GRUPO I – CLASSE ___ – Plenário
TC 031.044/2019-0
Natureza: Relatório de Levantamento
Órgãos/Entidades: Agência Nacional de Aviação Civil; Banco Central do Brasil; Banco do Brasil S.A.; Banco Nacional de Desenvolvimento Econômico e Social; Caixa Econômica Federal; Empresa de Tecnologia e Informações da Previdência - Dataprev; Instituto Nacional de Tecnologia da Informação; Petróleo Brasileiro S.A.; Secretaria Especial da Receita Federal do Brasil; Secretaria Especial de Desburocratização, Gestão e Governo Digital; Serviço Federal de Processamento de Dados.
Representação legal: não há.

SUMÁRIO: LEVANTAMENTO DE AUDITORIA. IDENTIFICAÇÃO DE OPORTUNIDADES E RISCOS NA ADOÇÃO DA TECNOLOGIA *BLOCKCHAIN*/DLT. DESCRIÇÃO DE FATORES CRÍTICOS DE SUCESSO E ARVORE DE DECISÃO DE APOIO A GESTORES. POSSÍVEIS IMPACTOS PARA O CONTROLE. RECOMENDAÇÕES. ARQUIVAMENTO.

RELATÓRIO

Transcrevo o Relatório de Levantamento elaborado pela Secretaria de Fiscalização de TI (Sefti), à peça 55, e que contou com a anuência do corpo diretivo da unidade (peças 56 e 57):

2. "Introdução

2.1 Deliberação que originou a fiscalização

7. O Levantamento em tela foi autorizado por despacho do Ministro Relator Aroldo Cedraz, de 21/8/2019 (peça 2), decorrente de proposta de fiscalização apresentada pela Sefti no âmbito do TC 022.018/2019-0 (Administrativo).

2.2 Motivação

8. O termo 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" em uma lista de discussão da internet. O referido documento apresenta uma combinação criativa de diversos conceitos relacionados à computação que permitem realizar pagamentos online sem a necessidade de uma terceira parte confiável: redes peer-to-peer (P2P), serviço de timestamp distribuído, criptografia, assinatura digital, árvore de merkle, funções hash e ponteiros de hash, além de outras inovações.

9. Nota-se que o *bitcoin* é a primeira e mais famosa aplicação baseada em *blockchain*. Mas esses conceitos não devem ser confundidos. A *blockchain* é um conceito tecnológico, enquanto o *bitcoin* é um dos casos de uso para um tipo específico da tecnologia *blockchain*. Por curiosidade, o termo *blockchain* não foi mencionado explicitamente no artigo elaborado por Nakamoto, mas o conceito de uma estrutura encadeada de *hashes* criptográficos (ou resumos criptográficos), na qual cada elemento faz referência ao *hash* do bloco anterior, surgiu no artigo original do *bitcoin*.

10. A *blockchain* pode ser enquadrada como uma tecnologia de propósito geral, ou seja, uma tecnologia com características únicas e capazes de impactar drasticamente nas relações econômicas e sociais pré-existentes, bem como prover significativas melhorias e facilitar a criação de inovações em diversos setores da economia.

11. De acordo com Andreas Antonopoulos, a rede *bitcoin* (i.e., *blockchain*), tal como a internet, é considerada uma rede "burra", em seu interior, que apenas realiza transações com base em uma linguagem de *script* de verificação muito simples. Porém, é uma rede capaz de suportar dispositivos muito inteligentes na borda, o que a torna incrivelmente poderosa na medida em que transfere toda a inteligência para os periféricos. Dessa forma, qualquer usuário final pode construir aplicações no topo da rede sem a necessidade de autorização específica ou modificar o centro da rede, o que facilita a inovação.

12. A *blockchain* possui um aspecto disruptivo porque suas características especiais têm o potencial de trazer diversas melhorias para a criação e o aprimoramento dos serviços digitais. Os projetos de *blockchain* no setor público estão em estágio inicial e sujeitos a diversos riscos. Há um movimento internacional de governos e organizações estudando o potencial transformador da tecnologia e seu impacto na sociedade, visto que a *blockchain* acelera as transações digitais por meio da automatização da confiança, que até então dependia de uma terceira parte confiável.

13. Importante ressaltar que a *blockchain* do *bitcoin* proposta por Nakamoto só possibilitava transações monetárias. Dessa forma, não havia como adicionar condições mais elaboradas a essas transações. Em 2013, Vitalik Buterin propôs uma plataforma para o desenvolvimento de aplicações descentralizadas chamada *ethereum*. Com o suporte para contratos inteligentes (em inglês, *Smart Contracts*), elevou-se a um novo patamar a tecnologia *blockchain*, uma vez que agora era possível executar de forma autônoma e confiável um código (ou programa) acordado previamente por duas ou mais partes.

14. É preciso observar que a transformação tecnológica vai além da inovação trazida pelas *blockchain*s do *bitcoin* e *ethereum*. Segundo o Gartner, até 2023 a tecnologia *blockchain* suportará o movimento global e o rastreamento de dois trilhões de dólares de bens e serviços anualmente. A empresa de consultoria também afirma que a *blockchain* tem, no mínimo, o potencial de otimizar e, possivelmente, transformar de forma disruptiva os serviços públicos.

