TECNOLOGIA *BLOCKCHAIN* E AUDITORIA

Audit and Blockchain technology

Diego Oliveira Farias
Bacharel em Ciência da Computação pela Universidade Salvador (UNIFACS). Pós-graduado em Redes de Computadores e Telecomunicações (UNIFACS) e Segurança da Informação (UNB). Profissional em tecnologia da informação há 12 anos e atualmente é auditor da Secretaria de Fiscalização de Tecnologia da Informação (Sefti) do TCU. Experiência nas áreas de redes de computadores, segurança da informação, *risk manager*, governança de TI e *Blockchain*. Incentivador da aplicação de tecnologias inovadoras no aperfeiçoamento de políticas públicas. E-mail: oliveiraf@tcu.gov.br

Eldon Teixeira Coutinho
Graduado em Processamento de Dados e atuando com engenharia de software desde 1990, com passagens na iniciativa privada, GDF e Judiciário Federal (STJ e TSE). Recentemente, maior ênfase em arquitetura e integração de aplicações com Microsserviços, EDA (*Event Driven Architecture*) e DDD - *Domain-Driven Design*. Instrutor de cursos de Kafka e DDD para a Administração Pública federal (TCU, STJ e BB). Estudioso e entusiasta da tecnologia *Blockchain*, com participação em auditoria do TCU sobre o tema e criação da RBB - Rede *Blockchain* Brasil, em parceria com o BNDES. E-mail: eldonc@tcu.gov.br

Monique Monteiro
Mestre e Bacharela em Ciência da Computação pela Universidade Federal de Pernambuco (UFPE). Experiência nas áreas de inteligência artificial, ciência de dados e desenvolvimento de *software*, nos papéis de Gerente de Projetos, Arquiteta de *Software* e Engenheira de *Machine/Deep Learning*. *Certified Blockchain Architect, Certified Big Data Scientist, Certified SOA Governance Specialist, Certified SOA Architect, Scum Master, SAFe Agilist, Oracle Certified Master Java EE 5 Enterprise Architect, Sun Certified Programmer for the Java 2 Platform, MCP .NET Framework Development Foundation, MCTS .NET Framework Web Applications e IBM Object-Oriented Analysis and Design with UML*. E-mail: moniquebm@tcu.gov.br

Tibério Cesar Jocundo Loureiro
Bacharel em Ciência da Computação pela Universidade Federal do Ceará (UFC). Mestrando em Computação pela Universidade Estadual do Ceará (UECE). Experiência profissional nas áreas de auditoria de Tecnologia da Informação, gestão de sistemas de informação, Certificação Digital, Segurança da Informação e gerência de projetos de Tecnologia da Informação. E-mail: tiberio.loureiro@tcu.gov.br

RESUMO

A tecnologia *Blockchain*, cuja origem remonta a 2008, com as contribuições seminais de Satoshi Nakamoto, ainda é considerada tecnologia emergente, frente aos seus desafios,

riscos e características inovadoras. Mais de uma década depois, todo um ecossistema de ferramentas, plataformas e casos de uso emergiram, frente a um novo paradigma de acesso descentralizado a dados. O objetivo deste trabalho é desmistificar o assunto, focando em definições, vantagens e riscos, propondo ainda um modelo de avaliação de necessidade para guiar agentes públicos para oportunidades de uso. Paralelamente, apresentamos um panorama do tema dentro do governo brasileiro, com foco na Rede Blockchain Brasil, e, por fim, introduzimos os impactos e oportunidades do uso da tecnologia em atividades de controle e auditoria.

Palavras-chave: *Blockchain*; auditoria; *Distributed Ledger Technology* (DLT); Rede *Blockchain* Brasil (RBB).

1. INTRODUÇÃO

A tecnologia *Blockchain* tem sua origem em 2008, quando um autor desconhecido de codinome Satoshi Nakamoto publicou o documento intitulado "*Bitcoin: a Peer-to-peer Electronic Cash System*" (NAKAMOTO, 2008) em uma lista de discussão na internet. A publicação apresentava combinação inovadora de diversos conceitos relacionados à computação - redes *Peer-to-peer* (P2P), criptografia, assinatura digital e funções *hash*, além de um novo algoritmo de consenso para redes distribuídas e descentralizadas, que permitiam realizar pagamentos *on-line* sem a necessidade de uma terceira parte confiável.

O *Bitcoin* é a primeira e mais famosa aplicação baseada em *Blockchain*. Mas esses dois conceitos não devem ser confundidos. A *Blockchain* é uma tecnologia de rede descentralizada, enquanto o *Bitcoin* é um caso de uso específico de uma rede *Blockchain*. Curiosamente, o termo *Blockchain* não foi mencionado explicitamente no artigo elaborado por Nakamoto, mas o conceito de uma estrutura encadeada de blocos com *hashes* criptográficos (ou resumos criptográficos), na qual cada elemento faz referência ao *hash* do bloco anterior, surgiu no artigo original do *Bitcoin*.

Em termos gerais, a rede *Bitcoin* valida as transações e registra todo o histórico de transações em blocos, que ficam armazenados em um formato de livro-razão distribuído nos nós da rede. O conceito de "bloco" refere-se ao fato de que o estado da rede é armazenado em blocos sequenciais que contêm transações.

Uma das limitações da *Blockchain* do *Bitcoin* proposta por Nakamoto é que a rede somente possibilitava o envio de transações monetárias entre seus participantes. O *Bitcoin* utiliza uma linguagem de *script* básica, mas sem a possibilidade de adicionar linhas de código complexas às transações. Para lidar com tais limitações, em 2013, Vitalik Buterin, um ex-membro da comunidade do *Bitcoin*, propôs uma plataforma para o desenvolvimento de aplicações descentralizadas, chamada de rede *Ethereum*.

A rede *Ethereum* implementa uma máquina virtual chamada *Ethereum Virtual Machine* (EVM), capaz de executar algoritmos do tipo *Turing Complete*, o que significa executar, em teoria, qualquer algoritmo computacional. Os programas desenvolvidos para

execução na rede *Ethereum* são chamados contratos inteligentes (*Smart Contracts*). Contratos inteligentes são executados na EVM, permitindo que a Blockchain *Ethereum* seja programável. A linguagem de programação mais popular utilizada na rede *Ethereum* é o *Solidity*.

O suporte para contratos inteligentes apresenta uma evolução do conceito de *Blockchain*, uma vez que agora é possível executar, de forma autônoma e confiável, códigos computacionais (programas) acordados previamente por duas ou mais partes.

O uso da tecnologia *Blockchain* é indicado quando há necessidade de aumentar a confiabilidade de informações e processos em situações que envolvam muitas partes interessadas e heterogêneas. Por meio de trilhas de auditoria confiáveis, é possível rastrear todas as operações sobre os dados, que são armazenados em um livro-razão distribuído (em inglês, *distributed ledger*), aumentando a transparência e aperfeiçoando o processo de prestação de contas.

Todavia, deve-se considerar que a empolgação gerada por uma nova tecnologia pode acarretar o desperdício de investimento e de dinheiro público, especialmente quando a tecnologia não é totalmente compreendida pelos gestores e as incertezas não são consideradas. Tecnologias inovadoras surgem com frequência e as empresas e os governos precisam estar preparados para lidar com novos riscos e aproveitar as oportunidades abertas.

Este artigo tem o intuito de descrever o que são as redes *Blockchain* / DLT (*Distributed Ledger Technology*), os conceitos e as tecnologias em torno dessas infraestruturas, assim como analisar o potencial e as incertezas destas, especialmente para os serviços digitais do governo. Além disso, será discutido como a tecnologia *Blockchain* pode impactar na atividade de controle externo.

2. *BLOCKCHAIN* E *DISTRIBUTED LEDGER TECHNOLOGY* (DLT)

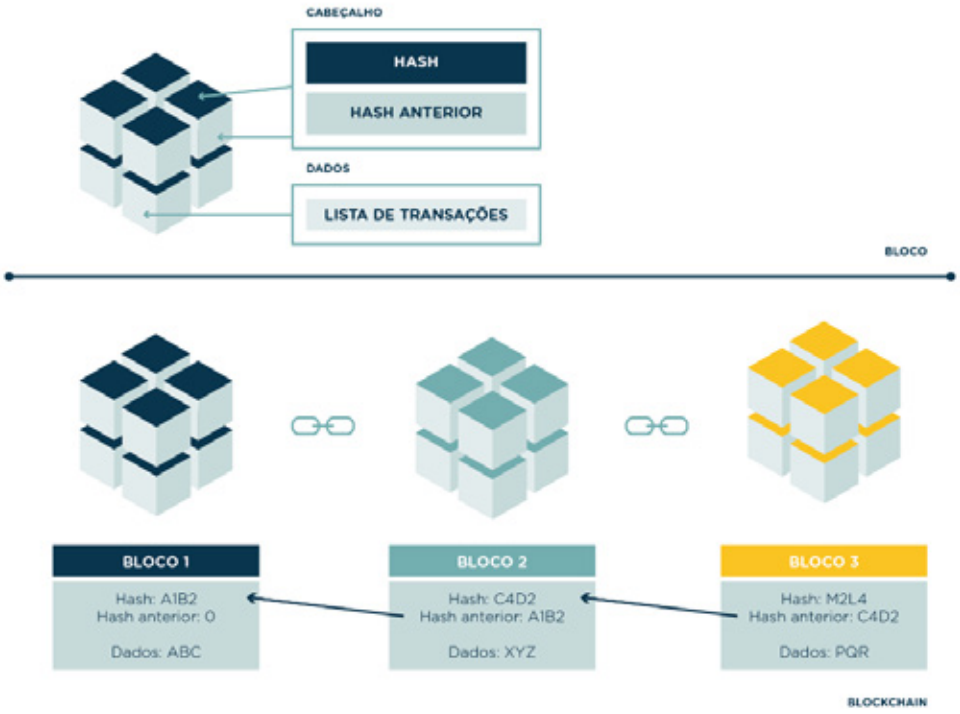
Segundo a Organização para a Cooperação e Desenvolvimento Econômico (OCDE, 2020), a tecnologia *Blockchain* é uma forma de tecnologia de livro-razão distribuído, que atua como um registro aberto e autenticado de transações de uma parte para outra (ou múltiplas partes), e que não são armazenadas ou controladas por uma autoridade central.

