

# Documentos Públicos Digitais em Blockchain: Fortalecendo a Responsabilidade Democrática

Danielle Alves Batista  
Victoria L. Lemieux

**Como citar:** BATISTA, Danielle Alves; LEMIEUX, Victoria L. Documentos Públicos Digitais em Blockchain: Fortalecendo a Responsabilidade Democrática. In: JORENTE, Maria José Vicentini; PADRÓN, Dunia Llanes; NASCIMENTO, Natália Marinho do; SOUZA, Gabriela de Oliveira (org.). **Contextos Paradigmáticos da Ciência da Informação e as transformações em suas práticas.** Marília: Oficina Universitária; São Paulo: Cultura Acadêmica, 2025. p. 115-137. DOI: <https://doi.org/10.36311/2025.978-65-5954-650-3.p115-137>.



All the contents of this work, except where otherwise noted, is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0).

Todo o conteúdo deste trabalho, exceto quando houver ressalva, é publicado sob a licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 (CC BY-NC-ND 4.0).

Todo el contenido de esta obra, excepto donde se indique lo contrario, está bajo licencia de la licencia Creative Commons Reconocimiento-No comercial-Sin derivados 4.0 (CC BY-NC-ND 4.0).

# CAPÍTULO 3

## DOCUMENTOS PÚBLICOS DIGITAIS EM BLOCKCHAIN: FORTALECENDO A RESPONSABILIDADE DEMOCRÁTICA

*Danielle Alves BATISTA  
Victoria L. LEMIEUX*

### 1. INTRODUÇÃO

A tecnologia melhorou processos e fluxos de trabalho e tornou as sociedades burocráticas mais eficientes com a possibilidade de reutilizar e transformar informações. Por outro lado, essa evolução trouxe desafios para as sociedades em geral, especialmente para os regimes democráticos, onde a liberdade de expressão e o acesso à informação fazem parte da estrutura legal básica. Os documentos públicos como informações governamentais também fazem parte do processo de reutilização e transformação. Segundo Lemieux (2022, p. 10, tradução nossa),

[...] enquanto a capacidade de manipular documentos transformando-os em novas formas de dados levou a grandes inovações e avanços científicos, também minou a base de prova social sobre eventos e ações passadas e, ao fazê-lo, contribuiu para

o surgimento de uma era de desinformação [...]. Blockchain, um tipo único de livro-razão, promete restaurar a base de evidências da sociedade.

A crise da democracia e a polarização que vemos agora não são novidades. A crise começou no início dos anos 2000 (Studebaker, 2023) e foi agravada pela crise financeira de 2008. O rápido surgimento das mídias sociais e a comercialização de dados pessoais por grandes empresas de tecnologia para manipular a opinião pública e os processos democráticos também contribuíram para a crise da democracia e a falta de confiança nas instituições governamentais (Vale, 2024). Nesta nova realidade, os documentos arquivísticos são vitais para servir como evidência da atividade governamental e a transparência pública é fundamental para que as instituições públicas possam recuperar a confiança do contribuinte. Este capítulo discute a relevância dos documentos de arquivo para a confiança pública e o fortalecimento da democracia e como blockchain pode contribuir para esse processo de fortalecimento.

## **2. CONFIANÇA PÚBLICA, BLOCKCHAIN E FORTALECIMENTO DA DEMOCRACIA**

O ano de 2012 marcou um declínio severo na confiança no governo. O relatório do Barômetro de Confiança Edelman de 2012 mostra os governos como as instituições menos confiáveis – principalmente devido à crise financeira de 2008 – pela primeira vez desde a primeira edição do relatório em 2000. O cenário não mudou, e a confiança nos governos diminuiu de maneira global desde então. A confiança decrescente nos governos é um fator crucial na crise da democracia. Como enfatiza Merkel (2018, p. 6, tradução nossa), “se [o governo] não for capaz de resolver problemas-chave e não entregar o que os cidadãos esperam, a legitimidade de sua entregas diminuirá e a estabilidade do sistema estará em risco”. Por exemplo, no contexto brasileiro, um estudo do Banco Mundial baseado em dados do Twitter (atualmente X) revelou que os gastos de Dilma Rousseff com

a Copa do Mundo atiçaram o senso de ‘disparidade relativa’ das pessoas (Lemieux, 2015).

No Brasil, a mudança significativa começou com os protestos nacionais de junho de 2013 contra o aumento das tarifas de transporte público e rapidamente evoluiu para um “movimento reacionário contra a corrupção e contra a política como tal” (Duarte, 2023, p. 68, tradução nossa). Combater a corrupção e a falta de confiança no governo logo se tornou a justificativa para várias manobras políticas para tirar o poder do Partido dos Trabalhadores, o que resultou na vitória do candidato presidencial de extrema-direita, Jair Bolsonaro. O movimento iniciado em 2013 permitiu que influenciadores digitais espalhassem notícias falsas, conhecidas popularmente como *fake news*, uma estratégia extremamente útil para partidos de extrema-direita tomarem o poder em todo o país (Vale, 2024).

Vale (2024) afirma que a transição do Brasil para se tornar uma democracia digital começou imediatamente após os protestos de 2013, em 2014, com mais da metade da população tendo acesso à rede mundial de computadores. De fato, segundo o autor,

[...] o maior acesso à tecnologia de informação digital significou que os usuários da internet no Brasil ficaram mais expostos à desinformação. Nesse contexto de polarização e antipartidarismo, a mídia digital ajudou a produzir mudanças críticas na dinâmica política, levando o Brasil a uma crise democrática (Vale, 2024, p. 83, tradução nossa).

Segundo Lemieux (2022, p. 47, tradução nossa),

Se o governo ou as autoridades públicas não forem vistos como confiáveis (por exemplo, quando se percebe que os funcionários públicos não seguem as regras ou que os mesmos instituem políticas que, embora aparentemente visem proteger o interesse público, na realidade só aumentam os poderes do governo), a base para a confiança, especialmente a confiança nos governos para cumprir fielmente suas missões, diminui. Em tais casos, os cidadãos podem protestar contra as regras institucionais que os governos ou autoridades públicas estabelecem ou aplicam [...], ou podem até rejeitar as regras institucionais do governo completamente [...], o

que pode levar à formação de movimentos políticos subversivos.