2.3 Objetivo, Escopo e Questões de Auditoria

15. O levantamento tem o intuito de conhecer os conceitos da tecnologia *blockchain* (Seção 3), identificar as áreas de aplicação (Seção 4) e os tipos de problema que os governos do Brasil e de outros países estão resolvendo (Apêndices I e II), bem como compreender o potencial disruptivo que tem na melhora dos serviços digitais da administração pública sob a ótica da desburocratização e combate à corrupção. Pretende-se também identificar os principais riscos e fatores críticos de sucesso (Seções 5 a 8), além de identificar os desafios e oportunidades para o controle externo (Seção 9). Destaca-se que os impactos da utilização de criptomoedas no mercado financeiro estão fora do escopo deste relatório.

16. Dessa forma, para direcionar os trabalhos de campo e alcançar os objetivos esperados, elaborou-se Matriz de Planejamento com as seguintes questões de auditoria:

> Q1 - Como a tecnologia *blockchain* pode ser vista por meio de estruturas de inovação e quais possibilidades existem para futuros desenvolvimentos no setor público?
>
> Q2 – Quais funcionalidades de uma *blockchain* podem atender a transformação digital no setor público e como o Brasil e governos de outros países estão lidando atualmente com os desafios desta nova tecnologia?
>
> Q3 – Quais são os benefícios e riscos esperados da tecnologia e quais são os impactos que podem surgir do uso da tecnologia na esfera pública?
>
> Q4 – Como a tecnologia impacta nas atividades de controle externo e auditoria?

2.4 Metodologia Utilizada

17. Inicialmente, cabe informar que os trabalhos foram realizados em conformidade com as Normas de Auditoria do Tribunal de Contas da União (NAT), definidas na Portaria-TCU 168/2011, e com o Roteiro de Levantamento, estabelecido na Portaria-Segecex 14/2019.

18. A fiscalização baseou-se nas técnicas de análise documental, nas quais a equipe de fiscalização buscou compreender o que é a tecnologia e quais suas áreas de aplicação por meio de fontes acadêmicas, como publicações científicas, e em sítios especializados, para levantar informações relevantes sobre o tema e responder às questões de auditoria.

19. Também foi feita inspeção *in loco* em vários órgãos da administração pública que possuem projetos relacionados à *blockchain*. Foram aplicados questionários aos gestores desses órgãos com o intuito de obter descrição integral do projeto (peças 40-53). A equipe de auditoria elaborou descritivo das aplicações vistas, o qual foi validado junto aos gestores (**Erro! Fonte de referência não encontrada.**).

20. Além disso, foram realizadas entrevistas com os seguintes especialistas da área, com o objetivo de identificar os principais benefícios e impactos da tecnologia no setor público:

Nome:	Descrição:
Tatiana Revoredo, Academia (peça 37)	Membro fundadora da *Oxford Blockchain Foundation*. *Blockchain Strategist* pela *University of Oxford*, e pelo *MIT*. Especialista em Mitigação de Risco Cibernético pela *Harvard University*. Autora dos livros "*Blockchain*: Tudo o que você precisa saber" e "*Cryptocurrencies in the International Scenario*".
William Veronesi Rocha, Dataprev (peça 38)	Gerente do Departamento de Inovação da Dataprev. Formado em Ciência da Computação pela PUC-MG e Especialista em Políticas Públicas e Gestão e Governança de TI.
Marco Tulio da Silva Lima, Serpro (peça 39)	Analista de Desenvolvimento do Serpro, Gestor de Produto *Blockchain*. Formado em Ciência da Computação pela PUC-Goiás e Especialista em Orientação a Objetos e Internet pela Universidade Uni-Anhanguera.

2.5 Benefícios Estimados da Fiscalização

21. Entre os benefícios estimados para esta fiscalização, podem ser mencionados:

a. Compreender o panorama geral sobre o estado da arte da tecnologia *blockchain* e os principais casos de uso no setor público do Brasil e no mundo, ou seja, como a tecnologia está sendo utilizada e quais áreas podem ser beneficiadas pela aplicação da tecnologia (Seção 3 e Apêndices I e II);

b. Subsidiar os gestores públicos com informações sobre a tecnologia, de modo que possam identificar possíveis casos de uso onde a tecnologia pode ser adotada na sua organização (Seções 3 e 4);

c. Maximizar os benefícios e chances de sucesso com projetos de tecnologias distribuídas no governo de modo que agreguem valor aos cidadãos, além de evitar contratações *blockchain* quando não é o caso ou com risco elevado, gerando economia ao evitar despesas desnecessárias (Seções 5-8);

d. Internalização de conhecimento sobre a *blockchain* no TCU, além de capacitar o Tribunal para avaliar os potenciais e riscos de tecnologias inovadoras (Seção 9);

e. Induzir uma reflexão sobre o potencial de utilização de ecossistemas de tecnologias descentralizadas no país, em prol da transformação digital (Seção 10).