Entenda-se livro-razão (*ledger*) como um banco de dados distribuído e replicado em uma rede P2P (*Peer-to-peer*), em que os registros são adicionados cronologicamente, mas nunca são alterados ou deletados, lembrando realmente um livro de lançamentos contábeis, justificando a metáfora.

Como não há um controle central de autoridade sobre os dados, cada nó da rede pode localmente armazenar uma cópia completa do livro-razão, executando um *software* cliente conectado a uma rede *Blockchain*. A cada inclusão de novo bloco contendo as transações, o estado atual do livro-razão é propagado para os demais nós através da rede P2P.

De forma mais técnica, a *Blockchain* é uma estrutura de dados que armazena transações organizadas em blocos, os quais são encadeados sequencialmente. Cada bloco é dividido em duas partes: cabeçalho e dados. O cabeçalho inclui metadados como um número único do bloco, o horário de criação do bloco e um apontador para o *hash* do bloco anterior, além do *hash* próprio do bloco. Os dados geralmente incluem uma lista de transações válidas e os endereços das partes, de modo que é possível associar uma transação às partes envolvidas (origem e destino). A Figura 1 ilustra como os blocos são sequenciados na *Blockchain*.

Figura 1: Encadeamento de blocos em uma rede Blockchain genérica



Fonte: *The International Telecommunication Union* - ITU (adaptado).

Como se observa, cada novo bloco incluído na cadeia possui um conjunto de transações e uma identificação única, gerada a partir de um resumo criptográfico (*hash*). O cabeçalho possui um campo que armazena o resumo criptográfico do bloco imediatamente anterior, estabelecendo uma sequência única entre os blocos. Como cada bloco faz referência ao seu antecessor, se um único bit do bloco anterior for alterado, o *hash* do bloco muda e consequentemente há uma inconsistência na cadeia, que pode ser facilmente detectável pelos nós da rede. Por esse motivo, assume-se que a existência de uma cadeia de blocos interligados garante a segurança e a integridade das transações armazenadas.

Já a transação é uma abstração de um evento de negócios que altera o estado de um livro-razão. Uma plataforma *Blockchain* facilita a execução segura de uma transação em um ambiente descentralizado e auditável. A Figura 2 resume o funcionamento genérico de como uma transação é realizada em uma *Blockchain*.

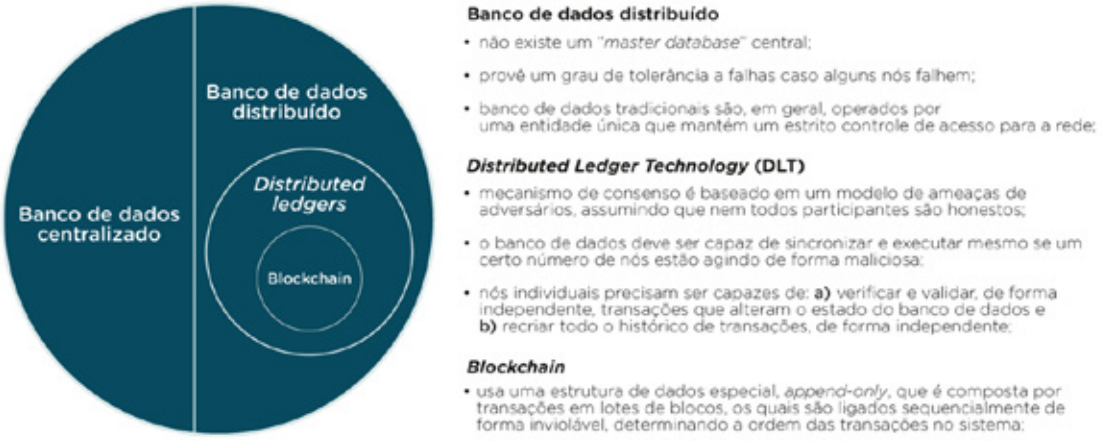
Figura 2. Funcionamento genérico de uma *Blockchain*

Fonte: Comissão Europeia (adaptado).

Conceitualmente, uma *Blockchain* é um caso específico de uma *Distributed Ledger Technology* (DLT), embora esses dois termos sejam frequentemente utilizados de forma intercambiável em diversos documentos pesquisados.

A Comissão Europeia define DLT como uma tecnologia que facilita a expansão de registros transacionais inalteráveis, assinados criptograficamente em uma lista ordenada cronologicamente e compartilhada por todos os participantes da rede. Qualquer participante com direito de acesso pode rastrear a origem de um evento transacional, em qualquer ponto de sua história, pertencente a qualquer ator da rede. A tecnologia armazena transações de uma forma descentralizada. Transações com troca de valores são executadas diretamente entre pares (*peers*) conectados e são verificadas consensualmente, aplicando-se algoritmos na rede. A Figura 3 exemplifica a diferença entre banco de dados tradicional, DLT e *Blockchain*.

Figura 3. Diferença entre tecnologias



Fonte: Universidade de Berkeley e Fórum Econômico Mundial (adaptados).

2.1 MECANISMO DE CONSENSO

Considerando que as primeiras aplicações de *Blockchain* são redes públicas e anônimas, como garantir que os usuários dessas redes se comportem de forma honesta? Deve haver uma forma coordenada em que todas as transações sejam validadas e os nós participantes cheguem a um acordo em relação ao estado da rede. Daí surgem os chamados mecanismos de consenso, que são as regras e os procedimentos pelos quais os nós de uma rede distribuída concordam em validar transações. Importante notar que os acréscimos de novos blocos no livro-razão só são feitos se as regras ditadas pelo mecanismo de consenso forem seguidas por todos.

Especificamente em uma rede *Blockchain*, o consenso é obtido por meio da convergência dos nós em direção a uma versão única e imutável do livro-razão. Importante notar que, para uma transação ser registrada em um livro-razão, ela precisa ser aprovada pelos nós validadores da rede; caso contrário, é automaticamente rejeitada, o que ocorre da seguinte maneira: sempre que uma transação é encaminhada à rede P2P, os nós primeiramente validam a transação segundo regras predefinidas. Se um dado nó concorda com sua legitimidade, a transação é encaminhada para os outros nós validadores da rede e aguardam em um pool de transações. À medida que novos blocos são minerados, as transações pendentes de confirmação saem do pool e são incluídas no bloco, respeitando o limite de transações que um bloco pode armazenar.

Um aspecto fundamental da tecnologia distribuída é determinar qual participante adicionará o próximo bloco (comumente chamado de "mineração do bloco"). Assim que um nó é eleito ou torna-se apto a criar um bloco, este novo bloco é adicionado à cadeia anterior de blocos de forma imutável, contendo as transações mantidas em seu pool. Dessa maneira, a sequência de blocos mais recente mantém uma visão compartilhada e acordada do estado atual da *Blockchain*.

Cada algoritmo de consenso tem diferentes configurações de conflitos de escolhas (*trade-offs*), que são otimizados para atender a determinada necessidade. Os dois principais algoritmos de consenso utilizados em *Blockchains* públicas são o *Proof-of-Work* (PoW) e Proof-of-Stake (PoS). O *Bitcoin* utiliza o PoW e recentemente a rede *Ethereum* migrou do PoW para o PoS.

O PoW, ou prova de trabalho, foi concebido para ambientes em que há uma falta de confiança mútua entre os usuários. Neste algoritmo, para que um nó adicione um bloco à *Blockchain*, ele precisa alocar recursos de processamento com o objetivo de resolver um problema matemático difícil, que é derivado da cadeia de blocos. A resolução do problema serve como uma prova de que o nó (denominado como nó minerador) conduziu o trabalho necessário para encontrar a solução do problema, de modo que ganha o direito de adicionar o próximo bloco.

Uma vez que o nó minerador é o primeiro a resolver o problema, ele envia o novo bloco para os outros nós da rede com a prova de trabalho. Estes, por sua vez, verificam se, de fato, o desafio matemático foi resolvido corretamente pelo nó minerador e se as transações incluídas nesse bloco são válidas, ou seja, se estão de acordo com as regras da rede. Em caso afirmativo, cada um dos nós adiciona o bloco à sua cópia do livro-razão (atualizando seu próprio estado) e o distribui pela rede. Depois disso, o processo de mineração é reinicializado, e assim sucessivamente.

O processo para resolver o desafio matemático é intencionalmente caro em termos de tempo de processamento e eletricidade, e, consequentemente, em termos financeiros. Não obstante, o processo de verificação da solução do desafio pelos demais nós da rede é intencionalmente muito rápido, ou seja, eficiente em termos computacionais.

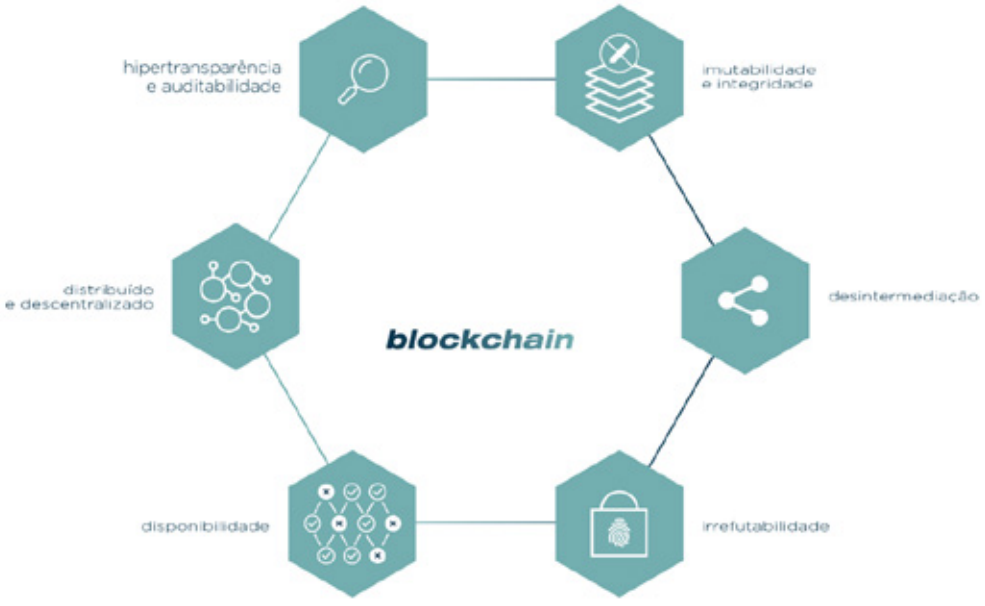
Já o modelo *Proof-of-Stake* tem como premissa o conceito de que os usuários que mais "apostaram" na rede, do ponto de vista do percentual de tokens que eles possuem na plataforma (geralmente criptomoedas ou criptoativos), são aqueles que têm um maior desejo de que a plataforma seja bem sucedida e, por isso, tomarão decisões no interesse da rede com a menor probabilidade de subvertê-la. Tal fator é considerado determinante pelo sistema para decidir qual usuário tem prioridade para adicionar novos blocos à cadeia.