Em outros momentos, os governos podem atuar como intermediários de confiança para fornecer garantias de confiabilidade nas interações entre indivíduos. Um exemplo disso é quando os governos emitem licenças para restaurantes para sinalizar que um são locais seguros para comer. Se a agência governamental emissora for vista como não confiável, então os cidadãos também não confiarão que o restaurante é realmente seguro.

Assim, os governos e as autoridades públicas desempenham funções importantes em relação aos relacionamentos de confiança dentro da sociedade, e o grau de confiabilidade percebida dos governos importa, seja essa percepção em relação ao governo como um todo, em relação a instituições específicas, braços do governo ou ainda, em relação ao agente público de forma individuais.

A confiança pública está relacionada, entre outras coisas, à *accountability*, transparência e acesso a informações confiáveis. Blockchain é uma tecnologia emergente com características que podem auxiliar no aumento da confiança nos governos e instituições públicas, fornecendo aos cidadãos um ambiente confiável para armazenar dados imutáveis e divulgar informações públicas fidedignas sobre governança, execução orçamentária e atos administrativos.

Blockchain é uma tecnologia lançada em 2008 pelo pseudônimo Satoshi Nakamoto como base para a criptomoeda Bitcoin (Nakamoto, 2008). Inicialmente, a tecnologia focava principalmente em resolver o problema do gasto duplo com moedas digitais através de sua estrutura descentralizada para validar transações de forma segura usando uma rede *peer-to-peer* (*P2P*). A tecnologia evoluiu para incorporar processos amplos e criação de documentos apenas com o surgimento dos contratos inteligentes (*smart contracts* em inglês), habilitados pela segunda geração de blockchains, como o Ethereum, criado em 2014. A tecnologia agora pode criar e executar contratos inteligentes (Buterin, 2018), fornecer uma plataforma para aplicativos descentralizados (*DApps*) e organizações autônomas descentralizadas (*Decentralized Autonomous Organizations – DAOs* em inglês), e produzir credenciais verificáveis (Sporny *et al.*, 2024) para fins além das transações de criptomoedas.

De acordo com Quiniou (2019), a blockchain é atualmente um ecossistema de soluções de registro de transações e operações baseado em dois eixos principais: descentralização e desintermediação. Quiniou aponta que

[...] o surgimento do blockchain como tecnologia está mudando significativamente o equilíbrio econômico de poder e a posição central atualmente ocupada por intermediários (financeiros, jurídicos, institucionais, editoriais, etc) (Quiniou, 2019, p. xiii, tradução nossa).

Alguns autores, como Tapscott (2023), afirmam que o blockchain é a tecnologia que possibilita a terceira era da Internet ao suportar a propriedade digital, seguindo a lógica da propriedade e as mudanças sociais do século XIX. Alguns dizem que o propósito do blockchain “é alcançar e manter a integridade em sistemas distribuídos” com base em suas características de imutabilidade e “gerenciar a propriedade em um sistema puramente distribuído *peer-to-peer* de livros-razão que opera em um ambiente completamente aberto e não confiável” (Drescher, 2017, p. 58, tradução nossa). Independentemente do caso ou do argumento, o fato é que a blockchain veio para ficar, e governos de todo o mundo estão estudando o uso da tecnologia para promover transparência e responsabilidade, como discutiremos na seção 4.

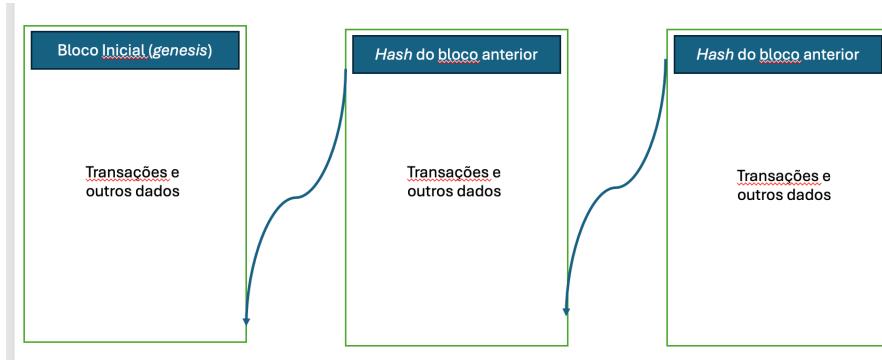
## **2.1 IMUTABILIDADE E INTEGRIDADE**

A imutabilidade é uma das principais características dos sistemas de blockchain. Segundo Attaran e Gunasekaran (2019, p. 13, tradução nossa), no contexto de blockchain, imutabilidade significa que “uma vez que algo é registrado na blockchain, não pode ser alterado”. A capacidade das blockchains de serem imutáveis depende da criptografia, especificamente dos *hashes* criptográficos<sup>1</sup>. Em um sistema de blockchain, cada

<sup>1</sup> A função *hash* (resumo) é qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo. Por esse motivo, as funções *hash* são conhecidas por resumirem o dado. A principal aplicação dessas funções é a comparação de dados grandes ou secretos.

transação registrada em um bloco corresponde a um *hash* relacionado a cada transação. Quando um bloco é assinado e adicionado à cadeia, ele recebe um *hash* do bloco anterior. Esse mesmo *hash* é repetido no próximo bloco criado com novas transações, e esses links criptográficos conectam cada bloco ao bloco seguinte, criando uma cadeia infinita. Alterar dados em uma única transação significa que o *hash* de um bloco inteiro não corresponde mais ao conteúdo do bloco, e essa única alteração impactaria os links criptográficos entre os blocos anteriores. A estrutura criptográfica dos blockchains “significa que os livros-razão e, portanto, o histórico de transações, não podem ser alterados uma vez registrados na cadeia” enquanto aceitam novas transações. O resultado é que o blockchain é uma estrutura de dados apenas de acréscimo na qual “é possível adicionar novas transações, mas é quase impossível alterar e apagar dados que foram adicionados no passado” (Drescher, 2017, p. 60, tradução nossa). A Figura 1 mostra a estrutura genérica de um blockchain com os links de hash entre os blocos.

Figura 1 - Estrutura genérica de um blockchain



Fonte: Bashir, 2017.

---

Dessa forma, as funções *hash* são largamente utilizadas para buscar elementos em bases de dados, verificar a integridade de arquivos baixados ou armazenar e transmitir senhas de usuários.