22. Por oportuno, informa-se que o TCU está participando como colaborador da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA) na "AÇÃO 08/2020: Elaborar diagnóstico sobre as possibilidades de uso de tecnologias como *blockchain* no setor público", de modo que as conclusões deste trabalho subsidiarão a atuação dos indicados pela Corte no grupo técnico da ENCCLA (http://enccla.camara.leg.br/acoes).

3. Visão geral sobre *blockchain*

23. Este capítulo apresenta definições a partir de publicações técnicas e estudos acadêmicos sobre *blockchain* e *Distributed Ledger Technology* (DLT), além de abordar as principais características da tecnologia que podem contribuir com o processo de transformação digital do governo.

3.1 Conceito

24. De uma forma geral, uma *blockchain* é um software que funciona como um livro-razão distribuído pelos nós de uma rede. O que distingue esse livro-razão dos bancos de dados ou softwares tradicionais é sua natureza de resistência à adulteração, pois a alteração dos dados de um bloco requer a manipulação de todos os blocos anteriores.

25. Há várias outras definições para o termo *blockchain*. Apresentam-se a seguir diversos conceitos utilizados por entidades internacionais:

> *Blockchain*s são livros-razões digitais resistentes contra intrusões e com acesso não autorizado facilmente detectável por observadores, implementados de forma distribuída, normalmente sem uma autoridade central (banco, empresa ou governo). Em seu nível básico, *blockchain*s habilitam que usuários registrem transações em um livro-razão compartilhado dentro da comunidade, de forma que, considerando a operação normal da rede *blockchain*, nenhuma transação pode ser alterada após ser publicada (tradução livre) (*National Institute of Standards and Technology* – NIST).
>
> *Blockchain* é o tipo de livro-razão em que transações com troca de valores (na forma de cripto-ocorrências, *tokens* ou informações) são sequencialmente agrupadas em blocos. Cada bloco contém uma assinatura baseada no conteúdo exato (*strings* de dados) daquele bloco. O próximo bloco contém esta assinatura também, encadeando todos os blocos anteriores um ao outro, até o primeiro bloco. Blocos são registrados de forma imutável através de uma rede *peer-to-peer*, usando confiança na autenticação criptográfica e mecanismos de garantia (tradução livre) (*European Commission*).
>
> Tecnologia *blockchain* é uma forma de tecnologia distribuída de livro-razão, a qual atua como um registro (uma lista) aberto e autenticado de transações de uma parte para outra (ou múltiplas partes), que não são armazenadas por uma autoridade central. Em vez disso, uma cópia é armazenada por cada usuário rodando um software *blockchain* e conectado a uma rede *blockchain* – também conhecido como nó. Ao invés de uma autoridade central manter exclusivamente a base de dados, todos os nós têm uma cópia do livro-razão, sendo que as atualizações do livro-razão *blockchain* são propagadas através da rede em minutos ou segundos (tradução livre) (Organização para a Cooperação e Desenvolvimento Econômico – OCDE).

26. Sob um aspecto mais técnico, uma blockchain é uma estrutura de dados que armazena transações organizadas em blocos, os quais são encadeados sequencialmente, servindo como um sistema de registros distribuído. Cada bloco é dividido em duas partes: cabeçalho e dados. O cabeçalho inclui metadados como um número único que referencia o 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 abaixa ilustra como os blocos são sequenciados na *blockchain.* Informa-se que alguns campos do bloco foram omitidos:

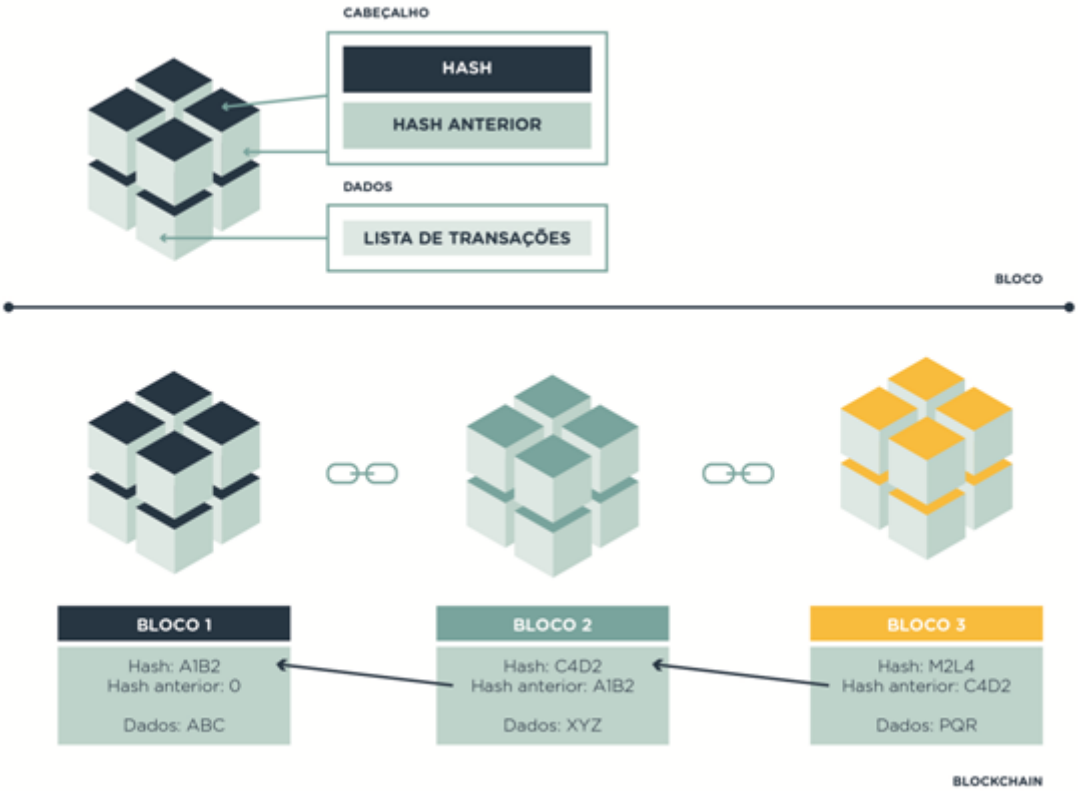

Figura 1 – Encadeamento de blocos na *blockchain*. Fonte ITU (adaptado).

27. 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 de *hash*. O cabeçalho possui um campo que armazena o resumo criptográfico (*hash*) do bloco imediatamente anterior, estabelecendo uma sequência única entre os blocos. Como cada bloco faz referência ao seu antecessor, se um bit do bloco anterior for alterado, o *hash* do bloco irá mudar e consequentemente haverá uma inconsistência na cadeia, que pode ser facilmente detectável. Por esse motivo, assume-se que a existência em uma cadeia de blocos encadeada garante a segurança e integridade das transações armazenadas.

28. A transação é a abstração de um evento de negócios que altera o estado de um livro-razão. Uma plataforma *blockchain* facilita a execução segura de uma transação no ambiente descentralizado e auditável. O mecanismo normalmente inclui o envio de uma mensagem assinada de uma conta para outra na *blockchain*.

29. À medida que as transações são encaminhadas ao sistema *blockchain*, um modelo de consenso é empregado para validar e determinar quais transações serão incluídas no próximo bloco a ser gerado e anexado ao livro-razão.

30. Cada novo bloco adicionado à *blockchain* contém algumas informações acessíveis para fornecer conhecimento público sobre a ação, a hora ou algum outro recurso do registro, criando uma transcrição pública de como as informações se desenvolvem.

31. Como a maioria dos softwares de *blockchain* é de código aberto, as regras que julgam os blocos e os dados de transação incluídos estão disponíveis para revisão. Para sistemas públicos de *blockchain*, os próprios dados estão disponíveis para observação direta por qualquer pessoa que necessite acessá-los. Isso torna os conjuntos de dados de *blockchain* percebidos como mais confiáveis por um número maior de usuários. A figura abaixo resume o funcionamento genérico de como uma transação é realizada em uma *blockchain*:

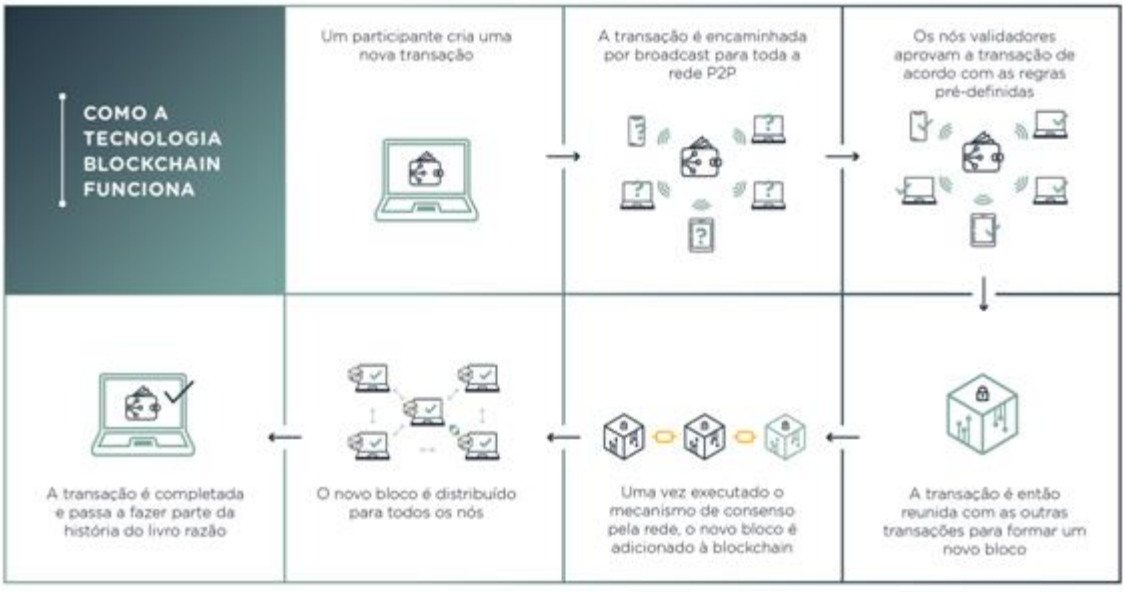

Figura 2 – Funcionamento genérico de uma *blockchain*. Fonte: Comissão Europeia (adaptado).