Há diversas formas de implementar, na prática, algoritmos do tipo PoS. Alguns métodos incluem escolher usuários aleatoriamente de forma proporcional às respectivas quantidades de tokens possuídos pela plataforma, pelo uso de votação, ou pela "idade" do ativo.

Assim como o modelo PoW, o modelo Proof-of-Stake é adequado para ambientes onde há altos níveis de desconfiança mútua. Porém, ao contrário do PoW, o processamento intensivo de recursos computacionais (gasto energético) não é necessário. A desvantagem é que o mecanismo de consenso fica menos descentralizado em relação ao PoW, uma vez que é possível identificar e atacar aqueles com mais tokens da plataforma.

2.2 PRINCIPAIS CARACTERÍSTICAS

Figura 4. Características da tecnologia Blockchain



Fonte: Fórum Econômico Mundial (adaptado).

2.2.1 Hipertransparência e auditabilidade

O livro-razão é um dado acessível e público a todos que façam parte da rede, o que significa que os participantes podem ver todo o histórico das transações em tempo real. Essa propriedade da *Blockchain* aumenta a rastreabilidade das operações. Qualquer usuário pode auditar completamente todas as transações; isso é particularmente importante para aplicações governamentais, considerando-se que muitas informações de programas governamentais devem ser públicas, permitindo a auditoria direta por participação da sociedade civil.

2.2.2 Distribuído e descentralizado

Descentralização refere-se à transferência de controle e tomada de decisão de uma entidade centralizada (indivíduo, organização ou grupo) para uma rede distribuída.

A rede *Blockchain* pode ser utilizada como uma camada de integração de bases de dados, permitindo o uso compartilhado entre diversas organizações e colaboradores externos, o que viabiliza um governo hiperconectado.

2.2.3 Desintermediação e automação de transações e processos

A tecnologia *Blockchain* introduz um novo paradigma: a possibilidade de diferentes partes transacionarem sem a necessidade de confiar em um intermediário central. A existência de uma terceira parte confiável para resolver conflitos das transações pode ser substituída por uma infraestrutura *Blockchain*.

Adicionalmente, reduz a necessidade de implementar processos complexos de reconciliação entre as partes e diminui custos, já que é possível usar contratos inteligentes, executados automaticamente, de acordo com regras predefinidas.

2.2.4 Disponibilidade

Como todos os participantes têm uma cópia local sincronizada com a rede, se um nó fica indisponível, o livro-razão pode ser acessado através de outros nós. Ou seja, a *Blockchain* é uma rede resiliente, com várias cópias compartilhadas de dados, de modo que serviços públicos que necessitam dessas informações podem continuar em operação mesmo que alguns nós não estejam disponíveis.

2.2.5 Imutabilidade e integridade

A *Blockchain* utiliza técnicas criptográficas para proteger seus registros, incluindo funções de *hash*, ponteiros de *hash* e assinaturas digitais. Isso faz com que qualquer tipo de adulteração seja percebido, por se tratar de uma violação matemática da cadeia de blocos.

Essa propriedade garante que a *Blockchain* seja um registro imutável, de modo que nenhuma entidade é capaz de alterar dados passados sem resultar em um alerta à rede, e que todas as partes podem verificar a consistência dos dados de forma independente.

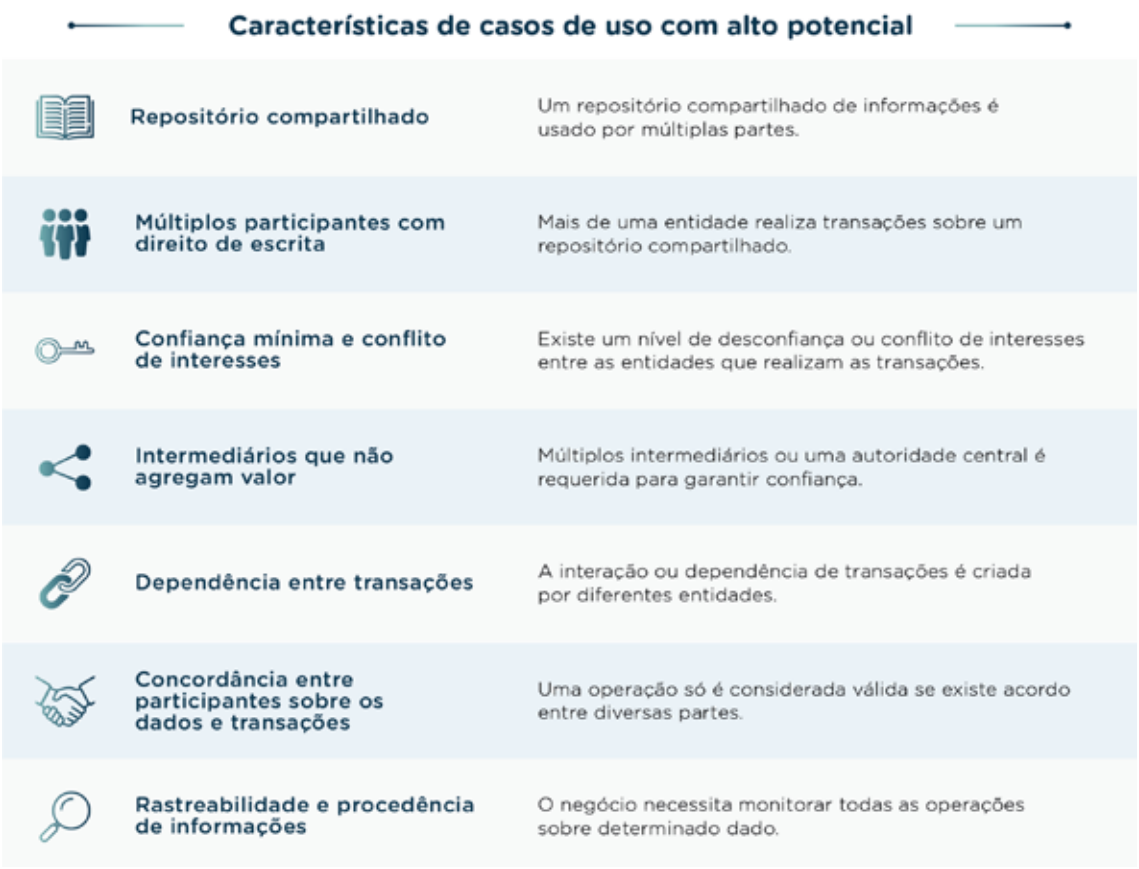
2.2.6 Irrefutabilidade

Uma das funcionalidades essenciais das tecnologias *Blockchain* é o uso da criptografia de chaves públicas (ou chaves assimétricas), que servem como uma base para a autenticação dos usuários da rede. Com o uso de chaves privadas e funções de *hash*, um participante é capaz de realizar assinaturas digitais sobre as transações, o que serve como uma prova inegável de que é o emissor de determinada mensagem (não repúdio).

3. MODELO DE AVALIAÇÃO DE NECESSIDADES

As tecnologias descentralizadas e distribuídas podem ser aplicadas em áreas que ainda não foram imaginadas. De todo modo, a Figura 5 apresenta características genéricas que indicam um alto potencial para a utilização da tecnologia *Blockchain*:

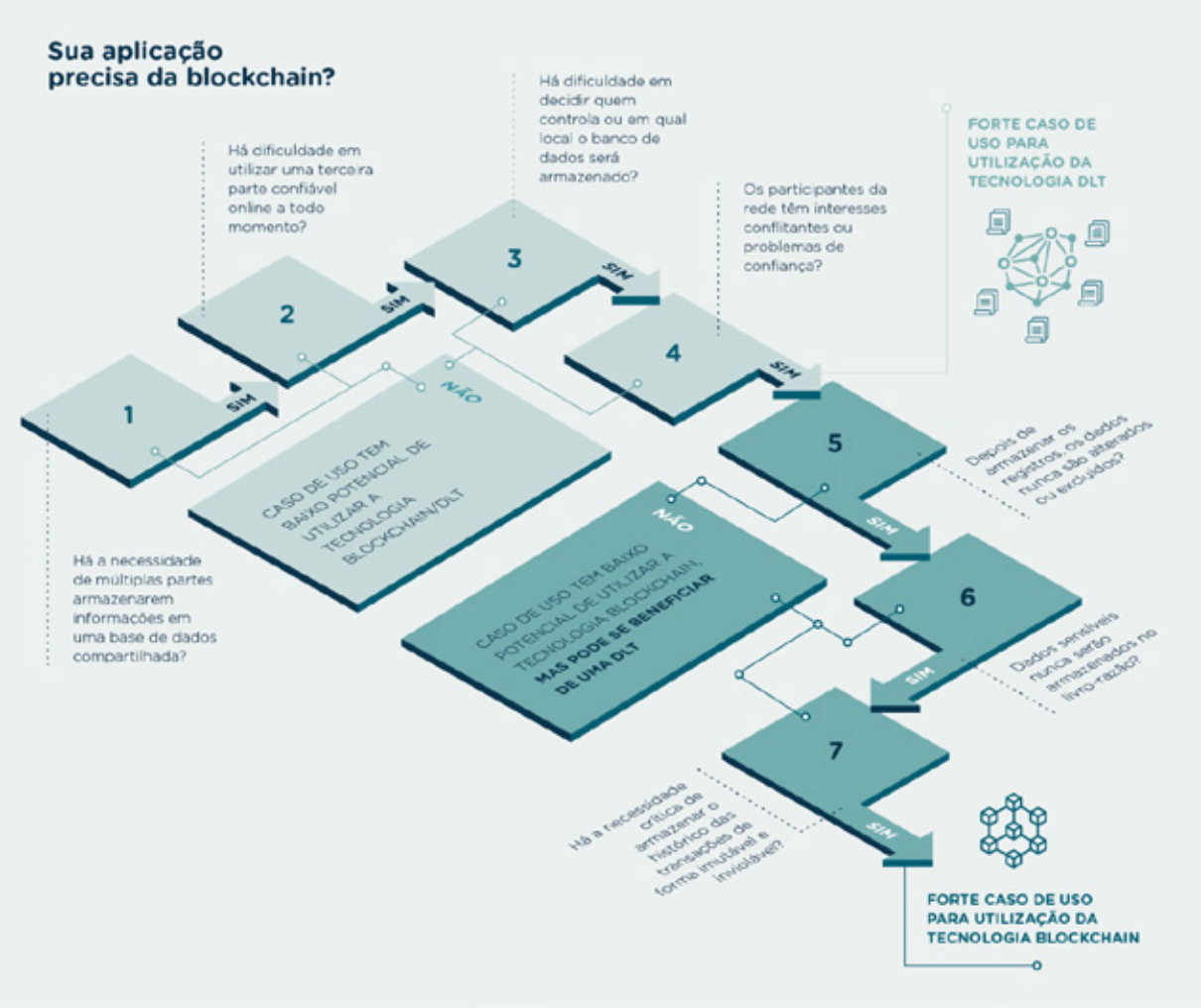
Figura 5. Características de possíveis casos de uso



