REVISTA DA EMERJ

DOI: 10.70622/2236-8957.2025.643

CADEIA DE CUSTÓDIA DA PROVA DIGITAL NO BRASIL: O QUE SE PRECISA, O QUE SE TEM E POR QUE PENSAR EM BLOCKCHAIN?

Chain of custody of digital evidence in Brazil: what is needed, what is available, and why consider Blockchain?

Catiane Steffen*

Resumo: Neste artigo, discorre-se sobre como a forma atual de concretização da cadeia de custódia no país contribui para que os dados digitais fiquem mais vulneráveis à desconsideração como elemento de prova no processo judicial, em decorrência de situações como falhas operacionais, lacunas procedimentais e o modo tradicional de estabelecimento da cronologia de acesso e manipulação da prova. Os algoritmos de geração de *hash* por si só não garantem a integridade da prova digital de modo pleno, pois não têm condições de afirmar nada sobre os dados digitais quanto ao que aconteceu com eles antes da efetiva aplicação da função sobre os dados de entrada. A fim de promover elementos como uma maior transparência na gestão da prova digital, o estabelecimento de um histórico cronológico de acesso à prova preciso e confiável, assim como auditoria e *accountability*, além da desmaterialização da cadeia de custódia, apresenta-se a possibilidade de exploração das propriedades da tecnologia *Blockchain* na conformação de uma cadeia de custódia da prova digital confiável e condizente com as necessidades demandadas no processo penal brasileiro.

Palavras-chave: Blockchain; cadeia de custódia; hash; processo penal; prova digital.

Abstract: This article examines how the current way of implementing the chain of custody in the country contributes to making digital data more vulnerable to being disregarded as evidence in legal proceedings, due to situations such as operational failures, procedural gaps, and the traditional method of establishing the timeline of access to, and manipulation of, evidence. Hash generation algorithms alone do not fully guarantee the integrity of digital evidence, as they lack the ability to affirm anything about the digital data regarding what happened to them before the actual application of the function on the input data. The possibility of exploring the properties of Blockchain technology is presented here to shape a reliable chain of custody of digital evidence which is compatible with the demands of the Brazilian criminal process. This is done in order to promote elements such as greater transparency in the management of digital evidence, the establishment of an accurate and reliable chronological history of access to evidence, as well as audit and accountability, in addition to the dematerialization of the chain of custody.

Keywords: Blockchain; chain of custody; hash; criminal procedure; digital evidence.

* Doutoranda na Pontifícia Universidade Católica do Rio Grande do Sul (Direito).
Submissão em: 30/04/2025 | Aprovação em: 21/07/2025 e 27/08/2025

Editor: Antonio Aurelio Abi Ramia Duarte

INTRODUÇÃO

No presente artigo, discorre-se sobre a cadeia de custódia da prova digital no Brasil e se problematizam algumas questões relativas ao assunto, a partir da compreensão de que a prova digital se trata de uma nova modalidade de prova. De forma introdutória e breve, apresenta-se o contexto de surgimento, assim como alguns conceitos e noções principais da tecnologia *Blockchain*, explorando-se, na sequência, como as características e propriedades dela podem contribuir para a efetivação de necessidades demandadas na cadeia de custódia do processo penal brasileiro com foco na prova digital.

Quando se trata de dados digitais, a natureza desses dados por si só já demanda tratamento diferenciado daquele que é dado aos vestígios, evidências e provas físicas, apresentando características específicas que não são capturadas pelos modelos tradicionais de preservação de conteúdo de outras naturezas. Essas características tornam os dados digitais mais facilmente adulteráveis. No entanto, os rastros dessas manipulações são mais difíceis de se constatar e, consequentemente, é mais difícil responsabilizar quem lhes deu causa, caso seja cabível.

Os algoritmos de geração de *hash* cada vez mais são aplicados sobre os dados digitais na tentativa de se garantir a confiabilidade na integridade desse tipo de conteúdo. Frequentemente, a ausência do valor *hash* torna-se motivo para a desconsideração dos dados digitais como prova no processo penal.

No entanto, até mesmo quando se fala em *hash*, há situações a se considerar. Nem todo algoritmo gerador de valor *hash* tem condições de apoiar o objetivo a que se destina em um determinado cenário de aplicação. Alguns dos algoritmos de *hash* existentes não suportam a verificação de integridade dos dados digitais na perícia forense, enquanto outros, que são considerados válidos para tanto, podem não ser adequados para outras atividades forenses.

Há de se considerar também que o que aconteceu com os dados antes de o valor *hash* ser gerado não é capturado pelo algoritmo, que somente pode comprovar a integridade dos dados digitais a partir do que recebeu de entrada em um certo instante de tempo, o da efetiva aplicação. Nesse contexto, a cadeia de custódia da prova digital torna-se de fundamental importância.

Por isso é preciso ampliar o olhar para que se verifique se o modo como se trabalha hoje a cadeia de custódia sobre os dados digitais no Brasil não contribui para que falhas operacionais, lacunas procedimentais e modelos de construção de cronologia/historicidade tradicionais do acesso e manipulação dos dados aumentem o risco do comprometimento da validade de dados digitais como prova no processo penal. Assim, realizadas essas considerações iniciais, apresenta-se a *Blockchain* a partir de um nível mais alto de leitura.

