p. 481-502.

LI, Jie. Research on the present situation of internet court and block chain evidence collection. **Journal Sichuan Vocational Technology College**, v. 3, 2019.

LIN, Jing. WeChat, Analysis of the Current Situation and Development of Tencent WeChat. **Advances in Economics, Business and Management Research**, Malibu. Disponível em: https://www.atlantis-press.com/proceedings/icemci-21/125965976. Acesso em: 12 abr. 2022.

LIU, Pinxin. Corroboração e probabilidade: objetivação da admissibilidade de prova eletrónica, **Global Law Review**, v. 4, 2017.

LOPES, Mariangela Tomé. **O reconhecimento como meio de prova**: necessidade de reformulação do direito brasileiro. p. 191. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012.

LU, Tian. PhD Candidate in Intellectual Property Law at Maastricht. (2021). **The Implementation of Blockchain Technologies in Chinese Courts.** Stanford Journal of Blockchain Law & Policy, v. 4.1, 2020.

LUCENA, A. U. de; HENRIQUES, M. A. A. Estudo de arquiteturas do blockchain de Bitcoin e Ethereum. *In*: ENCONTRO DE ALUNOS E DOCENTES DO DCA/FEEC/UNICAMP (EADCA), 9., 2016, Campinas. Disponível em:

https://doi.org/10.51359/2448-2307.2022.253028

https://www.fee.unicamp.br/sites/default/files/departamentos/dca/eadca/eadcaix/artigos/lucena_henriques.pdf. Acesso em: 20 abr. 2022.

MCEWAN, J. **Evidence and the Adversarial Process**. Oxford: Blackwell Publishers, 1992. 326 p.

MESQUITA, Paulo Dá. **Processo Penal, Prova e Sistema Judiciário**. Coimbra: Coimbra Editora, 2010. 452 p.

NAKAMOTO, Satoshi. **Bitcoin**: A Peer-To-Peer Electronic Cash System. Manuscrito não publicado. Disponível em: https://bitcoin.org/bitcoin.pdf [https://perma.cc/QGW4-W934]. Acesso em: 20 abril. 2022.

POLLACCO, Alexia. **The Interaction between Blockchain Evidence and Courts**: A cross-jurisdictional analysis. 2020. Disponível em: https://blog.bcas.io/blockchain_court_evidence. Acesso em: 20 abril. 2022.

RAMOS, Armando Dias. **A Prova Digital em Processo Penal**. 1. ed. Lisboa: Chiado Editora, 2014. p. 86.

RODRIGUES, Benjamim Silva. **Direito Penal**: parte especial. Coimbra: Coimbra Editora, 2009. p. 7222. t. 1.

SAYEED, Sarwar; MARCO-GISBERT, Hector. Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. **Appl. Sci**. v. 9, 2019. Disponível em: applsci-09-01788-v2.pdf. Acesso em: 20 abril. 2022.

UNITED KINGDOM. Ministry of Justice. **Increasing trust in criminal evidence with blockchains**. Disponível em: https://mojdigital.blog.gov.uk/2017/11/02/increasing-trust-in-criminal-evidence-with-blockchains/. Acesso em: 02 maio. 2022.

VAZ, Denise Provazi. **Provas Digitais no Processo Penal**: formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese (Doutorado em Direito Processual) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012.

VERMONT. Vermont General Assembly Rule 902 Self-authentication, de 18 de abril de 2022. **Case TextEUA** , jan. 2022. Disponível em: https://casetext.com/rule/vermont-court-rules/vermont-rules-of-evidence/article-ix-authentication-and-identification/rule-902-self-authentication. Acesso em: 02 maio 2022.

WERBACH, Kevin. Trust, But Verify: Why the Blockchain Needs the Law . **Berkeley Technology Law Journal**, v, 33, n. 487, p. 489, 2018. Disponível em: http://dx.doi.org/10.2139/ssrn.2844409. Acesso em: 02 maio 2022.

WIGMORE, Jonh Henry. Evidence in Trials at Common Law. **Tillers Review Boston**, p. 608, 1983.

YLI-HUUMO, J; KO, D; CHOI, S; PARK, S; SMOLANDER, K. Where is current research on blockchain technology? A systematic review, **Pios One**, v. 10, p.77, 2016.

https://doi.org/10.51359/2448-2307.2022.253028