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

33. 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 direitos 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

algoritmos na rede. O diagrama a seguir exemplifica a diferença entre blockchain, DLTs e banco de dados tradicionais:

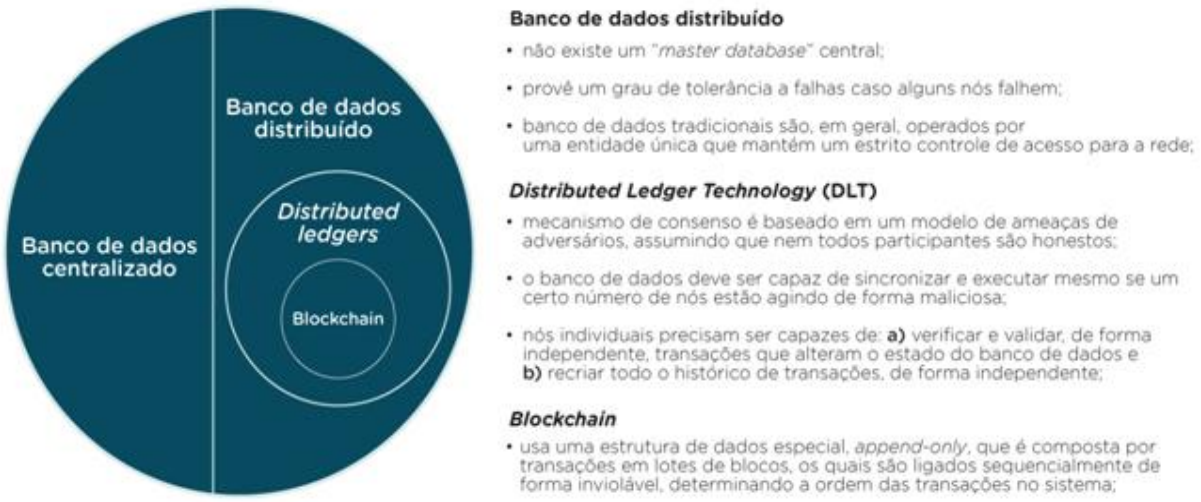

Figura 3 – Diferença entre tecnologias. Fonte: Universidade de Berkeley e Forum Econômico Mundial (adaptados).

3.2 Componentes da tecnologia *blockchain*

34. As implementações da tecnologia *blockchain* incluem tipicamente os seguintes componentes, os quais serão detalhados a seguir:

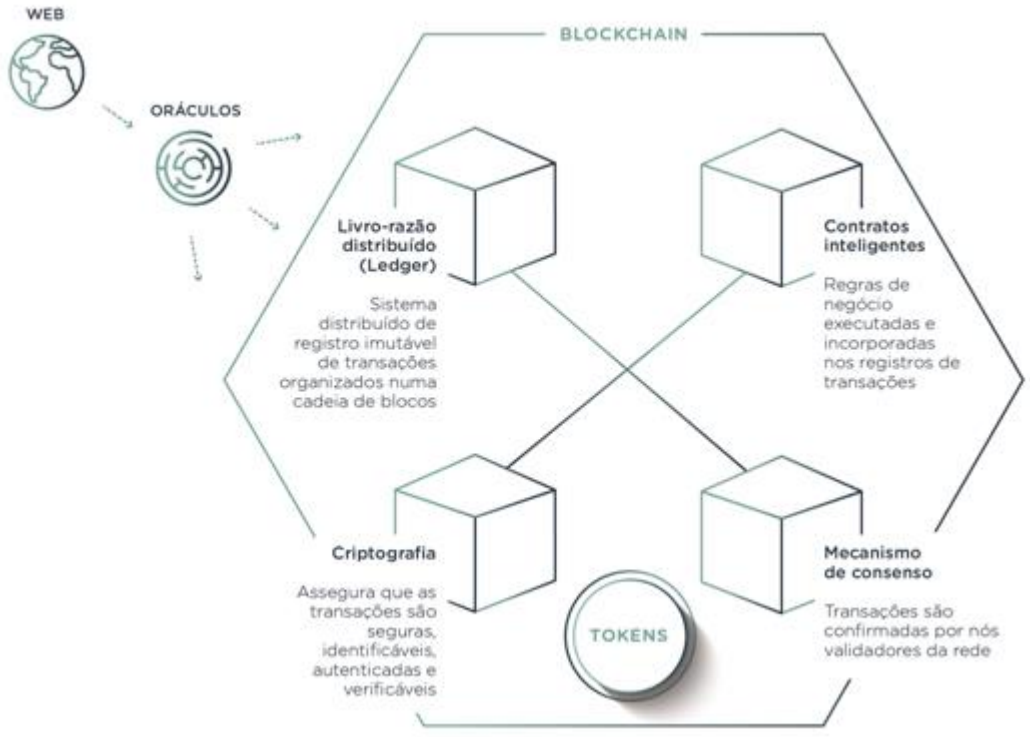

Figura 4 – Componentes da tecnologia blockchain.