A integridade possui diferentes conceitos dependendo da disciplina. Nos sistemas de blockchain, a integridade pode se referir à integridade do sistema, dos dados ou dos documentos. Drescher (2017) menciona os três componentes significativos da integridade do sistema como

[...] integridade dos dados – os dados usados e mantidos pelo sistema são completos, corretos e livres de contradições [precisão em diplomática]; integridade comportamental – o sistema se comporta conforme o esperado e está livre de erros lógicos; e segurança [confiabilidade em diplomática] – o sistema é capaz de restringir o acesso aos seus dados e funcionalidades apenas aos usuários autorizados (Drescher, 2017, p. 6, tradução nossa).

Embora o mesmo autor aponte que a integridade dos sistemas e dos dados não é uma característica que apenas o blockchain pode resolver, ele explica que o blockchain é uma tecnologia adequada para resolver problemas de integridade em sistemas distribuídos P2P, especialmente aqueles relacionados ao problema do gasto duplo<sup>2</sup>, dependendo do domínio de aplicação (Drescher, 2017). Para esclarecer o problema do gasto duplo e sua relação com o domínio de aplicação, Drescher (2017) explica

### **Gasto Duplo como um Problema de Cópia de Bens Digitais**

No contexto da cópia de bens digitais, o problema do gasto duplo refere-se ao fato de que dados em um computador podem ser copiados sem limitações perceptíveis. Esse fato causa problemas com dinheiro digital ou qualquer outro dado que deve ter apenas um proprietário em um determinado momento. A cópia torna possível replicar dados que representam pedaços de dinheiro digital e usá-los mais de uma vez para fazer pagamentos. Isso é o equivalente digital a replicar notas bancárias com uma máquina de cópia. Além de ser tecnicamente possível, a cópia de dinheiro digital viola o princípio central do dinheiro: uma peça idêntica de dinheiro não pode ser dada a diferentes pessoas ao mesmo tempo. A capacidade de copiar e gastar dinheiro digital várias vezes torna o dinheiro inútil, daí o problema do gasto duplo.

<sup>2</sup> O problema do gasto duplo é uma vulnerabilidade que pode estar presente em sistemas distribuídos P2P, como o uso duplicado de dados que representam o mesmo token de dinheiro digital para duas ou mais transações diferentes com destinatários diferentes.

### **Gasto Duplo como um Problema de Sistemas Distribuídos P2P de Livros-Razão**

Quando usado para descrever o problema de um sistema distribuído peer-to-peer de livros-razão, o problema do gasto duplo refere-se ao fato de que encaminhar informações para todos os elementos de tal sistema requer tempo, portanto, nem todos os pares têm as mesmas informações de propriedade ao mesmo tempo. Como nem todos os pares têm informações atualizadas, eles são propensos a serem explorados por qualquer pessoa que já tenha as informações mais recentes. Como resultado, alguém pode ser capaz de transferir a propriedade mais de uma vez, resultando em gasto duplo (Drescher, 2017, p. 51, tradução nossa).

A imutabilidade e a integridade são características do blockchain que apoiam a confiança pública, pois dificultam a modificação de dados públicos por agentes corruptos, dificultando também a alteração de documentos digitais públicos registrados na cadeia. O blockchain também viabiliza verificações de integridade dos documentos públicos por meio de seus *hashes* criptográficos como representações das impressões digitais de tais documentos.

## **2.2 TRANSPARÊNCIA E RESPONSABILIDADE**

As plataformas blockchain são geralmente classificadas como públicas ou privadas. Para Morabito (2017), as blockchains públicas são a alta capacidade de inovação da tecnologia, já que nesse tipo de plataforma qualquer pessoa pode se juntar à rede sem aprovação de qualquer intermediário ou terceiro e pode criar, enviar e escrever transações no livro-razão que é a plataforma. Segundo o autor, nas blockchains privadas, “apenas participantes conhecidos e autorizados (usuários) podem incluir dados no blockchain” e “blockchains privados não dão acesso de leitura nem de escrita a participantes desconhecidos” (Morabito, 2017, p. 8, tradução nossa). A Tabela 1 apresenta a diferença entre blockchains públicos e privados.

Tabela 1 - Diferenças entre campos de blockchain público e privado

Blockchains Públicas	Blockchains Privadas
Participantes não são necessariamente identificados	Participantes são conhecidos e confiáveis
Participantes não são necessariamente confiáveis	Participantes são confiáveis
Qualquer um pode acessar dados na rede sem autorização de uma autoridade central	Apenas participantes autorizados podem acessar dados da rede
Qualquer um pode gravar dados na rede sem autorização de uma autoridade central	Apenas participantes autorizados podem gravar dados da rede

Fonte: Morabito, 2017.

Os dados registrados na maioria dos sistemas de blockchain estão disponíveis e abertos para os participantes da rede lerem a qualquer momento. Dependendo das decisões de design<sup>3</sup> do desenvolvimento de um sistema de blockchain, é possível identificar a autoria das transações nos blockchains. A cadeia sempre fornecerá o histórico de transações e propriedade. Essa característica também contribui para aumentar a responsabilidade das instituições públicas, pois o blockchain permite acesso a transações, autoria e propriedade.

## **2.3 DISTRIBUIÇÃO, DESINTERMEDIAÇÃO E SEGURANÇA**

As blockchains são sistemas distribuídos *peer-to-peer* (P2P), especificamente livros-razão distribuídos (Drescher, 2017). A arquitetura distribuída<sup>4</sup> da blockchain proporciona uma rede que não possui um controlador específico ou autoridade central. Sua estrutura é distribuída entre nós responsáveis por manter a rede ativa e em funcionamento. Segundo Drescher (2017, p.

<sup>3</sup> Para mais informações sobre decisões de design de sistemas blockchain leia Lemieux; Feng, 2021b.

<sup>4</sup> Sistemas distribuídos são aqueles em que não há um único componente que possa encerrar todo o sistema.

21, tradução nossa), “sistemas *peer-to-peer* têm o potencial de remodelar indústrias inteiras com base em uma ideia simples: substituir o intermediário por interações *peer-to-peer*”, ou seja, através da desintermediação. Como as blockchains públicas, como por exemplo o Bitcoin, são uma categoria de sistemas P2P distribuídos, seus nós têm direitos iguais sobre a rede, disponibilizam seu poder computacional diretamente para todos os outros nós, e não há um ponto de coordenação central (Drescher, 2017).