No tocante à tecnologia, há mais detalhes e aprofundamentos que poderiam ser explorados. No entanto, devido ao escopo do trabalho, uma análise mais completa está para além dele, mas poderá estar presente em trabalhos futuros. Em seguida, discorre-se brevemente sobre como algumas das propriedades da tecnologia *Blockchain*, do modelo original às variações dela, vão ao encontro das necessidades da cadeia de custódia da prova digital no processo penal brasileiro, e, na sequência, apresentam-se as considerações finais.

1 BLOCKCHAIN

A tecnologia conhecida como *Blockchain* começou a ser propagada no ano de 2008, quando apareceu em artigo (Nakamoto, 2008) disponibilizado na internet. A ideia central consistia em um modelo capaz de sustentar e viabilizar as transações sobre uma moeda digital, o Bitcoin (BTC). Pouco tempo depois, a tecnologia *Blockchain* tornou-se não somente a base das criptomoedas como também foi aprimorada nas características dela. Assim, encontrou aplicação em diversos setores, suportando os *smart contracts* (que são pedaços de código que, ao verificarem que certas condições são atendidas, automaticamente executam ações predefinidas).

As noções técnicas por detrás da *Blockchain* envolvem múltiplos conceitos, e um deles é o da função *hash*, que, aplicada sobre uma entrada (dados digitais) de tamanho variável, produz uma saída (representação condensada dos dados de entrada) de tamanho fixo. Dentro da perícia forense, algoritmos de geração de *hash* já são utilizados em cenários como os que envolvem a verificação da integridade de dados digitais, que é um dos requisitos que devem ser garantidos dentro da cadeia de custódia no Brasil para que os dados digitais tenham validade como prova no processo penal.

Nesta seção, não se pretende esgotar a análise técnica do conteúdo apresentado (o que nem mesmo seria possível pela extensão do que possibilita, do que promove e do estágio de aprimoramento da *Blockchain*, que se abre em diversas direções), e, sim, apresentar essa tecnologia em um panorama breve e geral que permita compreendê-la desde a ideia inicial, assim como as possíveis variações, discorrendo sobre a possibilidade de exploração das propriedades dela na cadeia de custódia da prova digital no Brasil. Assim, a seguir, apresenta-se uma visão geral da tecnologia *Blockchain*.

1.1 Conceitos e definições

Ao estudar o estado da arte, verifica-se que a tecnologia *Blockchain* avançou muito desde a concepção original. As possibilidades de utilização, exploração e adaptação dessa tecnologia para

vários cenários a torna versátil e lhe confere robustez para ser aplicada no apoio de diversas atividades. Considerando-se que *Blockchain* pode ser implementada utilizando-se alguns dos melhores e mais seguros algoritmos, capazes de apoiar a aplicabilidade dela para muito além da ideia inicial, e em conjunto com outras estruturas, verifica-se que a tecnologia *Blockchain* já materializa parte do potencial de evolução dela, com aplicação em diversos cenários.

A *Blockchain* é apresentada na literatura em trabalhos que envolvem diferentes contextos. Uma rápida revisão em alguns desses materiais permite visualizar e extrair conceitos e definições que se complementam. Em Alharby e Van Moorsel (2017), os autores descrevem a tecnologia *Blockchain* sob a visão de uma base de dados replicada e distribuída entre os participantes da rede que registra todas as transações que aconteceram nela. A base de dados é descrita como sendo formada por uma composição de blocos, encadeada de maneira ordenada, de modo que cada bloco tem um valor *hash* que o identifica. Além disso, cada bloco aponta para o bloco imediatamente anterior e armazena um conjunto de transações. Uma vez que um bloco é criado e anexado à cadeia de blocos, as transações do bloco não podem ser alteradas ou revertidas, o que contribui para garantir a integridade das transações.

A tecnologia *Blockchain* é colocada por alguns pesquisadores como um novo paradigma, sendo destacada a utilização de um mecanismo de consenso distribuído, o armazenamento das informações das transações efetuadas em uma rede ponto a ponto em uma cadeia de blocos e a possibilidade de uso da *Blockchain* para muito além do suporte ao Bitcoin e a qualquer outra criptomoeda. A aplicação estendida da tecnologia *Blockchain* para outros cenários é apresentada na literatura em trabalhos na medicina (Roman-Belmonte, De La Corte-Rodriguez e Rodriguez-Merchan, 2018), na internet das coisas (IoT) (Kshetri, 2017), no *e-government* (Lykidis, Drosatos e Rantos, 2021) e no *plea bargaining* (Sinaga; Bolifaar, 2020).

No artigo de Sinaga e Bolifaar (2020), os autores discorrem sobre a possibilidade de uso dessa tecnologia para atender às necessidades judiciais locais da Indonésia, apresentando um modelo conceitual no qual a utilização da *Blockchain* apoiaria a propositura do *plea bargaining* em crimes corporativos naquele país. Eles destacam a descentralização no controle sobre os dados e a imutabilidade ao trazerem no texto considerações sobre a tecnologia *Blockchain* se comportar como um *ledger*[1] distribuído, que permite o armazenamento dos registros das transações que aconteceram em uma rede ponto a ponto, possibilitando que os nós participantes verifiquem as alterações de estado e suportem conjuntamente a consistência da cadeia de blocos, que deixa de estar sob controle de uma única parte.

[1] Entenda *ledger* como se fosse um livro-razão semelhante a um livro contábil.