Fonte: Fórum Econômico Mundial (adaptado).

Contudo, como identificar precisamente se uma organização pode se beneficiar de soluções baseadas em *Blockchain*? Para decidir se uma solução *Blockchain* se aplica ou não ao caso de uso de uma instituição, apresenta-se um modelo de avaliação de necessidade, que consiste em perguntas diretas sobre as características do processo de negócio da organização. Quanto mais respostas "sim" nas perguntas de 1 a 7, maior a probabilidade de o caso de uso precisar de uma *Blockchain* ou DLT. As perguntas de 5 a 7 referem-se ao caso especial de uma *Blockchain*. A Figura 6 representa o fluxograma do modelo de avaliação mencionado, seguido do detalhamento de cada uma das perguntas.

Figura 6. Modelo de avaliação de necessidade



Fonte: os autores.

1. Há necessidade de múltiplas partes armazenarem informações em uma base de dados compartilhada?

Primeiramente, deve-se avaliar se uma ou mais partes têm a necessidade de compartilhar e gravar dados em um mesmo banco de dados. A utilização da tecnologia *Blockchain* ou DLT requer situações em que múltiplas partes estão envolvidas em uma transação, ou seja,

somente faz sentido se existem múltiplos atores e se os dados têm origem em diversas fontes. Caso essa condição não seja verdadeira, deve-se avaliar outros tipos convencionais de banco de dados.

2. Há dificuldade em utilizar uma terceira parte confiável *on-line* a todo momento?

A utilização de uma *Blockchain* ou DLT envolve a mudança da arquitetura cliente-servidor, frequentemente utilizada pelas aplicações, para o paradigma P2P. Caso exista um sistema centralizado que possa resolver determinado problema com elevado grau de disponibilidade, devem ser explicitados os ganhos com a adoção de uma arquitetura distribuída, capaz de garantir a confiabilidade das informações armazenadas. Além disso, deve-se avaliar se existe a necessidade da área de negócio de remover intermediários ou funções burocráticas, uma vez que essas tecnologias favorecem a desintermediação, pelo fato de não dependerem de uma terceira parte confiável.

3. Há dificuldade em decidir quem controla o banco de dados ou em qual local será armazenado?

Nos sistemas tradicionais, os dados são controlados (*data authority*) por um participante que detém a supremacia sobre os dados; os demais participantes apenas confiam que o controlador dos dados mantém a fonte de dados íntegra e confiável. Quando há dificuldade em se eleger um participante que exercerá o controle sobre os dados, a arquitetura distribuída em DLT ou *Blockchain* é indicada. A adoção de uma arquitetura distribuída pressupõe um modelo de negócio descentralizado, em que múltiplas partes podem ter níveis diferentes de controle dos dados.

4. Os participantes da rede têm interesses conflitantes ou problemas de confiança?

A utilização da tecnologia *Blockchain* é potencializada quando não há confiança mútua entre participantes, uma vez que uma *Blockchain* resolve esse problema descentralizando o controle e armazenamento de dados para toda a rede, garantindo que todos os participantes executem as mesmas regras.

5. Depois de armazenar os registros, os dados nunca são alterados ou excluídos?

Em uma *Blockchain*, novas informações são apenas apensadas, não havendo alteração dos dados que já foram gravados no livro-razão. Isto é particularmente difícil de se atingir em casos em que a Lei Geral de Proteção de Dados e o direito de esquecimento devem ser aplicados, já que não há como deletar as transações registradas na *Blockchain*.

6. Dados sensíveis nunca serão armazenados no livro-razão?

Se a aplicação pretendida deve manter os dados sob sigilo, a utilização de redes públicas *Blockchain* é contraindicada. No caso de redes públicas, as aplicações com acesso aos nós podem visualizar e rastrear todo o histórico de transações. Logo, uma *Blockchain* pública deve ser utilizada para armazenamento de dados não sensíveis.

7. Há necessidade crítica de armazenar o histórico das transações de forma imutável e inviolável?

A imutabilidade e integridade são benefícios essenciais das redes *Blockchain*, já que os blocos são encadeados e armazenados de forma distribuída por nós que seguem as mesmas regras.

Assim, basicamente, uma *Blockchain* será útil quando há necessidade de armazenar, de forma íntegra, consistente e inviolável, todos os detalhes de transações que foram validadas pela rede, permitindo a rastreabilidade dessas transações, e o não repúdio de sua autoria.

4. SMART CONTRACTS: UMA VISÃO TEÓRICA

Um contrato celebrado entre partes interessadas usualmente tem um conjunto de cláusulas (promessas) que são pactuadas e assinadas entre essas partes. Contratos são geralmente escritos por partes envolvidas, e são autenticados e auditados por entidades intermediárias. Intermediários como advogados, cartórios (tabeliões), corretores, auditores e empresas são responsáveis por estabelecer uma relação de confiança entre as partes. No caso de cartórios, o próprio contrato fica registrado em um ente intermediário, que detém sua custódia e dá fé pública ao documento. A principal razão para a existência de tais intermediários é a necessidade de mediação entre partes que não têm uma relação de confiança entre si.

Contratos inteligentes, ou *Smart Contracts*, são códigos-fonte em linguagem de programação que podem ser definidos e autoexecutados em uma infraestrutura de *Blockchain*. A definição e execução de um contrato inteligente nesses ambientes se dá sem a necessidade de intermediários.

O conceito de contrato inteligente foi definido por Nick Szabo (SZABO, 1997), pesquisador em criptografia e especialista em Direito. Em seus artigos, Szabo define contrato inteligente como cláusulas contratuais embutidas em *hardware* e *software* cuja violação é proibitiva sob o ponto de vista computacional e, consequentemente, econômico, portanto, não vantajosa a um possível violador.

Outro conceito dado pela (ITU, 2019) é que contrato inteligente é um programa de computador que utiliza transações assinadas criptograficamente em uma rede *Blockchain*. O contrato inteligente é executado por um nó que recebe uma recompensa pelo processamento e os resultados da execução são validados por consenso e registrados no livro-razão distribuído. A automação inteligente de contratos reduz custos e riscos de erros, mitiga riscos de fraude e, potencialmente, otimiza muitos processos de negócios.

O contrato inteligente é executado por envio de mensagem ao endereço do contrato em uma *Blockchain*, que sinaliza um evento significativo para as regras de negócio que governam as relações entre os participantes do contrato. O papel do intermediário do contrato é delegado à própria tecnologia empregada para o uso de contratos inteligentes, ou seja, a própria infraestrutura da *Blockchain*. Além disso, é assegurado que os nós daquela rede possuem instalado o mesmo software para execução do contrato inteligente.

Devido às características da *Blockchain*, contratos inteligentes são imutáveis quanto a sua definição de código-fonte e seu estado (dados); o resultado de sua execução, uma vez que os nós validadores cheguem a um consenso sobre esse resultado, torna-se imutável após a inclusão na *Blockchain*. As características de imutabilidade são desafios na adoção dessa tecnologia, conforme veremos adiante.

Um contrato inteligente pode utilizar outros contratos inteligentes e serviços externos, conhecidos como oráculos, que fornecem dados que auxiliam na execução do contrato. Por exemplo, um contrato inteligente que precisa validar o nome de um cidadão junto à Receita Federal pode usar um serviço externo (API) à *Blockchain* para essa validação.

Apesar dos benefícios supracitados, contratos inteligentes enfrentam desafios tecnológicos e legais que "freiam" a sua adoção em larga escala. Desafios legais incluem a adequação às leis de proteção a dados, a exemplo da Lei Geral de Proteção dos Dados (LGPD) brasileira e da *General Data Protection Regulation* (GDPR) europeia, já que essas legislações definem o "direito ao esquecimento", o que vai na contramão dos aspectos de imutabilidade dos dados em *Blockchain*. Outro desafio é a resiliência de serviços off-chain ou serviços oráculos, que podem afetar a execução de contratos inteligentes devido a indisponibilidade ou mal funcionamento. A natureza de imutabilidade do código-fonte do contrato inteligente é outro desafio.

Na verdade, uma vez publicado o código-fonte em *Blockchain*, só é possível excluir ou alterar um contrato apenas se o programador adicionou a função no código, caso contrário, é impossível modificar um contrato inteligente, o que pode ser muito prejudicial em casos de descobertas futuras de bugs ou vulnerabilidades de segurança. Ainda, por mais que esses códigos fontes sejam exaustivamente testados antes de sua publicação, a própria definição do "negócio" de que trata o contrato inteligente pode mudar; seja por acordo entre os participantes, seja por mudanças na legislação.

Por fim, outro desafio é a escalabilidade, ou seja, a capacidade de os contratos inteligentes continuarem com sua execução em tempos razoáveis, mesmo com o incremento do número de transações processadas; os atuais protocolos de consenso utilizados em redes *Blockchain* públicas, como Ethereum Mainnet, não permitem a execução de transações com alta escalabilidade, a despeito dos esforços da comunidade Ethereum na adoção de protocolos de consenso com melhor desempenho.