Sem um ponto central de coordenação, não há um ponto central de falha, então a característica de distribuição da blockchain proporciona maior disponibilidade do sistema. Além disso, a distribuição fornece uma plataforma sem poder concentrado em poucas mãos, dependendo do design. Por exemplo, no caso dos governos, a desintermediação e a distribuição fornecem um ambiente em que a tomada de decisão pode ser feita por meio de consenso de diferentes autoridades e entidades, dificultando que um único agente corrupto execute ou conclua transações. Segundo o Secretário de Tecnologia da Informação do Tribunal de Contas do Brasil, uma das maiores vantagens dos governos ao usar blockchains é proporcionado por seu caráter descentralizado e transparente, culminando no aumento da confiança dos cidadãos no sistema e nas instituições públicas (Rede [...], 2024).

A distribuição e a desintermediação da blockchain contribuem para o *accountability* e a confiança nas instituições públicas porque essas características permitem a chamada ‘confiança sem confiança’ (Werbach, 2019). Em blockchains a confiança é depositada no sistema como um todo e na forma como o consenso é alcançado entre componentes descentralizados e interativos. É uma “perspectiva de confiança focada na “estrutura profunda” (Wand; Weber, 1995) da tecnologia e em como os criadores de blockchains e sistemas de livros-razão distribuídos buscam resolver problemas de confiança entre atores sociais humanos” (Lemieux, 2022 p. 56), incluindo agentes públicos. Consequentemente, a blockchain é uma tecnologia que pode contribuir para o fortalecimento da democracia, proporcionando capacidades para fortalecer os cinco regimes de democracia embutida (estado de direito) propostos por Merkel (2018), como a) o regime eleitoral democrático (aumentando a integridade do processo de votação), b) o regi-

me de direitos de participação política (aumentando a transparência e o acesso à informação), c) o regime parcial de liberdades civis (aumentando o acesso à informação), d) a salvaguarda institucional de restrições mútuas e responsabilidade horizontal (fornecendo a base para o controle de partes independentes e a participação da sociedade civil), e, e) a garantia de que o poder efetivo de governar dos representantes eleitos democraticamente é assegurado *de jure e de facto*" (Merkel, 2018, p. 7, tradução nossa).

### **3 BLOCKCHAIN E DOCUMENTOS GOVERNAMENTAIS**

Desde a sua criação em 2008, houve vários casos de uso bem-sucedidos de blockchain por governos. Na Estônia, o Governo Federal criou o Blockchain KSI, um projeto parte do e-Estonia. Ele usa tecnologia blockchain escalável para "garantir a integridade dos dados armazenados em repositórios governamentais e proteger seus dados contra ameaças internas" (Cyber [...], 2024). O uso do blockchain é um meio de garantir uma estrutura completa de cibersegurança para processos de governo eletrônico.

O objetivo do blockchain KSI é mitigar ameaças de manipulação interna de dados em seus documentos públicos, permitindo auditoria e transparência em um sistema que pode ser verificado a qualquer momento, mantendo um histórico de atualizações de documentos dos seguintes bancos de dados estonianos: Sistema de Informação de Vigilância/Rastreamento, Registro Oficial de Leis e Regulamentos, Anúncios Oficiais do Estado, Registro de Saúde, Registro de Propriedade, Registro de População, Registro de Empresas, Registro de Sucessão e Sistema Judicial Digital (Guardtime [...], 2024). As razões por trás do uso do blockchain como garantia da integridade dos dados governamentais, de acordo com a Guardtime Technology (2024), são a capacidade de confiar 100% nos dados governamentais em qualquer situação; a capacidade de impor a integridade dos dados governamentais mitigando ameaças internas focadas na manipulação e abuso dos dados armazenados; e a capacidade de verificar a integridade dos dados governamentais independentemente de seu banco

de dados de origem, em tempo real, permitindo a interoperabilidade dos dados entre sistemas e além das fronteiras (Guardtime [...], 2024).

O governo da Colúmbia Britânica (CB), no Canadá, tem realizado vários projetos usando tecnologia blockchain para apoiar processos governamentais<sup>5</sup>. Existem três projetos em andamento usando tecnologia blockchain e credenciais digitais verificáveis no que a província chama de iniciativa *Digital Trust* (Confiança Digital em português). O primeiro desenvolvido e implementado usando Hyperledger Aries e Indy (Hyperledger Aries; Hyperledger Indy, 2024) é o BC ORGBook. Neste serviço digital, qualquer parte interessada pode verificar a autenticidade de documentos emitidos pelo Registro Oficial de Organizações da Colúmbia Britânica (órgão similar à junta comercial no Brasil), como o cadastro legal de uma organização na província, seus números de registro (similar à inscrição estadual de uma empresa) e a revogação de licenças. De acordo com o site do OrgBook BC,

[...] ao fornecer fácil acesso aos documentos [do Registro Oficial de Organizações da Colúmbia Britânica], os cidadãos podem ter confiança em suas interações comerciais, as entidades legais podem validar detalhes chave da organização, os departamentos governamentais podem simplificar e agilizar processos, e as organizações podem monitorar e avaliar atualizações como um indicador de atividade econômica (British Columbia, 2023, tradução nossa).

Outro projeto do *BC Digital Trust* é o *Energy and Mines Digital Trust – EMDT* (Confiança Digital em Minas e Energia em português), um serviço digital do governo da província que emite permissões de exploração de minas de acordo com os regulamentos vigentes. O site do EMDT afirma que “com credenciais digitais, os operadores de mineração e energia podem compartilhar dados confiáveis e verificáveis, permitindo que eles concorram em mercados focados em sustentabilidade” globalmente, um recurso habilitado pela infraestrutura blockchain (British Columbia, 2024). A plataforma usa os mesmos protocolos Hyperledger Aries e Indy

<sup>5</sup> Mais detalhes sobre os projetos envolvendo credenciais verificáveis podem ser obtidas no sítio do projeto BC Digital Trust: <https://digital.gov.bc.ca/digital-trust/home/>

usados no projeto OrgBook. Ela torna as permissões de mineração disponíveis para verificação por qualquer parte ao redor do mundo, fortalecendo a confiabilidade dos negócios de exploração de minas nas terras da Colúmbia Britânica.