Os pesquisadores salientam, ainda, que o encadeamento sequencial dos blocos na *Blockchain* por si já tem a possibilidade de reduzir o impacto dos danos de atividades fraudulentas, pois estando cada bloco ligado ao imediatamente anterior, o cenário mais provável seria o de que uma eventual fraude fosse contida em algum momento contanto que algum dos blocos pudesse identificar o problema e interrompesse a continuidade do fluxo dela. Nesse caso, os dados fraudulentos, no máximo, afetariam algumas partes da cadeia, mas não ela toda.

Assim, realizadas essas considerações a partir de uma breve revisão da literatura sobre a parte de conceitos e definições da tecnologia *Blockchain*, discorre-se um pouco mais, explicando-se de maneira concentrada alguns dos principais elementos que suportam e conformam a estrutura operacional dela. Começa-se a análise a partir da ideia original por detrás dessa tecnologia, pois, conforme se apresenta ao longo do trabalho, hoje, a *Blockchain* tem variações em relação ao que se buscava priorizar de propriedades quando ela foi apresentada, cada qual com especificidades próprias.

Para que a moeda virtual criptografada Bitcoin pudesse circular pela internet com segurança, era necessário garantir a confiabilidade das transações. Ao mesmo tempo, queria se promover um cenário de livre circulação para ela. A ideia foi conceber um sistema no qual não houvesse uma autoridade centralizadora no controle das operações, como as instituições regulatórias que se conhece para moedas físicas ou, ainda, um servidor central dedicado a isso. Uma situação como essa poderia comprometer a segurança em casos como ataques, exploração de falhas e vulnerabilidades, assim como colocar em questionamento a confiança em quem fosse manter a base centralizadora dos registros, o que poderia causar uma dificuldade de aceitação da moeda no mercado.

Diante disso, a tecnologia *Blockchain* foi pensada por Nakamoto (2008) para fazer um caminho contrário: em vez de apoiar a confiabilidade das transações sobre uma autoridade central, ela descentralizou esse controle, concebendo a ideia de um mecanismo de confiança distribuído, trabalhando com uma rede ponto a ponto[2] e um algoritmo de consenso[3]. Quando o consenso é obtido, o que acontece pela satisfação de uma série de regras definidas no protocolo de consenso aplicado na rede, garante-se a transparência e a consistência dos dados nos múltiplos nós participantes dela, pois há uma concordância entre os nós para que um conjunto de dados seja armazenado na cadeia de blocos de forma definitiva.

[2] Na rede ponto a ponto, cada ponto ou nó pode ser tanto cliente quanto servidor, de modo que não há a necessidade de os nós se reportarem a um nó intermediário, específico, centralizador da confiança na rede para conhecer e confirmar um determinado estado de uma transação, por exemplo, vez que cada nó pode tanto enviar quanto receber transações.

[3] Os algoritmos de consenso buscam que os nós cheguem a um acordo sobre a atualização do estado do *ledger*, fornecendo uma maneira de os nós manterem a consistência e a confiabilidade dos dados na cadeia de blocos sem necessitar de uma autoridade central para isso. Uma vez que o conjunto de dados sobre o qual se busca a concordância dos nós seja aceito para inserção na cadeia de blocos, o conteúdo não poderá ser alterado ou excluído. Após a aplicação de algoritmos de consenso, mecanismos de propagação dos blocos garantem aos participantes da rede o conhecimento de um estado único da cadeia de blocos, que é replicado entre os nós.

Além disso, essa impossibilidade de se alterar ou excluir conteúdo aumenta a confiabilidade no histórico cronológico dos eventos persistentes na cadeia de blocos, que se pode levantar a partir do conteúdo registrado no *ledger* distribuído e contribui para a cadeia de blocos armazenar dados de forma segura. Nessa rede ponto a ponto, não há um nó central, e cada nó participante pode tanto validar quanto comunicar transações aos demais. Cada nó mantém uma cópia do *ledger* (livro-razão) distribuído que é gerenciado coletivamente pelos computadores ou nós da rede. Para que todos os nós tenham o mesmo conteúdo nessas cópias, o estado da cadeia principal precisa ser reconhecido e propagado de maneira consistente por todos os nós para que haja uma uniformização, de modo que todos eles espelhem o mesmo estado. Daí a importância da sincronização dos blocos recém-gerados entre todos os nós da *Blockchain*.

Essa sincronização em uma rede *Blockchain* acontece por meio da aplicação de mecanismos de propagação de blocos, que têm as próprias especificidades conforme o tipo e podem ser trabalhados com diferentes níveis de sincronia. As atualizações promovidas na rede são refletidas em todas as cópias, garantindo-se a fidedignidade e a segurança dos registros de dados, o que gera confiança no sistema sem que haja a necessidade de um terceiro confiável centralizando o controle dos dados no *ledger*.

A seguir, discorre-se sobre o encadeamento dos blocos. A tecnologia *Blockchain* expressa exatamente aquilo que ela é: uma sequência de blocos (*block*) interligados entre si, que formam uma cadeia (*chain*), nos quais são armazenadas transações. Cada transação é em si um conjunto de dados que é encapsulado em um bloco, e cada bloco carrega um conjunto de campos, além de englobar dados de uma ou mais transações. Dentre esses campos estão o *timestamp* (data e hora) das transações[4], dois valores de *hash* e um *nonce*, que é um número de 32 bits[5]. Assim, cada bloco armazena um valor *hash* referente ao próprio bloco e o valor *hash* do bloco anterior.