5. NON-FUNGIBLE TOKENS (NFTS)

Antes de explicar o que é um NFT, é necessário entender o que faz um ativo ser fungível. Fungibilidade é o atributo pertencente aos bens móveis que podem ser substituídos por outros da mesma espécie, qualidade e quantidade. Esses itens são intercambiáveis porque são definidos pelo seu valor e não pela sua exclusividade. São exemplos uma nota de dez reais, um *bitcoin* e *commodities*.

Enquanto moedas físicas e criptomoedas podem ser trocadas uma pela outra, sem distinção, os NFTs não são intercambiáveis entre si. Cada NFT tem um identificador distinto e único, que o torna diferente dos demais.

Um token não fungível é um ativo criptográfico baseado na tecnologia *Blockchain* que representa um ativo digital ou físico. Os NFTs são projetados para serem verificáveis criptograficamente, únicos ou escassos e facilmente transferíveis.

Um NFT é registrado publicamente na *Blockchain* de forma que qualquer pessoa possa verificar a propriedade de um objeto. Um NFT pode ter apenas um proprietário por vez. Cada vez que um NFT é transferido ou criado, a ação é gravada permanentemente no *Blockchain* e tem registro de data e hora, o que significa que é possível rastrear qualquer NFT até sua gênese. Os NFTs são cunhados ou "mintados" (*minted*) por meio de contratos inteligentes que gerenciam a propriedade e transferência dos NFTs. Quando alguém cria ou cunha um NFT, ele publica um código armazenado em contrato inteligente que está em conformidade com diferentes padrões, como o ERC-721 ou ERC-1155 da rede *Ethereum*.

O criador de um NFT é quem define a escassez do ativo digital. Por exemplo, os ingressos para a arquibancada de um estádio de futebol podem ser vendidos como NFTs (*tickets* virtuais) em que a numeração de 1 a 50.000 representa as cadeiras do estádio. Podem ser também criados colecionáveis digitais na forma, por exemplo, de gatos virtuais, cada um com propriedades únicas registradas na *Blockchain*, como foi o caso dos *CryptoKitties* no ano de 2017, uma das primeiras aplicações que popularizaram a tecnologia, em que cada NFT tem traços (*traits*) de diferentes graus de raridade e é possível combinar um NFT com outro para produzir (*breed*) um terceiro NFT exclusivo, com características raras herdadas dos pais.

Figura 7. Gato virtual registrado na *Blockchain* da Ethereum

Fonte: Disponível em: https://opensea.io/collection/cryptokitties

Atualmente, o processo de verificação da propriedade de ativos físicos e digitais é um componente integral da maioria dos negócios e sistemas. O uso de NFTs, portanto, implementa esse modelo em uma rede *Blockchain*, simplificando as transações e removendo intermediários.

Além disso, o uso de contratos inteligentes permite aos criadores dos NFTs escreverem linhas de código definindo regras que reflitam o funcionamento do mundo real. Assim, os aplicativos NFT podem melhorar a eficiência da economia digital.

Outra vantagem do uso de NFTs é a possibilidade de implementar o conceito de royalties, de forma que o NFT pague automaticamente ao seu criador quando for vendido. Assim, o uso

combinado de *Blockchain*, contratos inteligentes e NFTs tem o potencial de criar uma nova economia em diversos setores, sejam públicos ou privados.

O setor público pode, por exemplo, criar uma aplicação em *Blockchain* para registro de imóveis pelas construtoras na forma de NFTs, substituindo o papel de criar certificados de autenticidade dos cartórios. Nesse cenário, há a possibilidade de arrecadação automática de imposto sobre a transmissão de bens imóveis, bem como sobre a propriedade do imóvel em determinada data. As construtoras também podem ter o interesse de registrar um prédio nessa rede *Blockchain* como uma coleção NFT de apartamentos, de modo que receba royalties nas vendas futuras dos apartamentos, substituindo e reduzindo os custos notariais e de corretagem.

6. RBB – REDE *BLOCKCHAIN* BRASIL

No levantamento realizado pelo TCU em 2020, que resultou no Acórdão nº 1.613/2020-TCU-Plenário (Rel. Min. Aroldo Cedraz)[1], foi discutido como as tecnologias descentralizadas poderiam ser utilizadas como camada comum e confiável para compartilhamento de informações entre diferentes esferas de governo (municipal, estadual e federal), indústria e sociedade, e até entre países.

Asseverou-se no trabalho de levantamento supracitado que, no futuro, a função de autoridade centralizada exercida pelo governo poderia evoluir para descentralização. Com uso de *Blockchain*, cria-se a oportunidade de descentralização de transações de interesse público de forma colaborativa. Com isso, ganha-se em transparência e rastreabilidade, permitindo-se que os mais diversos setores da sociedade participem ativamente dos processos de auditoria ou de interesse público, possibilitando o surgimento de novos arranjos institucionais.

Além disso, discutiu-se como a tecnologia *Blockchain* poderia ser utilizada no combate a fraude e corrupção, como controle tanto preventivo quanto detectivo. A utilização das tecnologias distribuídas permite a criação de trilhas de auditoria para rastrear operações de governo, além de favorecer a abertura de dados. Assim, o fato de cada participante da rede manter seu próprio registro atualizado das transações aumenta a confiabilidade e reduz as oportunidades de fraude, dificultando a ocorrência de delitos e comportamentos antiéticos.

1 O levantamento realizado pelo TCU no âmbito do TC (TC 031.044/2019-9) teve por objetivo conhecer os conceitos da tecnologia *Blockchain*, identificar as áreas de aplicação e os tipos de problema que os governos do Brasil e de outros países estão resolvendo, bem como compreender o potencial disruptivo que tem na melhoria dos serviços digitais da administração pública sob a ótica da desburocratização e combate à corrupção. Foram identificados também os principais riscos e fatores críticos de sucesso, além de identificar os desafios e oportunidades para o controle externo. Participaram do levantamento os autores do presente artigo e in memorian Francisco Osório de Carvalho Ramos.

Nesse contexto, a criação da Rede *Blockchain* Brasil (RBB) nasce como ambiente de infraestrutura de execução para as mais diversas aplicações de interesse público. É uma "estrada" por onde passarão soluções inovadoras que permitirão o compartilhamento de dados e execução de contratos inteligentes, que serão habilitadores de aplicações voltadas à descentralização, com a participação ativa dos entes governamentais e sociedade, provendo maior transparência e controle social. A iniciativa tem por objetivo a remoção de barreiras de entrada às entidades interessadas, criando infraestrutura comum e habilitadora, reduzindo custos e prazos. Ademais, insere-se no esforço de construção de infraestrutura digital do país, em formato novo, aderente à era da sociedade em rede, consubstanciando-se em uma plataforma de inovação de negócios para o governo e sociedade. A RBB poderá ser a infraestrutura onde aplicações possam ser desenvolvidas para otimizar serviços e assegurar a transparência dos gastos públicos.

A RBB foi fundada pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES) e o Tribunal de Contas da União (TCU), por meio do Acordo de Cooperação nº 121.2.0014.22, assinado em 12/04/2022.

Em 2019, o BNDES e outras instituições públicas, que já faziam uso da tecnologia *Blockchain*, perceberam, em workshop realizado naquele banco de desenvolvimento, que havia duplicação de esforços na adoção da tecnologia *Blockchain* para propósitos parecidos. Observou-se que cada organização interessada na construção de aplicações com uso de *Blockchain* precisava superar barreiras legais, organizacionais e técnicas. Em muitos casos em que as aplicações em *Blockchain* têm caráter empresarial, o uso de infraestrutura comum não faz sentido, mas para aplicações de interesse público, uma plataforma comum para uso de *Blockchain* é bem-vinda. Foi para este último cenário que a RBB foi concebida.

A RBB foi inspirada em iniciativas internacionais que tiveram o mesmo propósito, como a **LACChain** - rede *Blockchain*/DLT para a América Latina e Caribe, liderada pelo Banco Interamericano de Desenvolvimento - **BID** (rede lançada em 2018), Alastria - rede *Blockchain* da Espanha (criada em 2017) e **EBSI** - European *Blockchain* Services Infrastructure, rede da Comissão Europeia (criada em 2018).

Assim como as redes citadas, a RBB busca a implementação de infraestrutura *Blockchain* do tipo permissionada, onde os nós participantes do consenso precisam de autorização (permissão) para participar, e ao mesmo tempo, pública, já que teoricamente qualquer entidade de interesse público poderá acessar a rede. As redes público-permissionadas aproveitam a transparência descentralizada das redes públicas e o baixo custo das transações das redes permissionadas, permitindo a participação engajada de entidades que promovam soluções de interesse público. Importante destacar que, nas redes totalmente públicas, como a rede Ethereum Mainnet, a inclusão de novos blocos de transações, advindos do protocolo de consenso adotado, gera custos em criptomoeda ao participante proponente da transação, situação que não ocorre com a RBB, onde os participantes do consenso são permissionados e o protocolo de consenso (validação) não gera custos em criptomoedas, somente custos de infraestrutura e operação dos nós.

Outra vantagem da adoção compartilhada da infraestrutura *Blockchain*, proposta pela RBB, é o possível compartilhamento de serviços na rede. Serviços de identificação e autenticação de documentos (notarização) são exemplos de contratos inteligentes que podem ser compartilhados, fornecendo uma base de serviços comuns, reduzindo custos e dando uniformidade de comportamento às transações. Além dos serviços, dados podem ser compartilhados entre as diversas transações, possibilitando integração das aplicações dos diversos participantes.

O acordo de cooperação firmado entre BNDES e TCU estabelece um Regulamento da Rede (em construção) e um arcabouço de governança. A governança da rede ocorre em dois comitês, sendo um Comitê de Governança e o outro, Comitê Técnico. Ainda, o acordo de cooperação estabelece três tipos de partícipes na RBB: parceiros, associados e patronos.