No Brasil, existem vários casos de uso de blockchain pelo governo. O Tribunal de Contas da União (TCU), em 2020, publicou dois documentos importantes para o Governo Brasileiro. Um forneceu uma lista de aplicações de blockchain no setor público<sup>6</sup> e entre os projetos citados nesse documento estão: (1) uma plataforma de colaboração e troca de informações entre os países do Mercosul chamada bConnect, (2) uma plataforma para disponibilizar para diversos órgãos públicos as bases de dados de registros de pessoas físicas e jurídicas da Receita Federal do Brasil chamada bCadastro, (3) o projeto piloto em andamento do Real Digital (DRex) do Banco Central do Brasil e diversos projetos envolvendo o Sistema Bancário Público Brasileiro. Há também uma parceria importante entre o TCU, o Banco Nacional de Desenvolvimento Econômico e Social (BNDES) e o Serviço Federal de Processamento de Dados (SERPRO) para desenvolver a Rede Blockchain Brasil (RBB)<sup>7</sup>.

A RBB é estruturada usando o Hyperledger Besu<sup>8</sup>, um cliente Ethereum de código aberto que pode ser executado em redes blockchain públicas e privadas. A escolha do Besu faz sentido porque 1) os governos precisam de uma plataforma que forneça recursos e suporte para executar redes públicas e permissionadas, e 2) o Besu fornece um ambiente para que os governos adicionem diferentes camadas à rede blockchain com diferentes regras e permissões para os participantes. A RBB foi construída para permitir que entidades governamentais desenvolvam aplicativos descentralizados e contratos inteligentes ou adicionem camadas para criar diferente soluções governamentais usando tecnologia de livro-razão distribuído. A RBB também foi projetada para considerar a necessidade de a sociedade civil e organizações não governamentais relacionadas ao monitoramento e

<sup>6</sup> Apêndice 1 do estudo sobre uso de blockchain no Brasil, intitulado Apêndice 1 – Aplicações Blockchain no Setor Público do Brasil, disponível em [https://portal.tcu.gov.br/data/files/58/02/CE/5E/C4854710A7AE4547E18818A8/Blockchain\\_apendice1.pdf](https://portal.tcu.gov.br/data/files/58/02/CE/5E/C4854710A7AE4547E18818A8/Blockchain_apendice1.pdf)

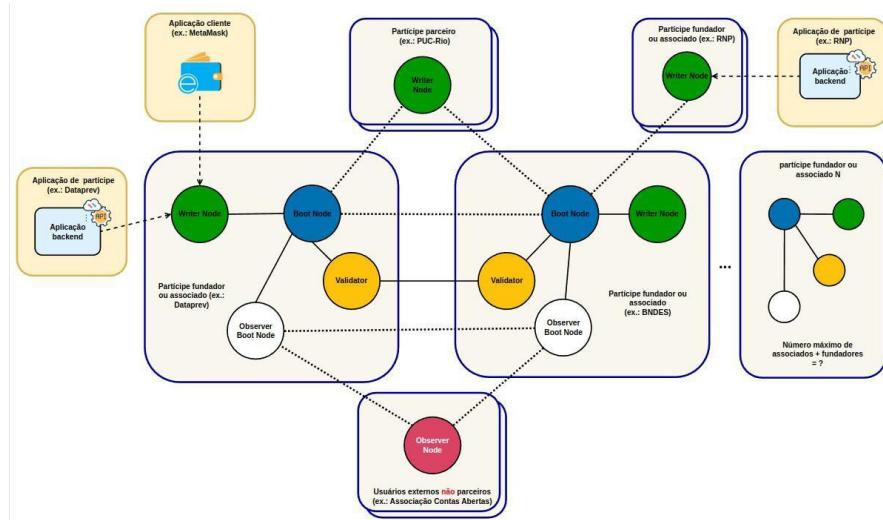
<sup>7</sup> Acesse a documentação da RBB em <https://github.com/RBBNet/rbb>

<sup>8</sup> Para mais informações sobre Hyperledger Besu visite: <https://besu.hyperledger.org/>

controle do governo acessarem dados e informações governamentais transparentes e confiáveis. Embora a RBB tenha sido lançada recentemente em setembro de 2024, espera-se que entidades públicas se juntem à rede, implementando diferentes projetos governamentais e criando e usando registros públicos digitais na plataforma blockchain.

A Figura 2 representa a visão geral da arquitetura da RBB, incluindo seus stakeholders e seus privilégios.

Figura 2 – Arquitetura geral da Rede Blockchain Brasil



Fonte: Coutinho, 2023.

Outro projeto importante brasileiro usando tecnologia blockchain implementado em setembro de 2023 é a Carteira de Identidade Nacional. O Serpro, em parceria com a Receita Federal do Brasil, está usando o sistema bCadastro para apoiar o processo de emissão de identidade nacional por qualquer uma das 27 instituições emissoras de identidade dos estados brasileiros. O objetivo é estabelecer um registro de identidade único para os cidadãos, substituindo o sistema anterior em que cada cidadão poderia solicitar um registro de identidade diferente nos 27 estados do país.

O bCadastro usa o Hyperledger Fabric e disponibiliza informações sobre o registro de pessoas físicas dos cidadãos para que as agências estaduais possam verificar o status dos cidadãos e atualizar suas informações em seu registro ou emitir suas primeiras identidades. Tal projeto já usa tecnologia blockchain para criar documentos públicos relacionados ao processo de emissão de identidade governamental. O Presidente do Serpro, Alexandre Amorim, destaca as vantagens percebidas do blockchain para a emissão de identidades.

A tecnologia blockchain desempenha um papel fundamental na proteção dos dados pessoais e na prevenção de fraudes, proporcionando uma experiência digital mais segura para os cidadãos brasileiros. O uso da plataforma blockchain b-Cadastrados é um grande diferencial para a segurança e a confiabilidade do projeto da Carteira de Identidade Nacional [...]

As aplicações que utilizam blockchain podem contar com vantagens como a imutabilidade dos dados, já que é praticamente impossível alterar ou falsificar os dados registrados em uma rede blockchain [...]