Esse valor *hash* é único e resultante de uma função matemática que, aplicada a uma entrada de dados de tamanho variável, produz como saída um valor de tamanho fixo. No entanto, se a partir de um conjunto de dados de entrada se consegue gerar um valor *hash*, a recíproca não deve ser verdadeira. A ideia é que a partir do valor *hash* gerado não seja possível derivar aquele conjunto de dados original passado para a função operar sobre.

Desse modo, conhecendo-se o valor *hash* do bloco anterior, se estabelece uma conexão entre blocos, na qual cada bloco subsequente consegue verificar a consistência dos dados do bloco anterior.

[4] Em diversos cenários de aplicação prática, ter controle sobre a cronologia das ações é fundamental, não somente pela contribuição na detecção de ações fraudulentas como também pela entrega de subsídios informacionais necessários para se restabelecer o estado anterior. Ao se ter controle sobre o tempo e a ordem das transações, torna-se possível auditar os registros de forma independente.

[5] Conforme a variação da *Blockchain*, pode-se trabalhar com mais campos e com números maiores de bits do que os descritos.

Como todos conhecem o último *hash* calculado, qualquer um deles pode verificar se os dados não foram alterados, pois qualquer mínima alteração deverá resultar em um valor *hash* diferente e, portanto, inválido. A utilização de algoritmos de *hash* fortalece a verificação de toda a cadeia de blocos, pois evita que o conteúdo desses seja alterado e que novos blocos sejam inseridos indevidamente na estrutura. Essa conformação cria a denominada imutabilidade da cadeia de blocos. Se uma transação contiver erros, uma nova transação deve ser criada, e ambas devem ficar visíveis.

Ainda analisando a concepção inicial da *Blockchain*, comenta-se um pouco sobre as variações nas permissões de acesso. A ideia original da *Blockchain* concebia um certo nível de anonimato em uma rede pública, mas é inviável de se operar sob essa conformação em diversos cenários. Hoje, a tecnologia *Blockchain* pode ser trabalhada a partir de uma concepção de permissão de rede de vários tipos, dentre as quais pública e privada, com a possibilidade de modelos híbridos. O desenvolvimento dessa tecnologia ao longo do tempo, que foi aprimorada e atualmente apresenta variações e é integrada a outras estruturas, já permite que se trabalhe a *Blockchain* a partir de participantes com identidades conhecidas e autorizadas a realizar um conjunto delimitado de transações às quais têm as identidades vinculadas.

Quando se estrutura a *Blockchain* a partir de um modelo em que se tem conhecimento e controle sobre os participantes, de modo que cada um tem uma identidade única, consegue-se trabalhar melhor aspectos como as políticas de restrição para a participação na rede, assim como o quanto de detalhes e de conteúdo das transações realizadas se pode delegar de visão a cada um. Além disso, torna-se mais viável de se trabalhar a proteção de dados e de se gerenciar as ações praticadas por cada participante.

Assim, conforme o modo como se estrutura a *Blockchain*, é possível se trabalhar uma arquitetura em que algumas propriedades sejam maximizadas em favor da aplicação a qual se destina e outras sejam reduzidas ou suprimidas em relação ao modelo original da tecnologia. Na prática, situações como essas são muito comuns quando se trabalham questões que envolvem segurança e escalabilidade, por exemplo, na qual, por vezes, a primeira pode ser melhor provida em um certo modelo, porém, com redução da segunda.

O cenário de aplicação e as demandas associadas devem ser considerados na escolha do modelo de permissão de acesso sobre o qual a *Blockchain* será trabalhada, de modo que seja possível fornecer a segurança necessária para suportar e viabilizar a realização da tarefa de acordo com os atributos que devem ser satisfeitos na realidade concreta. Considerando-se uma rede na qual os participantes são conhecidos e confiáveis, o consenso das partes na *Blockchain* pode acontecer por meio de vários mecanismos, para além dos mais usuais, pensados inicialmente para suportar uma rede pública de transações com a moeda Bitcoin.

Na ideia original da *Blockchain*, o consenso acontecia por meio da aplicação do algoritmo Proof-of-Work (PoW) (Gupta; Mahajan, 2020). Esse algoritmo ainda é utilizado em diversos cenários, mas ele é bastante caro computacionalmente falando. Hoje, há vários algoritmos de consenso para suportar e conferir excelentes características à tecnologia *Blockchain*, como o Proof-of-Stake (PoS) e o Delegated Proof-of-Stake (DPoS), que consomem menos recursos computacionais do que o Proof-of-Work. Cada um desses algoritmos tem as especificidades próprias e realizam o consenso de diferentes formas.

De acordo com o caso concreto e aquilo que se busca e que se quer priorizar na implementação, pode se decidir pela aplicação de um ou outro algoritmo. Assim, se houver outros mecanismos de consenso que se mostrem mais adequados para a arquitetura proposta e a necessidade concreta, eles também poderão ser utilizados.