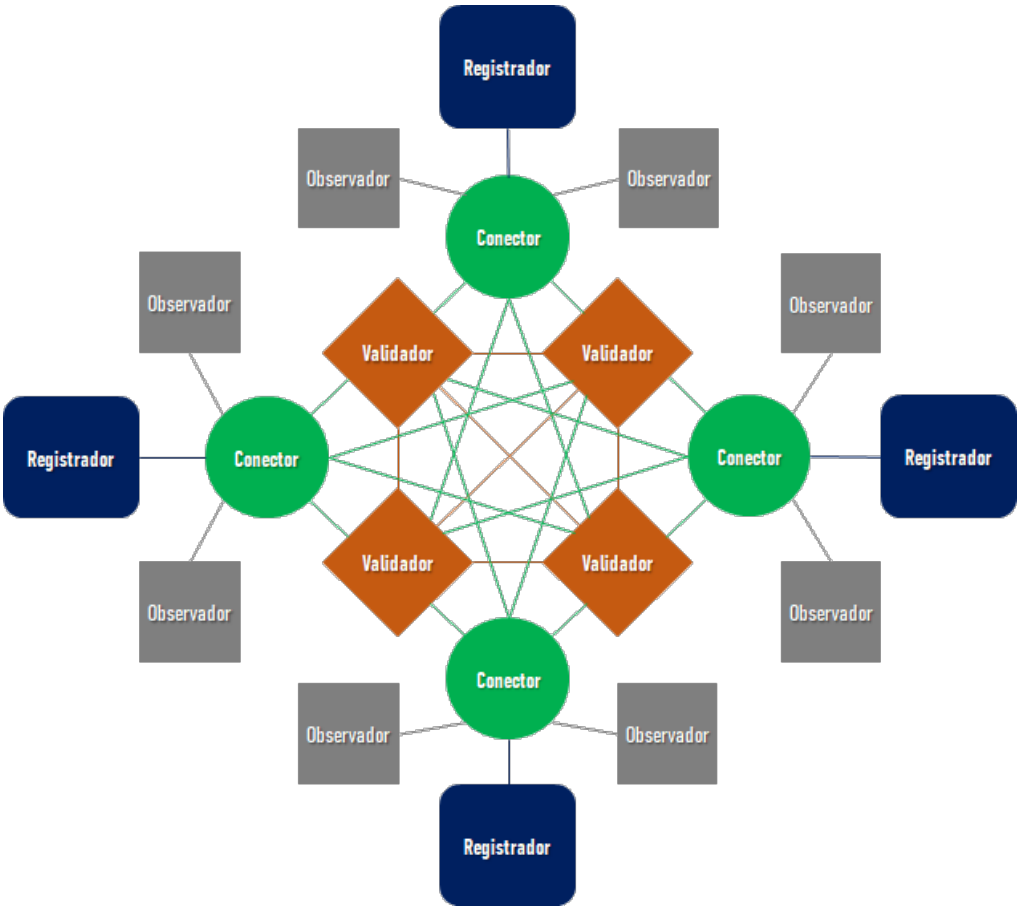
Os partícipes **Parceiros** podem enviar transações para a rede através de seus próprios nós. Também podem apresentar propostas e participar das reuniões dos comitês. Os partícipes **Associados** têm o mesmo direito dos partícipes Parceiros, e ainda podem executar nós que participam do protocolo de consenso da rede (tendo o compromisso de manter esses nós ativos sob um certo acordo de nível de serviço) e votar nas reuniões dos comitês. Já os partícipes **Patronos**, no caso o TCU e BNDES, têm os mesmos direitos e deveres dos partícipes Associados, além de direito a voto de desempate e veto nas propostas apresentadas aos comitês.

A RBB está sendo implementada com o uso da tecnologia *Ethereum*, mais especificamente, adotando-se como plataforma o software de código aberto *Hyperledger* Besu. Vale destacar que redes *Blockchain* baseadas em Ethereum suportam a execução de contratos inteligentes (*Smart Contracts*), requisito fundamental para a habilitação das aplicações candidatas a execução na RBB. O fato de a RBB usar *software* baseado em *Ethereum* não significa que outras redes futuras não poderão ser implementadas usando outras tecnologias. Conforme a evolução do uso da rede e da implantação das possíveis aplicações, outras plataformas de *Blockchain* podem ser utilizadas.

Quanto à topologia de rede, com forte inspiração na rede LACChain, a RBB é composta de nós de núcleo e nós-satélites. O nós de núcleo são nós do tipo conectores e validadores; já os satélites são nós do tipo registradores e observadores.

O núcleo da rede é responsável por executar o protocolo de consenso, gerando novos blocos para a rede, e ainda é responsável por admitir os nós-satélites na rede, através dos nós conectores. Nós conectores são responsáveis ainda por repassar os novos blocos aos demais nós-satélites (registradores e observadores), lembrando que todos os nós em uma rede *Blockchain* mantém uma cópia integral de todas as transações, ou blocos de transações (*ledger*). Os nós-satélites do tipo registradores podem enviar transações à rede (*writer nodes*), sempre se conectando à rede por nós conectores do núcleo. Já os nós do tipo observadores somente leem transações da rede. A Figura 8 resume a topologia da RBB.

Figura 8. Topologia da Rede Brasil *Blockchain* (RBB)



Fonte: Disponível em: https://github.com/RBBNet/rbb

A RBB funciona atualmente (setembro/2022) em caráter de laboratório e em processo de admissão de partícipes que formarão a rede de produção em breve. Alguns órgãos e entidades em processo de admissão são: RNP, Dataprev, Serpro, Prodest, Prodemge e PUC-Rio.

7. *BLOCKCHAIN*, AUDITORIA E CONTROLE

Com a aplicação da tecnologia *Blockchain* nas instituições públicas e privadas, os custos de transação e comunicação devem ser reduzidos, acarretando o surgimento de novos tipos de auditorias (DREW, 2018). À medida que as organizações investirem nessa nova plataforma digital com o objetivo de transformar as práticas tradicionais em novas abordagens de negócios e de prestação de serviços, haverá um novo campo para a profissão de auditor dentro desse novo ecossistema, fornecendo novos serviços de asseguração e auditoria.

As DLTs têm o potencial de se tornarem, por exemplo, a infraestrutura para um sistema de votação eletrônica, o registro de ativos digitais, a assinatura digital e a transmissão de dados seguros. Como os dados armazenados no *blockchain* são assegurados por várias partes e atualizados continuamente, ele oferece às equipes a possibilidade de relatórios em

tempo real tanto para a administração quanto para auditoria interna e auditores externos (TAPSCOTT, 2016).

Dessa forma, os serviços contábeis, fiscais e organizacionais precisam ser atualizados de acordo com essas mudanças inovadoras, enquanto, ao mesmo tempo, a abordagem de auditoria precisa também seguir essa atualização. Com a ampla aplicação da tecnologia *Blockchain*, novos objetivos e abordagens precisam ser definidos para o profissional de auditoria.

A *Blockchain* pode levar as firmas de auditoria a criarem oportunidades potenciais para desenvolverem novos serviços, mas também afetar serviços existentes, que serão total ou parcialmente substituídos por sistemas tecnológicos (APPELBAUM et al., 2017). Conscientes do potencial de desenvolvimento muito significativo dessa tecnologia, as maiores empresas de auditoria estão investindo mais de US$ 3 bilhões por ano nela (SMITH, 2018).

Como exemplo, a Ernst & Young (EY), primeira empresa a aceitar *Bitcoin* para seus serviços de consultoria em 2017, investiu no desenvolvimento de aplicativos e serviços para facilitar o uso da tecnologia *Blockchain* em seus negócios. A KPMG lançou novos serviços baseados em *Blockchain* com seu parceiro Microsoft para auxiliar as empresas na implementação de processos de negócios (KPMG, 2017). A Deloitte criou o primeiro laboratório de *Blockchain* em 2016, enquanto a PWC lançou serviços de ativos digitais em 2016 usando a tecnologia *Blockchain*.

As entidades fiscalizadoras públicas também precisam criar metodologias para as atividades de auditoria, especialmente para construir uma abordagem de auditoria para esse novo mundo de gerenciamento de dados em tempo real. A auditoria pode concentrar-se mais avaliando e dando garantia à confiabilidade de uma *Blockchain* do que nos dados em si.

O acesso a informações em tempo real por meio de *Blockchain*s pode apresentar uma oportunidade maior para aplicar análises de auditoria, embora os auditores ainda precisem avaliar a adequação das avaliações, das classificações e dos reconhecimentos da administração, entre outros assuntos complexos (ORTMAN, 2018).

A *Blockchain* cria mudanças significativas na transformação de entrada-processamento-saída das informações de uma organização. Em vez de usar documentos impressos como entradas, as transações serão coletadas entre várias partes em uma rede on-line. As organizações que fazem parte da cadeia farão parte do banco de dados compartilhado e poderão obter uma cópia idêntica das transações. Assim, o ciclo do processo da informação muda consideravelmente, uma vez que a *Blockchain*, associada com outras tecnologias digitais, pode mudar o processo de auditoria alterando a forma pela qual o auditor acessa e analisa os dados e coleta evidências (ROZARIO; THOMAS, 2019).

A natureza distribuída da *Blockchain* é a mudança mais significativa no ambiente institucional, uma vez que possibilita provar de forma digital segura quando ocorre uma transação. A transação de valor entre as partes também se descentraliza das estruturas econômicas tradicionais do ecossistema organizacional. Transferindo valores e informações entre as partes

sem qualquer intercessor agiliza o processo, usando um processador descentralizado e mantendo uma infraestrutura precisa, confiável e segura.

Em estudo qualitativo realizado com o objetivo de verificar como a inovação em *Blockchain* pode afetar a atividade de auditoria, Elommal et al. (2022) identificaram os seguintes aspectos principais de mudança :

- Economia de tempo e melhoria da eficiência das auditorias;
- Possibilidade de a auditoria cobrir toda a população em vez de uma auditoria baseada em amostras;
- Foco da auditoria na avaliação de controles em vez de avaliação de transações;
- Possibilidade da implementação de um processo de auditoria contínua;
- Papel mais estratégico da atividade de auditoria;
- Desenvolvimento de novos serviços de consultoria.

Dessa forma, vários são os aspectos em que a introdução da tecnologia *Blockchain* proporcionará mudanças no perfil da atividade de auditoria tanto interna quanto externa.