Outra vantagem é a descentralização, pois a tecnologia é distribuída em várias máquinas e nós da rede, o que reduz a vulnerabilidade a ataques cibernéticos, tornando mais difícil para invasores comprometerem a segurança do sistema. O blockchain também promove mais transparência, já que permite rastrear todas as transações e atividades realizadas na rede, aumentando a confiança dos usuários no sistema. (Brasil, 2023).

O blockchain é uma tecnologia promissora para a produção e manutenção de documentos públicos, no entanto, existem algumas limitações tecnológicas para garantir a confiabilidade e preservação de tais documentos. É necessário estar em conformidade com a legislação vigente e a teoria arquivística, normas internacionais (como a ISO 15489:2016 e a associada ISO DTR 24322 Informação e documentação — Blockchain e tecnologia de livro-razão distribuído) em relação a documentos oficiais, incluindo as práticas de gestão documental e os sistemas de gestão arquivística de documentos digitais (ISO, 2025). De acordo com a discussão de Lemieux e Feng (2020a), também é fundamental fazer as melhores escolhas de design

de sistemas ainda no momento de seu desenvolvimento. Para garantir a criação e manutenção de documentos públicos confiáveis usando sistemas de blockchain, devemos discutir a relação entre blockchain e a confiabilidade de documentos de arquivo.

## **4. BLOCKCHAIN E CONFIABILIDADE DOS DOCUMENTOS**

Como discutido na seção 2, a confiança pública depende de *accountability*, transparência e acesso confiável à informação, que são mantidos por meio de documentos confiáveis que atendem aos requisitos de confiança pública. Reconhecer blockchains como sistemas de criação e manutenção de documentos é essencial para vinculá-las a conceitos arquivísticos. Definir blockchains dessa maneira permite que sejam tratados como uma única categoria; independentemente dos vários tipos de blockchain e livros-razão distribuídos agora ou no futuro, todos compartilham as características fundamentais de um livro-razão (Lemieux, 2022) . Projetar sistemas de blockchain e livros-razão distribuídos capazes de criar, capturar e preservar evidências requer a aplicação de teorias, princípios, métodos e práticas de gestão documental.

Pesquisas relacionadas a sistemas de blockchain e manutenção de documentos de arquivo até o momento envolvem: a proposição de uma tipologia de sistema de blockchain de acordo com o local onde o documento é armazenado com base em estudos de caso de uso de blockchain (Lemieux, 2017); críticas diplomáticas para avaliar a confiabilidade dos documentos, baseadas em casos de uso de blockchain envolvendo documentos digitais (Flores; Lacombe; Lemieux, 2018; Lemieux, 2016); e o estabelecimento de uma metodologia para decisões de design sobre sistemas de blockchain para melhorar seu desenvolvimento desde a concepção (Lemieux; Feng, 2021a). Esta seção utiliza críticas diplomáticas como uma ferramenta para avaliar a confiabilidade dos registros em casos de uso de blockchain realizados por Lemieux e estabelece uma metodologia para orientar decisões de

design para sistemas de blockchain desde o início, focando na melhoria da confiabilidade dos documentos.

Em pesquisas anteriores, Lemieux explorou o potencial do blockchain para criar e preservar documentos digitais confiáveis, ao mesmo tempo em que considerava limitações, riscos e oportunidades (Lemieux, 2016). Sua pesquisa analisou o uso do blockchain para registro de títulos de terras em Honduras como um estudo de caso, avaliando seus riscos e a viabilidade de usar blockchain para fins de manutenção de documentos íntegros. As descobertas destacaram questões como governança, confiabilidade dos documentos, autenticidade e a capacidade da tecnologia de garantir a preservação a longo prazo de documentação em meio digital. Especificamente, a solução hondurenha não atendia totalmente aos padrões de confiabilidade e apresentava vulnerabilidades na autenticidade, levantando preocupações sobre a preservação e acessibilidade a longo prazo dos registros originais, já que o projeto autenticava registros armazenados fora da cadeia blockchain (Lemieux, 2016).

Tabela 2 – Reflexões de Lemieux sobre a blockchain da criptomoeda Bitcoin e as funções de gestão documental

1. A blockchain do Bitcoin funciona como um arquivo descentralizado, armazenando documentos originais de forma que possam ser acessados a qualquer tempo? Não. Documentos originais não são armazenados na blockchain do Bitcoin, apenas <i>hashes</i> dos registros originais.
2. É possível reproduzir um documento original a partir do seu <i>hash</i> armazenado na blockchain do Bitcoin? Não. Não é possível fazer engenharia reversa de um hash para reproduzir um documento.
3. O uso da blockchain do Bitcoin garante a confiabilidade dos registros? Não. A confiabilidade só é garantida se os registros forem tanto fidedignos quanto autênticos. As soluções de blockchain não abordam a confiabilidade dos documentos, e há muitas características da blockchain do Bitcoin que podem afetar negativamente a autenticidade das informações.

Fonte: Lemieux, 2016.

Análise adicional de um sistema protótipo de registro de terras em blockchain no Brasil, em colaboração com especialistas arquivísticos brasileiros

(Flores; Lacombe; Lemieux, 2018)<sup>9</sup>, identificou vários desafios na aplicação do blockchain ao registro de terras, particularmente em relação à qualidade das evidências e à acessibilidade ao longo do tempo. Usando padrões arquivísticos alinhados com requisitos legais, as descobertas indicaram que falhas de design poderiam reduzir a qualidade ou a acessibilidade dos documentos, potencialmente minando a transparência, a responsabilidade pública e os direitos de propriedade da terra. Abordar essas questões requer a adaptação de estruturas legais, administrativas e procedimentais. Embora a tecnologia blockchain ainda esteja evoluindo, a pesquisa visa destacar áreas para melhoria em soluções baseadas em blockchain para fortalecer a eficiência do setor público, a responsabilidade e os processos democráticos, em vez de desencorajar a adoção (Flores; Lacombe; Lemieux, 2018).

Apesar dos avanços desde esses primeiros estudos, os sistemas de blockchain ainda carecem de muitos recursos necessários para garantir totalmente a fidedignidade dos documentos arquivísticos e alguns elementos necessários para a autenticidade. Embora a tecnologia possa garantir a integridade dos registros armazenados na sua própria cadeia, ela permanece limitada na capacidade de armazenamento de dados, mesmo para registros PDF leves. A transparência entre os participantes da rede é uma característica fundamental do blockchain, mas os dados armazenados na cadeia são representados principalmente por *hashes* criptográficos, tornando-os ilegíveis em sua forma bruta. Para informações sensíveis, essa transparência também pode ser menos desejável.