Conforme pode-se perceber pelo explicado até aqui, a *Blockchain* de hoje não é exatamente aquela *Blockchain* do artigo publicado por Nakamoto, em 2008. Diz-se isso no sentido de que houve muitas evoluções na tecnologia *Blockchain*, a partir daquele modelo proposto por ele. Isso faz com que se possa explorar algumas características do modelo original da *Blockchain* em modelos variantes, que, por vezes, conformam desvios mais acentuados em relação ao que se propunha na ideia inicial.

Essa situação faz com que alguns autores questionem na literatura se de fato as variações devem ser consideradas como tipos de *Blockchain* ou se elas já se afastaram demais da essência para serem nominadas assim. Neste trabalho, uniformiza-se o termo com o entendimento mais difundido na literatura, que considera as variações como formas de *Blockchain*. Do ponto de vista da tecnologia, há muito mais do que o apresentado aqui para ser explorado, mas, conforme referido no começo deste trabalho, aprofundamentos maiores ficam para outra oportunidade.

1.2 Por que pensar em explorar características e propriedades da tecnologia Blockchain na cadeia de custódia da prova digital no Brasil?

O avanço das tecnologias trouxe desafios na esfera penal para muito além das violações de direitos na persecução penal (Steffen, 2023). Cada vez mais, atividades ilícitas são praticadas a partir da exploração das possibilidades, especificidades e potencialidades do plano virtual e dos recursos tecnológicos. A dificuldade na obtenção de indícios de autoria e provas de materialidade aumenta substancialmente nesses cenários, diante dos quais, frequentemente, os Estados não se encontram preparados para suportar a persecução penal sem dar causa a questionamentos sobre a validade da prova.

A perícia digital forense é um importante e necessário recurso do Estado para garantir a aplicação da lei nas investigações criminais modernas. Ela necessita de mecanismos de tratamento robustos para garantir a manutenção do estado original dos dados digitais, que é algo que impacta na validade e no uso deles junto aos tribunais.

A produção de prova digital é complexa. As características dos dados digitais, como a natureza frágil e, em alguns casos, volátil, fazem com eles fiquem mais suscetíveis a adulterações do que conteúdos físicos e mais expostos a alterações não intencionais quando sobre os dados digitais incidem procedimentos de manuseio inadequados, algo que pode comprometer a integridade dos dados. Essa dinâmica torna a coleta e a preservação dos dados digitais um desafio aos Estados.

A cadeia de custódia é essencial para se garantir a integridade e a autenticidade dos dados digitais. Por meio da cadeia de custódia aplicada aos dados digitais, se estabelece um processo de documentação e de manutenção de registros que mostra o histórico cronológico do manuseio dos dados. Isso é muito importante porque ter um registro fidedigno de todos os detalhes – dentre eles informações completas sobre quem teve contato com o conteúdo, quando e como os dados digitais foram acessados e manipulados – permite reconstituir o que aconteceu com uma prova quando a validade dela é questionada e que tratamento recebeu quando foi acessada pelos diferentes níveis de hierarquia das autoridades competentes.

Logo, não basta a existência meramente formal de uma cadeia de custódia nem de uma cadeia de custódia implementada de qualquer jeito, ou operacionalizada da mesma maneira como se procedia anos atrás, como se isso fosse suficiente para garantir os atributos que precisam ser preservados para se conferir condição de validade aos dados digitais como prova. O que tradicionalmente se fazia na ciência forense está sendo continuamente tensionado, ainda mais em um cenário como o atual, em que cada vez mais há dispositivos eletrônicos sendo objeto de perícia, com características específicas e uma grande massa de dados com diferentes formatos a ser coletada e examinada.

É preciso que a cadeia de custódia seja pensada e efetivada de um modo que garanta a preservação dos dados digitais que ela visa manter íntegros para a utilização na persecução penal. Do momento da coleta do vestígio até a utilização do conteúdo em decisões pelo juízo, vários são os acessos feitos sobre os dados digitais. Independentemente da natureza digital ou física, a cadeia de custódia deve entregar um modo de tratamento que não retire dos materiais custodiados a condição de validade para utilização em julgamento. No entanto, somente garantir que não há prejuízos à validade dos dados digitais não basta. É preciso ter transparência na cadeia de custódia para ser possível demonstrar e sustentar a validade da prova apoiado no conhecimento em tempo real de todos os acessos feitos ao material e de como esses acessos não impactaram em nenhuma modificação,

refletindo na confiabilidade do conteúdo e garantindo-se que a prova não sofreu interferências na condição original.

Nesse sentido, a tecnologia *Blockchain* pode contribuir ao fornecer atributos como a imutabilidade, a rastreabilidade, a descentralização, a transparência, a segurança e a privacidade, permitindo um gerenciamento eficiente dos dados digitais que garanta a admissibilidade e a credibilidade desse conteúdo no processo penal. A combinação e a exploração de propriedades da *Blockchain* com outras tecnologias faz com que se possa alcançar um alto nível de gerenciamento de acesso por meio de identidades digitais com privilégios, por exemplo.

No Brasil, a cadeia de custódia entrou expressamente por meio das alterações introduzidas pelo chamado Pacote Anticrime (Lei 13.964/2019), sendo definida no artigo 158-A e seguintes do Código de Processo Penal (CPP). Por meio da observância da cadeia de custódia, deve ser possível rastrear cronologicamente todo o acesso e a manipulação dos vestígios, assim como mantê-los intactos ao longo da persecução penal, preservando-os no exato estado tal qual se encontravam no momento da coleta na cena do crime ou na vítima. Embora não haja a previsão expressa no texto do artigo de lei sobre o tratamento incidir sobre os dados digitais, aplica-se de igual maneira por decorrência lógica do próprio instituto.