Já no relatório de levantamento sobre a utilização da *Blockchain* realizado pelo TCU (TC nº 031.044/2019-9), foram identificados os seguintes aspectos de transformação da atividade de auditoria, listados a seguir:

7.1 AUDITORIA CONTÍNUA E EM TEMPO REAL

Soluções distribuídas melhoram significativamente a governança e a transparência dos órgãos públicos, fornecendo à sociedade e aos órgãos de controle acesso imediato e irrestrito aos dados, proporcionando-lhes uma visão completa e confiável sobre operações do governo. Dessa maneira, a integração das atividades de auditoria com a operação de processos controlados por DLTs possibilita um monitoramento contínuo dos atos e gastos públicos.

Em vez de verificar as contas públicas após a apresentação anual de relatórios, será possível realizar avaliações *on-line* e contínuas durante todo o período de fiscalização (GENEST, 2018; PSAILA, 2017). A coleta contínua de evidências aprimora a auditoria, reduzindo o intervalo de tempo entre a ocorrência do evento e o procedimento de auditoria (APPELBAUM, 2017).

Além disso, o tempo de planejamento para obter informações das fontes e para verificar as transações também é reduzido. Com a informação disponível via *Blockchain*, os auditores podem implantar mais recursos de automação, análise e aprendizado de máquina, como alertar automaticamente a Administração Pública sobre transações incomuns ou suspeitas quase em tempo real (CPA, 2017).

7.2 MUDANÇA DE PARADIGMA DE AUDITORIA BASEADA EM AMOSTRA PARA AUDITORIA BASEADA EM TODO O UNIVERSO DE DADOS

Em uma auditoria, deve-se delimitar a amostra a ser examinada e definir o respectivo critério de seleção, o período abrangido e o seu tamanho, sendo que as conclusões generalizadas a partir da amostra selecionada embutem um certo grau de incerteza inerente aos cálculos estatísticos.

Com a utilização de *Blockchain*, os testes substantivos baseados em amostras poderão ser substituídos, uma vez que será possível examinar e testar todo o universo de dados dentro do período em observação, com base na cópia local do livro-razão. Essa extensa cobertura melhorará o nível de segurança obtido nos trabalhos de auditoria realizados, sem a necessidade de solicitar ao jurisdicionado a base completa de dados (PSAILA, 2017).

De acordo com o *International Telecommunication Union*, a melhor prática sugerida para obter uma cópia do livro-razão será utilizar um nó de auditoria na rede. No entanto, para auditar transações a partir de um nó de auditoria, outros elementos, conforme o caso de uso, precisam ser considerados e endereçados. Por exemplo, como as informações na transação podem ser criptografadas, as chaves para decriptografar devem estar acessíveis para a função de auditoria. Além do mais, a regulamentação pode definir requisitos específicos, que precisam ser auditáveis na *Blockchain* (ITU-T, 2019).

7.3 AUDITORIA AUTOMATIZADA

Como autoridades que certificam a conformidade das operações, os auditores também podem ser substituídos por um sistema *Blockchain*. Quando uma instituição lida com todas as suas transações por meio de um sistema *Blockchain*, uma vez que todas as transações são validadas de forma descentralizada em tempo real, elas podem ser confiáveis por aqueles que concordam com a utilização da tecnologia. Uma auditoria central adicional pode ser considerada dispensável. No entanto, as potenciais vantagens e os riscos das *Blockchain*s para a auditoria ainda são pouco explorados (DAI, 2017).

Dessa forma, as instituições que usam a tecnologia *Blockchain* podem questionar se a auditoria formal ainda é ou não necessária. Como todas as transações de *Blockchain* já são aprovadas descentralizadamente por vários participantes, eles são considerados transparentes, seguros e confiáveis. A certificação por terceiros pode não ser mais necessária (DAI, 2017), e auditorias adicionais podem se tornar obsoletas.

Por outro lado, uma vez que os mecanismos de governança, gerenciamento de riscos e controle estão associados à *Blockchain*, e não especificamente a um sistema ou organização (ROONEY et al., 2017), os auditores podem desenvolver procedimentos e rotinas de auditoria para obter evidência diretamente da aplicação *Blockchain* de forma automatizada. Por exemplo, a necessidade de reconciliar dados contábeis em vários bancos de dados é eliminada, economizando tempo e reduzindo substancialmente o risco de erro humano.

Assim, o trabalho do auditor será aprimorado pelo uso de consultas ao banco de dados, automação de relatórios, detecção automática de características de fraude e outras. O TCU poderá, por exemplo, automatizar seu trabalho definindo alertas no sistema que avisam os auditores em caso de preço excessivo antes que a transferência de valores ocorra. Essa capacidade aumenta a percepção de risco das agências, por serem continuamente auditadas (aumento da expectativa de controle), o que leva a níveis mais baixos de corrupção (OLIVEIRA, 2017).

7.4 NOVOS CONHECIMENTOS EXIGIDOS PARA O AUDITOR

O ceticismo profissional deve ser mantido na condução de uma auditoria de um sistema *Blockchain*. Por ser uma nova forma de registro em ambiente digital, cada sistema *Blockchain* pode ter características diferentes que precisam ser levadas em consideração, de forma que ele pode trazer novos riscos totalmente diferentes dos métodos atuais de auditoria (SADU, 2018). Fiscalizar um objeto que utiliza tecnologia inovadora pressupõe que os auditores devam compreender os riscos específicos dessa tecnologia e como a entidade auditada está respondendo a esses riscos por meio da implementação de controles.

No que diz respeito às DLTs e ao *Blockchain*, os profissionais devem adquirir habilidade e proficiência sobre questões técnicas e componentes críticos da tecnologia, tais como: sistemas distribuídos, redes, segurança, criptografia, gerenciamento de chaves e controles e processos de tecnologia. Também é desejado que o auditor tenha a capacidade de entender e avaliar a confiabilidade do protocolo de consenso e se ele pode ser manipulado ou subvertido.

O uso crescente de contratos inteligentes e NFTs, possivelmente, exigirá o entendimento da linguagem de programação técnica para verificar se os acordos, as normas contábeis e outros regulamentos codificados implementam corretamente a lógica de negócio. Assim, o auditor também deve possuir conhecimento do negócio e da legislação aplicada, considerando a gestão descentralizada dos processos.

Blockchain aumentará a quantidade de informação disponibilizada pelas organizações, de modo que caberá ao auditor planejar sobre como e quais evidências podem ser coletadas de acordo com padrões profissionais, bem como deverá estar apto a acessar os dados em novos formatos oriundos da tecnologia de encadeamento de bloco.

Outra consideração é que os auditores, em algumas ocasiões, precisarão trabalhar em colaboração com as organizações para garantir que todos os requisitos sejam atendidos antes da implementação de uma *Blockchain* ou de um contrato inteligente (compliance by design), o que requer habilidades interpessoais.

7.5 AUDITORES DEVEM TER PERCEPÇÃO DA OCORRÊNCIA DE NOVOS TIPOS DE RISCOS E FRAUDES

Com a operação distribuída entre os nós participantes, a segurança do ambiente subjacente torna-se essencial para o funcionamento correto da rede. Assim, para estar em condições de

fornecer o nível necessário de confiança, os processos de auditoria precisam avançar ainda mais na avaliação da eficácia operacional dos controles internos de tecnologia e criptografia (PSAILA, 2017). Além disso, o risco de conluio de participantes em uma rede permissionada e vulnerabilidades em contratos inteligentes são novos pontos de atenção do auditor.

7.6 COMPLIANCE BY DESIGN

O termo compliance by design surge da necessidade de validar controles antes de a solução *Blockchain* ser concebida e executada, garantindo que as regras do que é permitido dentro e fora da rede estejam em conformidade com as leis e normas jurídicas (*BLOCKCHAIN*GOV, 2020).

Assim, haverá uma maior demanda para que os auditores participem do estágio de planejamento das aplicações baseadas em *Blockchain* juntamente com os auditados. Ao invés de atuar para encontrar irregularidades, contratos inteligentes serão escritos com intuito de que elas não ocorram. É muito mais fácil incorporar os aspectos de governança, gerenciamento de riscos e controles desde o início de um projeto do que adaptá-los após um problema ser identificado, de modo que os auditores devem avaliar se existem controles automatizados eficazes para validar as transações e as regras de negócio antes de publicarem um contrato inteligente (ROONEY, 2017).

7.7 NECESSIDADE DE VALIDAR INFORMAÇÕES *OFF-CHAIN*

Quando uma *Blockchain* transaciona ativos puramente digitais, como o token de uma criptomoeda, o livro-razão fornece fonte segura e confiável da verdade dos fatos. Porém, aplicações permissionadas podem utilizar a tecnologia para registrar transações que ocorrem no mundo físico, geralmente utilizando oráculos e contratos inteligentes. Nesses casos, o uso de uma *Blockchain* não fornece evidência adicional de que uma transação específica realmente ocorreu, pois não é garantida a proveniência do evento subjacente (APPELBAUM, 2017).

Mentiras registradas em uma *Blockchain* continuam sendo mentiras, elas apenas são agora mentiras imutáveis. Assim, essa situação leva a um questionamento: como o auditor pode ter certeza de que as origens de um evento representam verdadeiramente a realização de uma transação? Em outras palavras, uma transação registrada em *Blockchain* ainda pode ser fraudulenta, ilegal, não autorizada ou pode não ter ocorrido. Portanto, caberá ao auditor pesquisar mecanismos para reconciliar transações registradas em *Blockchain* e as transações reais, especialmente no que diz respeito a como as transações são iniciadas, processadas, registradas, reconciliadas e relatadas pelos participantes da *Blockchain* (CPA, 2017; SCHMITZ, 2019).

7.8 NOVOS DESAFIOS E OPORTUNIDADES

Um desafio com o qual o auditor precisará lidar é com o fato de que uma *Blockchain* provavelmente não será controlada exclusivamente pela entidade que está sendo auditada. Além disso, pode ser improvável que as empresas decidam registrar todas as transações na

Blockchain. Com apenas transações específicas do negócio sendo registradas, os benefícios de uma fiscalização contínua podem ser parcialmente obtidos (SCHMITZ, 2019).

Porém, mesmo que uma auditoria seja realizada em um ambiente em que toda a operação da organização seja registrada em *Blockchain*, a experiência do auditor ainda será requerida na seleção e na realização de testes de auditoria.