## **5. MITIGAÇÃO DE FRAUDES EM DOCUMENTOS**

A fraude em documentos ocorre sempre que peças são omitidas em um procedimento documentado ou quando os documentos são adulterados durante o desenvolvimento do procedimento. Por exemplo, em casos de licitações públicas, quando um agente público modifica uma proposta apresentada para favorecer qualquer participante, isso é um caso claro

<sup>9</sup> There is a Portuguese version of this report on [https://blogs.ubc.ca/recordsinthe-chain/files/2018/01/Versão-1.4-em-PT-BR-do-Projeto-Records-in-the-Chain\\_Final.pdf](https://blogs.ubc.ca/recordsinthe-chain/files/2018/01/Versão-1.4-em-PT-BR-do-Projeto-Records-in-the-Chain_Final.pdf)

em que ocorreu fraude em documentos para permitir a corrupção. Como mencionado anteriormente, o blockchain pode potencialmente diminuir as oportunidades de fraude em documentos, contribuindo para combater a corrupção e aumentar a responsabilidade pública.

Um estudo sobre fraude em documentos de licitações públicas brasileiras propõe uma taxonomia de fraude documental com base nos requisitos de confiabilidade de documentos arquivísticos. Um artigo publicado na fase inicial da pesquisa analisa 217 Tomadas de Conta Especial do TCU, lista as fraudes significativas detectadas e propõe uma taxonomia relacionando os tipos de documento e irregularidades detectadas de acordo com as principais categorias de fraude documental (Batista, 2024). O blockchain é discutido como uma solução para desenvolver aplicativos para evitar as fraudes mencionadas naquela pesquisa.

Em relação à fidedignidade, blockchain pode ser essencial no controle do procedimento de criação de documentos. Através de contratos inteligentes, as entidades governamentais podem garantir que algumas transações sejam executadas seguindo os passos necessários, e essas transações só são concluídas e registradas na cadeia se todos os passos forem completados. Os contratos inteligentes podem, então, ser uma excelente ferramenta para diminuir a oportunidade de omissão de documentos em procedimentos específicos. A adulteração de documento públicos também pode ser mitigada usando blockchains. De fato, documentos armazenados fora da cadeia da rede não podem ter sua integridade garantida pelo blockchain. No entanto, devido à sua desintermediação, a tecnologia fornece recursos para, pelo menos, verificar, por meio de criptografia, a integridade dos documentos armazenados fora da cadeia. Por exemplo, credenciais verificáveis emitidas por plataformas específicas de blockchain garantem a proveniência do documento e contribuem para a manutenção do atributo de autenticidade documental e da identidade do criador do documento. Além disso, as credenciais verificáveis podem fornecer informações sobre um indivíduo sem comprometer sua privacidade.

## **6. CONCLUSÃO**

Em resumo, este capítulo explorou o potencial transformador da tecnologia blockchain em melhorar a transparência, a *accountability* e a confiança nas instituições democráticas, particularmente na gestão de documentos públicos. Com sua imutabilidade inerente e design descentralizado, blockchain oferece um mecanismo promissor para abordar desafios persistentes na confiança pública, o que é crucial quando a responsabilidade democrática é cada vez mais ameaçada pela desinformação e pela desconfiança sistêmica nas entidades governamentais.

A análise ilustra como blockchain, aplicada em várias iniciativas governamentais globais e brasileiras, já é uma tecnologia usada para produzir documentos públicos. No entanto, ainda há trabalho a ser feito para que essa tecnologia garanta uma infraestrutura de manutenção de documentos segura e transparente. Há potencial para blockchain ajudar a prevenir fraudes em documentos e também possibilitar o que podemos chamar de responsabilização pública verificável - um aspecto crítico para restaurar e manter a confiança pública nos processos democráticos. Além disso, ao aproveitar as capacidades do blockchain para integridade de dados e transações verificáveis seguras, os governos podem mitigar riscos de corrupção, promovendo uma esfera pública mais resiliente e inclusiva.

Embora a promessa do blockchain em preservar a autenticidade e a fidedignidade dos documentos públicos seja substancial, ainda existem limitações tecnológicas, como a capacidade de armazenamento e os desafios associados à gestão de dados fora da cadeia. Abordar essas lacunas por meio de escolhas de design direcionadas, alinhadas com a teoria e os padrões arquivísticos, será essencial para maximizar o papel do blockchain na governança pública. Em conclusão, a tecnologia blockchain representa uma oportunidade crucial para melhorar a resiliência democrática, protegendo os registros públicos contra fraudes e manipulações. Ao promover a transparência, a desintermediação e uma abordagem descentralizada para a manutenção de documentos, o blockchain pode contribuir significati-

vamente para fortalecer as estruturas democráticas e, em última análise, a confiança pública.

## REFERÊNCIAS

- ATTARAN, M.; GUNASEKARAN, A. **Applications of blockchain technology in business: challenges and opportunities**. Switzerland: Springer, 2019.
- BASHIR, I. **Mastering blockchain**: distributed ledgers, decentralization and smart contracts explained. Birmingham: Packt, 2017.
- BATISTA, D. A. Enhancing transparency and accountability in public procurement: exploring blockchain technology to mitigate records fraud. **Records Management Journal**, Bingley, v. 34, n. 2-3, p. 151-170, 2024.
- BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Governo começa a utilizar o blockchain na emissão da Carteira de Identidade Nacional**. Brasília: Gov.br, 2023. Disponível em: <https://www.gov.br/gestao/pt-br/assuntos/noticias/2023/setembro/governo-comeca-a-utilizar-o-blockchain-na-emissao-da-carteira-de-identidade-nacional>. Acesso em: 6 nov. 2024.
- BUTERIN, V. A Next generation smart contract & decentralized application platform. **Ethereum White Paper**. [2018]. Disponível em: [http://blockchainlab.com/pdf/Ethereum\\_white\\_paper-a\\_next\\_generation\\_smart\\_contract\\_and\\_decentralized\\_application\\_platform-vitalik-buterin.pdf](http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf). Acesso em: 6 jul. 2018.
- BRITISH COLUMBIA. **OrgBook BC**. Victoria (British Columbia): digital.gov.bc.ca, 26 July 2023. Disponível em: <https://digital.gov.bc.ca/2023/07/26/orgbook-bc/>. Acesso em: 1 nov. 2024.
- BRITISH COLUMBIA. **Energy & mines digital trust**. Victoria (British Columbia): digital.gov.bc.ca, 25 June 2024. Disponível em: <https://digital.gov.bc.ca/2024/06/25/energy-mines-digital-trust-pilot/>. Acesso em: 1 nov. 2024.
- COUTINHO, E. T. **Infra-rbb-visão-geral**. 2023. 1 imagem, formato png. GitHub: RBBNet. Disponível em: <https://github.com/RBBNet/rbb/blob/master/arquitetura/imagens/infra-rbb-visao-geral.png>. Acesso em: 1 dez. 2024.
- CYBER security. **E-Estonia**. [2024]. Disponível em: <https://e-estonia.com/solutions/cyber-security/ksi-blockchain/>. Acesso em: 1 nov. 2024.
- DRESCHER, D. **Blockchain basics**: a non-technical introduction in 25 steps. Frankfurt am Main: Springer Science+Business Media, 2017.
- DUARTE, A. **Pandemic and crisis of democracy**: biopolitics, neoliberalism, and necropolitics in Bolsonaro's Brazil. New York: Routledge, 2023.