3.2.1 Livro-razão distribuído (*Ledger*)

35. O livro-razão (*ledger*) é a estrutura de dados imutável, em que transações são registradas e o estado global do sistema é mantido. O livro-razão mantém-se completamente replicado em todos os nós da rede P2P. Logo, o livro-razão distribuído é replicado e imutável

36. Um livro-razão distribuído pode ser visto como um registro de transações ou contratos mantidos de forma descentralizada em diferentes locais, eliminando a necessidade de uma autoridade central para controlar o armazenamento dos dados.

37. Enquanto um livro-razão centralizado está propenso a diversos ataques cibernéticos, um livro-razão distribuído é mais difícil de atacar, porque todas as cópias distribuídas precisam ser atacadas simultaneamente para que um ataque seja bem-sucedido. Além disso, os registros distribuídos são resistentes a alterações maliciosas por um único participante da rede.

38. Destaca-se que o elemento de descentralização das tecnologias de livro-razão distribuído cria um sistema no qual todas as transações são compartilhadas, verificadas e aceitas por todas as partes, eliminando a necessidade de intermediários.

3.2.2 Mecanismos de consenso

39. O problema de se chegar ao consenso em um meio não confiável em que nós da rede podem falhar (por questões técnicas ou ataques maliciosos) é geralmente conhecido como Problema dos Generais Bizantinos. 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.

40. Daí surgem os chamados mecanismos de consenso, que são as regras e procedimentos pelos quais os nós de uma rede distribuída concordam em validar transações. Importante notar que acréscimos no livro-razão só são feitos se as regras ditadas pelo mecanismo de consenso são seguidas por todos.

41. 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. O mecanismo de consenso é responsável por permitir que os atores ou nós da rede concordem entre si com o conteúdo a ser armazenado na *blockchain*, levando em consideração o fato de que alguns atores podem ser maliciosos ou estarem indisponíveis. Isso pode ser atingido por diferentes maneiras, conforme as necessidades específicas de cada rede.

42. Importante notar que, para uma transação ser registrada em um livro-razão, ela primeiro precisa ser aprovada pelos nós validadores da rede, caso contrário, é automaticamente rejeitada. Isso ocorre da seguinte maneira: sempre que uma transação é encaminhada na rede P2P, os nós primeiramente validam a transação segundo regras pré-definidas. Se os nós concordarem com sua legitimidade, a transação é encaminhada para os outros nós validadores da rede e aguardam em um *pool* de transações. Um aspecto fundamental da tecnologia distribuída é determinar qual usuário adiciona o próximo 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*.

43. Cada algoritmo de consenso tem diferentes configurações de conflitos de escolhas (*trade-offs*, ver seção 3.4), que são otimizados para atender determinada necessidade. Cabe ao gestor avaliar que tipo de problema distribuído que precisa resolver com a utilização de solução DLT ou *blockchain* a fim de selecionar o mecanismo de consenso que se ajusta ao seu ambiente, em termos de escalabilidade do número de nós e transações, bem como quais e quantos serão os participantes da rede.

44. Uma descrição mais técnica sobre os algoritmos de consenso existentes é apresentada no **Erro! Fonte de referência não encontrada.**, deste relatório.

3.2.3 Contratos Inteligentes

45. Um contrato celebrado entre partes interessadas usualmente tem um conjunto de cláusulas (promessas) que são pactuadas e assinadas entre estas partes. Contratos são geralmente escritos pelas partes envolvidas, 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 a 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.

46. Contratos inteligentes, ou *smart contracts*, são código-fonte em linguagem de programação (*scripts*), que podem ser definidos e auto executados em uma infraestrutura de *blockchain* ou DLT. A definição e execução de um contrato inteligente nestes ambientes se dá sem a necessidade de intermediários.

47. O conceito de contrato inteligente foi definido por Nick Szabo, pesquisador em criptografia e especialista em Direito. Szabo define contrato inteligente em seus artigos como cláusulas contratuais embutidas em hardware e software, que tornam a violação destas cláusulas proibitiva sob o ponto de vista computacional e consequentemente econômico, portanto, não vantajosa a um possível violador.

48. Um outro conceito dado pela *International Telecommunication Union* (ITU) é que contrato inteligente é um programa de computador que utiliza transações assinadas criptograficamente em uma rede DLT. O contrato inteligente é executado pelos nós e os resultados da execução são validados por consenso e registrados no livro-razão distribuído. A automação inteligente de contratos reduz custos, reduz riscos de erros, mitiga riscos de fraude e, potencialmente, otimiza muitos processos de negócios.