Algoritmos como os de geração de *hash* podem ser utilizados para demonstrar que nenhuma alteração aconteceu nos dados digitais, mas, na prática, nem sempre são aplicados. No entanto, ainda que se aplique um algoritmo de geração de *hash*, isso por si só não garante a confiabilidade da prova digital, pois o valor *hash* não se presta a atestar a confiabilidade e a segurança na inalteração do conteúdo digital antes de ele ter sido submetido ao algoritmo. Em outras palavras, quando se efetua a verificação de integridade analisando-se o valor *hash*, está se determinando se os dados foram ou não alterados desde que o valor *hash* foi calculado.

Além disso, o valor *hash* precisa ser registrado e guardado com segurança. A manipulação dos dados digitais anterior à aplicação da função *hash* não será capturada pelo algoritmo, que quanto a isso não atestará nada. Por isso a importância de haver controles técnicos e processuais anteriores à geração do valor *hash*, efetivando-se a cadeia de custódia da prova digital. Contudo, uma cadeia de custódia sobre a qual não se possa assegurar que, nas etapas dela, preservam-se atributos como a integridade, a autenticidade e a confiabilidade da prova não pode ser usada para validar ou conferir à prova aquilo que a partir da cadeia de custódia não se pode concluir porque não se consegue demonstrar, repetir ou verificar.

De um lado, a inobservância da cadeia de custódia pode significar a absolvição de culpados, do outro, pode significar a condenação de inocentes. Em meio a tudo isso, o exercício do contraditório e da ampla defesa (com plenitude de defesa) pode se tornar impraticável, corroendo-se a estrutura do devido processo legal. Uma cadeia de custódia confiável precisa ser condizente com as necessidades

demandadas no processo penal pelas diferentes naturezas de provas, evitando-se transformar em alternativa primária (ou em procedimento padrão) a flexibilização que conduz à aceitação daquilo que não se consegue assegurar adequadamente os mais elementares atributos necessários à validade do conteúdo como prova no processo penal.

A forma como se estabelece e se implementa a cadeia de custódia deve afastar questionamentos sobre a validade dos dados digitais em qualquer etapa da persecução penal. Em diversas situações, aplica-se a função *hash* sobre os dados digitais para garantir a confiabilidade na integridade deles, mas falha-se na garantia de outros atributos essenciais, que precisam ser preservados. Isso acontece em grande medida em decorrência de problemas que envolvem essencialmente questões relacionadas à cadeia de custódia dos dados digitais. Exemplificando a partir de cenários reais e recorrentes, há situações como a inobservância da cadeia de custódia (1) no acondicionamento e transporte de dispositivos físicos, como HDs e pen drives, em investigações nacionais e nas que envolvem cooperação jurídica internacional, (2) no registro documental dos procedimentos adotados pela polícia quanto à coleta e preservação dos dados digitais e (3) na documentação da cronologia de acesso aos vestígios digitais. Essas situações são algumas das várias que podem dar causa à quebra da cadeia de custódia.

No Brasil, hoje, a fim de atender à disposição do procedimento da cadeia de custódia constante no Código de Processo Penal (1941)[6], no concernente à rastreabilidade do acesso aos vestígios, em diversas situações, ainda se faz necessário o preenchimento de formulários, muitas vezes, em papel. Há também a necessidade de migração de históricos manualmente descritos e armazenados para sistemas informatizados de gestão de cronologia e acesso. Ainda que os documentos sejam produzidos na maior parte das repartições por meio de ferramentas – como processadores e editores de texto – e que mais tarde se faça o upload desses formulários ao sistema eletrônico, ou que as informações sejam inseridas diretamente em um sistema próprio, isso por si pode representar um consumo de tempo do recurso humano que poderia ser melhor investido e alocado, examinando-se rapidamente, com métricas de sistema, informações como as de cronologia/historicidade, por exemplo.

Além disso, situações como o preenchimento manual de documentação podem implicar em prejuízo ao andamento processual e em quebra da cadeia de custódia, como nos casos em que se verifica a não realização da juntada de um formulário contendo informação pertinente ou de necessária observação e documentação. Há outras situações exemplificáveis: quando juntado o formulário, é possível que informações nele constantes estejam permeadas com problemas de

[6] Código de Processo Penal, artigo 158-E, § 3º expressa que "Todas as pessoas que tiverem acesso ao vestígio armazenado deverão ser identificadas e deverão ser registradas a data e a hora do acesso".

inexatidão ou que nem mesmo tenham sido documentadas. Também pode acontecer de que na transcrição das informações do papel a um sistema de gestão de histórico de cronologia e acesso específico da unidade laboratorial de um Estado aconteçam inconsistências que as afetem e que elas sejam persistidas desse modo, comprometidas por situações diversas, dentre as quais situações análogas ao descrito.

Um simples erro pode afetar toda a persecução penal e, em muitos casos, a prova digital pode ser a única prova existente ou, ainda, a principal fonte de sustentação de uma tese no processo. O reconhecimento da quebra da cadeia de custódia pela impossibilidade de se assegurar a integridade dos dados digitais pode acarretar a inadmissibilidade da utilização do material como prova e a retirada dele dos autos, assim como das provas derivadas, em atendimento ao disposto no artigo 157, § 1º, do Código de Processo Penal (Brasil, 1941).