FLORES, D.; LACOMBE, C.; LEMIEUX, V. **Real estate transaction recording in the blockchain in Brazil**: case study 1. Vancouver: University of British Columbia , 9 Jan. 2018. Disponível em: [https://blogs.ubc.ca/recordsinthechain/files/2018/01/RCPLM-01-Case-Study-1\\_v14\\_English\\_Final.pdf](https://blogs.ubc.ca/recordsinthechain/files/2018/01/RCPLM-01-Case-Study-1_v14_English_Final.pdf). Acesso em: 1 nov. 2024.

GUARDTIME KSI protecting Estonian digital state. **Guardtime**. [2024]. Disponível em: <https://showroom.demos.guardtime.com/1-ksi-stack.html>. Acesso em: 1 nov. 2024.

HYPERLEDGER Aries: an epicenter for decentralized digital identity collaboration and innovation. **LFDecentralized Trust**. [2024]. Disponível em: <https://www.lfdecentralizedtrust.org/blog/hyperledger-aries-an-epicenter-for-decentralized-digital-identity-collaboration-and-innovation>. Acesso em: 1 nov. 2024.

HYPERLEDGER Indy. **LFDecentralized Trust**. [2024]. Disponível em: <https://www.lfdecentralizedtrust.org/projects/hyperledger-indy>. Acesso em: 1 nov. 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/TR 24332**: information and documentation: blockchain and distributed ledger technology (DLT) in relation to authoritative records, records systems and records management. Geneva: ISO, 2025. Disponível em: <https://www.iso.org/standard/78465.html>. Acesso em: 12 nov. 2024.

LEMIEUX, V. L. **“We Feel Fine”**: big data observations of citizens sentiment about state institutions and social inclusion. Washington, DC: Worls Bank Group Governance, July 2015.

LEMIEUX, V. L. **Searching for trust**: blockchain technology in an age of disinformation. Cambridge: Cambridge University Press, 2022.

LEMIEUX, V. L. Trusting records: is blockchain technology the answer? **Records Management Journal**, Bingley, v. 26, n. 2, p. 110-139, 2016.

LEMIEUX, V. L.; FENG, C. Introduction: theorizing from multidisciplinary perspectives on the design of blockchain and distributed ledger systems (part 1). *In*: LEMIEUX, V. L.; FENG, C. (ed.). **Building decentralized trust**: multidisciplinary perspectives on the design of blockchains and distributed ledgers. Cham: Springer, 2021a. p. 1-20.

LEMIEUX, V. L.; FENG, C. Conclusion: theorizing from multidisciplinary perspectives on the design of blockchain and distributed ledger systems (part 2). *In*: LEMIEUX, V. L.; FENG, C. (ed.). **Building decentralized trust**: multidisciplinary perspectives on the design of blockchains and distributed ledgers. Cham: Springer, 2021b. p. 129-163.

LEMIEUX, V. L. A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation. *In*: IEEE INTERNATIONAL CONFERENCE ON BIG DATA, 2017, Boston. **Proceedings** [...]. Boston: IEEE, 2017.

- MERKEL, W. Challenge or crisis of democracy. In: MERKEL, W.; KNEIP, S. (ed.). **Democracy and crisis**: challenges in turbulent times. Cham: Springer, 2018. p. 1-28.
- MORABITO, V. **Business innovation through blockchain**: the B<sup>3</sup> perspective. Cham: Springer, 2017.
- NAKAMOTO, S. Bitcoin: a peer-to-peer electronic cash system. **Bitcoin**. [2008]. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 4 dez. 2017.
- QUINIOU, M. **Blockchain**: the advent of disintermediation. London: ISTE; Hoboken: John Wiley, 2019.
- REDE blockchain Brasil: integridade, segurança e inovação de interesse público. Brasília, DF: Tribunal de Contas da União, 2024. 1 vídeo (205 min). Disponível em: [https://www.youtube.com/watch?v=mV\\_g88PGM5A](https://www.youtube.com/watch?v=mV_g88PGM5A). Acesso em: 6 nov. 2024.
- SPORNY, M. *et al.* (ed.). Verifiable credentials data model v2.0. **W3C**, Oct. 2024. Disponível em: <https://www.w3.org/TR/vc-data-model-2.0/>. Acesso em: 6 nov. 2024.
- STUDEBAKER, B. **The chronic crisis of American democracy**: the way is shut. Cham: Springer, 2023.
- TAPSCOTT, A. **WEB3**: charting the internet's next economic and cultural frontier. New York: HarperCollins, 2023.
- VALE, H. F. Brazil's digital politics and the crisis of democracy (2013-2018). In: VALE, H. F. (ed.). **Democracy**: crises and changes across the globe. London: IntechOpen, 2024. p. 83-104.
- WAND, Yair; WEBER, Ron. On the deep structure of information systems. **Information Systems Journal**, v. 5, n. 3, p. 203–223, 1995.
- WERBACH, Kevin. **Summary**: blockchain, the rise of trustless trust? [Philadelphia]: Penn Wharton University of Pennsylvania, [2019].