49. Ainda segundo Szabo, um contrato inteligente pode ser caracterizado pelo atingimento de quatro objetivos principais: observabilidade, verificabilidade, privacidade e obrigatoriedade (imposição das regras contratuais):

> a. **Observabilidade:** a habilidade de verificar se as partes envolvidas no contrato cumpriram a sua parte, ou seja, se o resultado esperado segundo a lógica computacional do contrato inteligente foi alcançado;
>
> b. **Verificabilidade:** é a possibilidade de uma das partes envolvidas reclamar que o contrato foi cumprido ou violado. A verificação pode ser feita por uma terceira parte, como juízes, fiscais, auditores etc.;
>
> c. **Privacidade:** o conhecimento sobre o conteúdo e a execução do contrato deve ser distribuído apenas na medida certa, ou seja, o mínimo possível de dados deve ser compartilhado (apenas o necessário para a criação e execução do contrato);
>
> d. **Obrigatoriedade**: se dá pela própria natureza automatizada do contrato inteligente. O contrato é executado de forma obrigatória, em sua completude, conforme programado em seu código-fonte, sem margem para interpretações diversas.

50. Devido às suas características, DLTs são ambientes ideais para definição e execução de contratos inteligentes, tornando as ideias de Szabo aplicáveis. Observabilidade e verificabilidade são garantidas pelo alto grau de transparência proporcionado por DLTs. A privacidade pode ser conquistada por meio dos inerentes mecanismos criptográficos comumente presentes nas DLTs. Tais mecanismos, por outro lado, também permitem a garantia de integridade ou não adulteração, contribuindo para a obrigatoriedade da execução dos contratos.

51. O contrato inteligente é executado por envio de mensagem ao endereço do contrato em uma DLT, 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 DLT. O uso de blocos de dados encadeados, criptografia e algoritmos de consenso, entre outras tecnologias, dá sustentação aos contratos inteligentes.

52. A utilização de contratos inteligentes provê as seguintes vantagens:

> a. **Transparência:** contratos inteligentes podem ser escritos e verificados a qualquer momento por todas as partes envolvidas, que podem verificar o código-fonte do contrato. E o mais importante, a execução do contrato fica totalmente registrada, reduzindo o número de disputas judiciais em torno de sua definição e execução;
>
> b. **Menor prazo para execução:** intermediários humanos podem causar todo tipo de atraso na elaboração e execução de contratos. A eliminação dos passos manuais torna, portanto, a execução do contrato mais rápida e eficiente;
>
> c. **Precisão:** como o contrato é descrito por um algoritmo computacional, sua execução é precisa, salvo se houver erro de programação. Qualquer condição não cumprida no contrato

gera erro de execução. Contratos em papel podem dar margem a interpretações diversas, causando imprecisão;

d. **Segurança:** a infraestrutura de DLT garante a segurança em contratos inteligentes, que são assinados por chaves criptográficas e não podem ser violados por terceiros sem permissão de acesso;

e. **Rastreabilidade:** todos os dados, de cada execução das "funções" do contrato ficam armazenados na DLT, permitindo que a execução do contrato seja auditável a qualquer tempo;

f. **Menor custo:** por sua natureza digital e eliminação de intermediários, os contratos inteligentes reduzem os custos de execução;

g. **Confiança:** as características citadas acima levam à maior confiança entre as partes envolvidas no contrato.

3.2.4 Criptografia

53. Soluções baseadas em *blockchain* utilizam intensivamente técnicas tradicionais de criptografia para garantir a integridade das informações armazenadas. Como exemplo, pode-se citar a utilização de algoritmos criptográficos de chaves públicas, funções de *hash* e assinaturas digitais. O detalhamento dessas técnicas está fora do escopo deste relatório, tendo em vista que existem diversos livros e publicações especializados que já tratam sobre o tema. Nada obstante, no **Erro! Fonte de referência não encontrada.**, são apresentadas de forma sucinta as seguintes técnicas e protocolos de criptografia que ampliam as funcionalidades de uma *blockchain*: *Zero-Knowledge Proofs, Proof of existence,* e *Atomic Swap*.

3.2.5 *Tokens*

54. A tecnologia *blockchain* permite que todo tipo concebível de ativos, direitos e obrigações de dívida, relacionados a bens materiais e imateriais, seja representado por *tokens*, e sua negociabilidade e permutabilidade sejam potencialmente simplificadas.

55. Dessa forma *tokens* são utilizados para representar ou materializar um ativo do mundo real, ou mesmo um direito, como ações de uma empresa ou investimento, ou mesmo uma recompensa por um serviço. A definição de *tokens* no ecossistema de plataformas DLTs e *blockchain* é difusa. O termo acabou sobrecarregado e são encontradas inúmeras definições e classificações de *tokens*.

56. *Tokens*, em plataformas distribuídas, utilizam os mesmos princípios que são utilizados, por exemplo, em um voucher de viagem, um ingresso para um show, uma reserva em um restaurante, um cartão de embarque, um cartão de fidelidade de uma companhia aérea, ou até mesmo uma cédula ou moeda; tudo isso são representações de um direito, crédito, vantagem, benefício, ou qualquer outra coisa que represente valor.