Diante disso, é importante se pensar em uma estrutura que permita concretizar os objetivos da cadeia de custódia sobre os dados digitais, demonstrando a todos os envolvidos na persecução penal que esses dados não foram adulterados em nenhum momento. Uma estrutura eficiente, que entregue atributos como agilidade, escalabilidade, transparência, confiabilidade, segurança, *accountability* e exatidão na verificação de informações. Uma estrutura que entregue subsídios para que, em vez de se construir confiança na preservação da prova a partir da obrigação de se acreditar no que é afirmado por agentes da lei, por exemplo, se possa construir confiança a partir de métricas do sistema, que possam ser questionadas e auditadas.

Nesse sentido, a persecução penal brasileira pode se beneficiar da implementação de uma arquitetura/*design* que explore as propriedades da tecnologia *Blockchain* a fim de desmaterializar o processo da cadeia de custódia, bem como garantir a integridade auditável dos dados digitais e a rastreabilidade de todo o acesso e manipulação sobre eles. Isso também é relevante no aspecto das tramitações que envolvem a cooperação jurídica internacional, as quais podem incrementar o risco da perda de integridade dos dados digitais. Por isso é importante o conhecimento sobre como a alteração no estado da prova custodiada aconteceu ao longo do tempo.

Conforme explicado até aqui, a tecnologia *Blockchain* evoluiu. Quando se fala no presente trabalho em se explorar *Blockchain* na cadeia de custódia da prova digital no Brasil, não se trata de uma aplicação direta daquela *Blockchain* do modelo original, feita para suportar o Bitcoin e que trabalhava com um certo nível de anonimato em uma rede pública.

No contexto da cadeia de custódia, aquele modelo não sustentaria a aplicação da tecnologia. O que está se propondo é a exploração das propriedades dessa tecnologia – que podem ser reguladas em diferentes níveis para satisfazer as necessidades da realidade local – e das variações da tecnologia *Blockchain* original – dentre as quais se destaca a *Blockchain* Ethereum –, conjuntamente com outras

estruturas, para apoiar atividades como as de análise, controle e monitoramento da preservação dos dados digitais.

A tecnologia *Blockchain*, como qualquer outra tecnologia, não deve ser confundida com algo que resolve todos os problemas. Nem deve ser confundida com uma substituição ao banco de dados, como por vezes alguns *frameworks* propõem irrestritamente sob pena de se causar uma sobrecarga que inviabilize a utilização em alguns cenários[7] (assunto para outro artigo). No entanto, a tecnologia *Blockchain* – do modelo original do Bitcoin às variações da *Blockchain* existentes hoje[8] – entrega propriedades que podem ser exploradas conjuntamente com outras técnicas, ferramentas e estruturas[9] para compor uma arquitetura da qual a cadeia de custódia da prova digital se beneficie quanto às necessidades que demandam satisfação no processo penal brasileiro.

CONSIDERAÇÕES FINAIS

A cadeia de custódia no Brasil precisa ser aperfeiçoada para que, a partir do modo como é concretizada, se consiga identificar com precisão, em qualquer momento da tramitação processual, quem esteve ou está no controle da prova, assim como o que, como e por qual motivo aplicou-se um determinado procedimento ou modo de ação sobre ela. Essa observação é colocada de maneira mais ampla, sem o enfoque na prova digital, porque cabe a qualquer natureza de prova. Especificamente no caso da prova digital, como pretendeu-se demonstrar neste trabalho, a complexidade envolvida na preservação de atributos, como a integridade, aumenta diante da maior facilidade de se promover a adulteração dos dados digitais custodiados.

Ao se pensar na preservação da prova digital no contexto de um devido processo legal como o instituído no Brasil, é preciso ir mais além da limitação da verificação de integridade apoiada na existência de um código *hash*. Conforme se explicou neste trabalho, o que aconteceu com os dados antes de o valor *hash* ser gerado, embora já incidindo sobre eles a proteção da cadeia de custódia, não é capturado pelo algoritmo de geração do *hash*. Nesse aspecto, há a necessidade de outros controles para garantir a integridade da prova digital a fim de permitir se afirmar que os dados sobre os quais se produziu a imagem forense e a geração do valor *hash* efetivamente refletem o estado original deles.

[7] A fim de evitar este pensamento de que a *Blockchain* seria uma tecnologia usada em substituição a um banco de dados foi que se preferiu usar a expressão base de dados ao longo deste trabalho.
[8] Dentre as quais se destacam a *Blockchain* Ethereum e a Hyperledger.
[9] Os *smart contracts*, por exemplo, podem ser utilizados para a atribuição de direitos de acesso sobre a prova digital aos envolvidos na tramitação judicial de cada caso concreto. Assim, quando se utiliza essa estrutura, pode-se atingir um nível de flexibilidade mais elástico na adaptação do modelo desenvolvido ao que é demandado no processo penal local, além de se fornecer métricas de conformidade para o ciclo de vida de tratamento da prova digital.