Haverá mudança na forma como se encontra a verdade das transações, e a forma como a governança da rede DLT é exercida será um dos principais fatores de observação do auditor. As evidências coletadas de redes com controles internos eficazes serão mais confiáveis do que as coletadas de redes com controles menos eficazes (APPELBAUM, 2017).

As fiscalizações potencialmente se tornarão mais orientadas a TI e mais prospectivas, com foco na prevenção de ocorrência de irregularidades, fraudes e corrupção. O uso de soluções DLT pelos auditados aumenta o comportamento transparente, forçando-os a divulgarem transações antes não registradas ou operações suspeitas, de modo que os órgãos de controle deverão prospectar meios para maximizar o valor das informações disponibilizadas em tempo real. Duas possibilidades são o uso de analytics e inteligência artificial (IA). Com a análise orientada a dados, os auditores poderão fornecer novas ideias para seus jurisdicionados (NATHALIE, 2019). Já o uso de IA junto com contratos inteligentes poderá prever irregularidades e outros desvios (SCHMITZ, 2019).

8. CONSIDERAÇÕES FINAIS

As tecnologias do ecossistema *Blockchain*, apesar do enorme potencial que podemos vislumbrar para sua aplicabilidade na área do controle, ainda apresentam desafios a serem superados pela comunidade de fiscalização. Tais desafios incluem não só a necessidade de capacitação e atualização contínua por parte dos auditores frente às constantes inovações tecnológicas na área, como também adequações normativas que porventura sejam necessárias para regulamentar o emprego de *Blockchain* na atividade de auditoria.

Por outro lado, entendemos que iniciativas como a Rede *Blockchain* Brasil podem ser um embrião para impulsionar maior transparência, divulgação e uso da tecnologia na Administração Pública como um todo.

REFERÊNCIAS

AMAZON. **Non-Fungible Tokens (NFTs) Explained**. Disponível em: https://aws.amazon.com/pt/*Blockchain*/nfts-explained/. Acesso em: 12 set. 2022.

ANTONOPOULOS, A. M. **A Internet do Dinheiro**. São Paulo: Rede Editora, v. 1, 2018. 124 p.

APPELBAUM, D., KOGAN, A., VASARHELYI, M. A. Big Data and Analytics in the Modern Audit Engagement: Research Needs, Auditing: **A Journal of Practice & Theory**, n. 36 v. 4, 2017. pp. 1-27. DOI: https://doi.org/10.2308/ajpt-51684

BERRYHILL, J.; BOURGERY, T.; HANSON, A. *Blockchain*s Unchained: *Blockchain* Technology and its Use in the Public Sector. **Oecd Working Papers On Public Governance**, n. 28, 2018. 53 p. DOI: http://dx.doi.org/10.1787/3c32c429-en.

BINANCE. **O que é um NFT?** Disponível em: https://www.binance.com/pt-PT/nft/what-is-nft. Acesso em: 12 set. 2022.

*Blockchain*Gov. **Relatório de atividades do BlockchainGov**. 2019. Disponível em: https://docs.google.com/document/d/1C3m0AGvZgHvoUgjG67Ve4VNai3kYr1nmpAbwcfJY5gs. Acesso em: 12 out. 2022.

BUTERIN, V. **A next-generation smart contract and decentralized application platform**. 2014. Disponível em: <http://*Blockchain*lab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf >. Acesso em: 13 out. 2022.

CHARTERED PROFESSIONAL ACCOUNTANTS OF CANADA (CPA) E ASSOCIATION OF INTERNATIONAL CERTIFIED PROFESSIONAL ACCOUNTANTS (AICPA). ***Blockchain* Technology and Its Potential Impact on the Audit and Assurance Profession**. 2017. Disponível em: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/*Blockchain*-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf. Acesso em: 12 out. 2022.

DAI, J.; VASARHELYII, M. A. Toward *Blockchain*–based accounting and assurance. **Journal of Information Systems**, n. 31, v. 3, 2017, pp. 5-21.

DREW, J. Paving the way to a new digital world. **Journal of Accountancy**, n. 6, v. 225, 2018. pp. 32-37.

ELLOMAL, N.; MANITA, R. How *Blockchain* Innovation could affect the Audit Profession: A Qualitative Study. **Journal of Innovation Economics & Management**, n. 37, v. 1, 2022/1. pp. 37-63. DOI: https://dx.doi.org/10.3917/jie.pr1.0103.

ETHEREUM. **Non-fungible tokens (NFT)**. Disponível em: https://ethereum.org/en/nft/. Acesso em: 12 set. 2022.

GENEST, I. **Canadian Audit And Accountability Foundation**. *Blockchain* and Audit: Overview of Potential Impacto on Legislative Audit. 2018. Disponível em: https://www.caaf-fcar.ca/en/performance-audit/research-and-methodology/research-highlights/3198-research-highlights-1. Acesso em: 12 out. 2022.

GREVE, F. et al. *Blockchain* e a Revolução do Consenso sob Demanda. In: **Minicursos do XXXVI do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)**. São Carlos-SP, 2018. 52 p. Disponível em: http://www.sbrc2018.ufscar.br/wp-content/uploads/2018/04/Capitulo5.pdf. Acesso em: 13 out. 2022.

ITU-T FOCUS GROUP ON APPLICATION OF DISTRIBUTED LEDGER TECHNOLOGY (FG DLT). T**echnical Report FG DLT D5.1**: Outlook on distributed ledger technologies. 2019. Disponível em: https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d21.pdf. Acesso em: 10 out. 2022.

KHAN, S. N.; LOUKIL, F.; GHEDIRA-GUEGAN, C. et al.. *Blockchain* smart contracts: Applications, challenges, and future trends. **Peer-to-Peer Netw**. Appl. 14, 2022. pp. 2901-2925. DOI: https://doi.org/10.1007/s12083-021-01127-0.

KPMG. **KPMG and Microsoft Announce New "*Blockchain* Nodes"**. 2017. Disponível em: https://home.kpmg/us/em/home/media/press-releases/2017/02/kpmg-and-microsoft-announce-new-*Blockchain*-nodes.html. Acesso em 13 out. 2022.

MULLIGAN, C. et al. *Blockchain* Beyond the Hype: **A Practical Framework for Business Leaders**. World Economic Forum. 2018. Disponível em http://www3.weforum.org/docs/48423_Whether_*Blockchain*_WP.pdf. Acesso em: 14 out. 2022.

NAKAMOTO, S. Bitcoin: A peer-to-peer eletronic cash system. **Bitcoin**. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 13 out. 2022.

NATHALIE, B. et al. The Potential Impact of *Blockchain* Technology on Audit Practice. **Journal Of Strategic Innovation And Sustainability**, [s.l.], v. 14, n. 2, 2018. 22 abr. 2019. North American Business Press. DOI: http://dx.doi.org/10.33423/jsis. v14i2.1370.

OECD. **The Tokenisation of Assets and Potential Implications for Financial Markets**. 2020. Disponível em: https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm. Acesso em: 14 out. 2020.

OLIVEIRA, L. C. Triple entry ledgers with *Blockchain* for auditing. International J**ournal Of Auditing Technology**, [s.l.], v. 3, n. 3, 2017. Inderscience Publishers. DOI: http://dx.doi.org/10.1504/ijaudit.2017.10007789.

ORTMAN, J. C. ***Blockchain* and the future of the audit**. Claremont Mckenna College. Seniour Thesis. 2018.

PSAILA, S. Deloitte. ***Blockchain*:** A game changer for audit processes. 2017. Disponível em: https://www2.deloitte.com/mt/en/pages/audit/articles/mt-Blockchain-a-game-changer-for-audit.html. Acesso em: 12 out. 2022.

REDE BLOCKCHAIN BRASIL. Disponível em: https://github.com/RBBNet/.

REVOREDO, T. Blockchain: Tudo O Que Você Precisa Saber. **Independently Published**, 2019. 408 p.

ROONEY, H.; AIKEN, B. ROONEY, M. Q&A. Is Internal Audit Ready for Blockchain? **Technology Innovation Management Review**, [s.l.], v. 7, n. 10, 2017 pp. 41-44, Carleton University. DOI: http://dx.doi.org/10.22215/t imreview/1113.

ROZARIO, A. M.; THOMAS, C. Reengineering the Audit with Blockchain and Smart Contracts. **Journal of Emerging Technologies in Accounting**, n. 16, v. 1, 2019. pp. 21-35.

SCHMITZ, J.; LEONI, G. Accounting and Auditing at the Time of Blockchain Technology: A Research Agenda. **Australian Accounting Review**, [s.l.], v. 29, n. 2, p. 331-342, 4 abr. 2019. Wiley. DOI: http://dx.doi.org/10.1111/auar.12286.

SILVA, M. M. L. Crimes da era digital. Rio de Janeiro. **Seção Ponto de Vista**, 1998. Disponível em: http://www.brazilnet.com.br/contexts/brasilrevistas.htm. Acesso em: 28 set. 2022.

SMITH, S. S. Blockchain Augmented Audit – Benefits and Challenges for Accounting Professionals. **Journal of Theoretical Accounting Research**, n. 14, v.1, 2018.

SZABO, N. **Formalizing and Securing Relationships on Public Networks**. First Monday, n. 2 v. 9. 1997. DOI: https://doi.org/10.5210/fm.v2i9.548.

SZABO, N. **Smart Contracts:** Building Blocks for Digital Markets, 1996. Disponível em: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. Acesso em: 13 out. 2022.

TAPSCOTT, A. Assurance, EY. **Retrieved from Ernst&Young.** 2016. Disponível em: https://www.ey.com/en_gl/assurance/how-Blockchain-could-introduce-real-time-auditing. Acesso em: 13 out. 2022.

The European Union Blockchain Observatory & Forum. **Blockchain for Government and Public Services**. 2018. Disponível em: https://joinup.ec.europa.eu/sites/default/files/document/2019-04/JRC115049%20Blockchain%20for%20digital%20government.pdf. Acesso em: 13 out. 2022.

WIKIPÉDIA. **Fungibilidade**. Disponível em: https://pt.wikipedia.org/wiki/Fungibilidade. Acesso em: 12 set. 2022.

YOUTUBE. (2022). Lançamento da Rede Blockchain Brasil (RBB). **YouTube**. Disponível em: https://www.youtube.com/watch?v=Mhm8buV3lVs. Acesso em: 10 out. 2022.