A dificuldade na rastreabilidade precisa da cronologia de acesso e manipulação da prova, a falta de uma uniformização procedimental de necessária observação e de um plano atualizado de gerenciamento de dispositivos e de dados digitais que acompanhe a evolução tecnológica são alguns dos cenários que podem impactar em prejuízos na preservação da integridade e no comprometimento da autenticidade da prova digital. Esse tipo de prova, pela própria natureza, que lhe confere características específicas, demanda um tratamento diferenciado, que não é entregue quando se aplicam métodos tradicionais de preservação de conteúdo de natureza diversa.

No concernente à cadeia de custódia, não se pode limitar o entendimento a um conjunto de ações praticadas para satisfazer as definições do legislador como se ela fosse mera formalidade na qual cabe qualquer forma de atuação. Não se trata de apenas encaixar o tratamento a ser dado ao conteúdo custodiado em um padrão praticado e concebido para provas de outras naturezas, com características e propriedades bastante distintas. Essa dinâmica tende a colocar os dados digitais sob a proteção de uma cadeia de custódia inadequada para esse tipo de prova, sem condições de assegurar e irradiar no contexto do processo aquilo que se necessita garantir e demonstrar sobre os dados digitais.

Quando se trata de prova digital, tem que se pensar em uma cadeia de custódia que a sustente, que capture as particularidades desse tipo de conteúdo e que o trate adequadamente, provendo controles técnicos e processuais antes mesmo da geração do valor *hash*. Isso tem repercussão direta no exercício de um processo penal democrático, no respeito, na garantia e na efetivação de disposições constitucionalmente expressas.

A cadeia de custódia da prova digital deve permitir identificar de maneira inequívoca todos os detalhes do acesso à prova, inclusive como foram transferidas e as condições de segurança durante o manuseio e o armazenamento, assim como toda a atuação dos profissionais forenses. Nesse sentido, conforme explorado no presente trabalho, a tecnologia *Blockchain* pode contribuir ao fornecer um modelo com atributos, características e propriedades que podem ser explorados conjuntamente com outras tecnologias na efetivação de uma cadeia de custódia transparente, rapidamente auditável, segura, de rastreamento preciso e confiável, que promova a *accountability* e que atenda às necessidades demandadas no processo penal brasileiro diante das especificidades da prova digital.

REFERÊNCIAS

ALHARBY, Maher; VAN MOORSEL, Aad. Blockchain-based smart contracts: a systematic mapping study. **Computer Science & information tecnology**, [*s.l.*], out. 2017. DOI: https://doi.org/10.48550/arXiv.1710.06372. Disponível em: https://arxiv.org/abs/1710.06372. Acesso em: 12 jun. 2023.

BRASIL. **Decreto-lei n. 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Brasília, DF: Presidência da República, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 1 set. 2025.

BRASIL. **Lei n. 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 1 set. 2025.

GUPTA, Chandranshu; MAHAJAN, Asmita. Evaluation of proof-of-work consensus algorithm for blockchain networks. *In*: INTERNATIONAL CONFERENCE ON COMPUTING, COMMUNICATION AND NETWORKING TECHNOLOGIES, 11, 2020, Kharagpur, India. **Anais** [...]. [*S.l.*], IEEE Xplore, 15 out. 2020. DOI: 10.1109/ICCCNT49239.2020.9225676. Disponível em: https://ieeexplore.ieee.org/ document/9225676. Acesso em: 15 jun. 2023.

KSHETRI, Nir. Can Blockchain strengthen the Internet of Things? **IT professional**, [*s.l.*], v. 19, n. 4, p. 68-72, 17 ago. 2017. DOI: 10.1109/MITP.2017.3051335. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8012302. Acesso em: 25 jun. 2023.

LYKIDIS, Ioannis; DROSATOS, George; RANTOS, Konstantinos. The use of Blockchain technology in e-government services. **Computers**, [*s.l.*], v. 10, n. 12, dez. 2021. DOI: https://doi.org/10.3390/computers10120168. Disponível em: https://www.mdpi.com/2073-431X/10/12/168. Acesso em: 12 jun. 2023.

NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. **Bitcoin.org**, [*s.l.*], 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 12 jun. 2023. White paper.

ROMAN-BELMONTE, Juan; CORTE-RODRIGUEZ, Hortensia De la; RODRIGUEZ-MERCHAN, E. Carlos. How blockchain technology can change medicine. **Postgraduate medicine**, [*s.l.*], v. 130, n. 4, p. 420-427, 2 maio 2018. DOI: https://doi.org/10.1080/00325481.2018.1472996. Disponível em: https://www.tandfonline.com/doi/full/10.1080/00325481.2018.1472996. Acesso em: 15 jun. 2023.

SINAGA, Henry Dianto P.; BOLIFAAR, Andhy. Blockchain adoption for plea bargaining of corporate crime in Indonesia. *In:* INTERNATIONAL CONFERENCE ON BLOCKCHAIN TECHNOLOGY, 2, 2020. Hilo, HI. **Anais** [...]. [*S.l.*]: Association for computing machinery, 2020. p. 115-119. DOI: https://doi.org/10.1145/3390566.3391680. Disponível em: https://dl.acm.org/doi/10.1145/3390566.3391680. Acesso em: 1 set. 2025.

STEFFEN, Catiane. A inteligência artificial e o processo penal: a utilização da técnica na violação de direitos. **Revista da EMERJ**, Rio de Janeiro, v. 25, n. 1, 2023. Disponível em: https://ojs.emerj.com.br/index.php/revistadaemerj/article/view/454. Acesso em: 12 jun. 2023.