57. Em plataformas DLTs, os *tokens* representam algo com valor no "mundo real" ou um direito de acessar produtos e serviços disponibilizados por outras pessoas, comunidade de pessoas ou empresas.

58. Atualmente não existe uma classificação unificada e aceita mundialmente a respeito de *tokens* criptográficos em DLTs. Porém, existem algumas iniciativas do Fundo Monetário Internacional (FMI), da *U.S. Securities and Exchange Commision* (SEC), entidade dos EUA que regula o sistema financeiro daquele país, e da *Swiss Financial Market Supervisory Authority* (FINMA), órgão suíço também voltado à regulação do mercado financeiro. Tais entidades propuseram uma classificação de *tokens*, que pode inclusive classificar *tokens* como híbridos, ou seja, que acumulam mais de uma classificação. Segundo estas entidades, os *tokens* podem ser categorizados como:

a. **Tokens de pagamento (*payment tokens*)**: são sinônimos de criptomoedas, utilizados tão somente para troca de valores entre partes em uma plataforma de *blockchain*;

b. **Tokens utilitários (*utility tokens*):** são *tokens* utilizados para provimento de acesso digital a uma aplicação ou serviço. Representa o direito de acesso, mas não a propriedade de um ativo;

c. **Tokens de ativos (*asset tokens*) ou *Security Tokens*:** representam ativos do mundo real como ações de uma empresa, direitos de dividendos ou direitos de recebimento de juros

sobre um investimento. *Security Tokens* também são *tokens* que representam um ativo sob o ponto de vista de valores mobiliários. A origem do nome advém da SEC, a qual define como *securities* os contratos de investimento em dinheiro, que visam lucro pelo trabalho de terceiros.

59. Ressalta-se que os primeiros sistemas de *blockchain*, tais como *bitcoin* e outras criptomoedas derivadas do *bitcoin*, foram projetos voltados exclusivamente para realizarem transferências de valores em moedas digitais, sendo que sua lógica de transação implementa um sistema baseado em *tokens*. A limitação desses sistemas é que apenas registram os saldos digitais associados a identidades ou endereços, juntamente com uma autenticação e as respectivas assinaturas digitais.

60. Por outro lado, sistemas baseados em contratos inteligentes têm a capacidade de implementar qualquer rotina de software, incluindo a lógica de *tokens* digitais. Isso abre a possibilidade para executar, de forma autônoma, lógicas complexas e fluxos de trabalho em código de computador com o qual todos os participantes autorizados podem examinar e concordar.

61. Por fim, uma outra classificação sobre *tokens* que merece ser citada é a utilizada pela OCDE. Para a organização, existe uma diferença entre *tokens* que representam ativos reais que existem fora da *blockchain* e os *tokens* que representam ativos nativos de uma *blockchain* ("*native tokens*").

3.2.6 Oráculos

62. *Blockchain*s e contratos inteligentes funcionam de forma independente do mundo externo e sem necessidade de uma autoridade central. Contudo, especialmente em *blockchain*s permissionadas, eventos do mundo exterior podem ter relevância no contexto das redes *blockchain*. Assim, pode haver a necessidade de um agente digital que funcione como um intermediário central de confiança sobre fatos externos à rede.

63. Um oráculo, no contexto de *blockchain*s, é um agente que localiza e verifica ocorrências do mundo real e envia essas informações para uma *blockchain*, a fim de serem usadas por contratos inteligentes. Os oráculos fornecem dados externos e acionam execuções de contratos inteligentes quando ocorrem condições pré-definidas.

64. Importante ressaltar que oráculos são serviços que não fazem parte do mecanismo de consenso da *blockchain*.Em outras palavras, são serviços que verificam ocorrências do mundo físico e enviam essas informações a contratos inteligentes, desencadeando mudanças de estado na *blockchain*.

65. Nota-se que um oráculo não é a fonte de dados em si, é uma camada que faz interface com as fontes de dados e a *blockchain*. Há de se ressaltar que, de um modo geral, os oráculos não fornecem as propriedades de segurança robustas dos protocolos *blockchain*, pois, diferentemente do que ocorre com as transações dentro de uma rede *blockchain*, os dados externos não são validados criptograficamente, de forma que podem apresentar respostas inconsistentes ou funcionamento incorreto, podendo ser um componente vulnerável do sistema.

3.3 Características da tecnologia *blockchain*

3.3.1. Hipertransparência e auditabilidade

66. 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 a um grau em que qualquer usuário pode auditar completamente todas as transações. Assim, considerando que, em regra, toda a informação do governo deve ser pública, o uso de *blockchain* está aderente à Lei de Acesso à Informação (LAI).

67. Para um nó participante, essa propriedade aumenta a confiança na rede e reduz comportamentos fraudulentos. Já para o governo, a possibilidade de visualizar *blockchain*s públicas das empresas ajuda a monitorar e regular mercados em que não seja um participante direto das operações. Do ponto de vista do cidadão, o fato de poder visualizar quando quiser os dados de *blockchain*s governamentais aumenta o controle social sobre as ações da Administração Pública.

68. Importante notar que, com a transparência ilimitada, qualquer organização pode identificar oportunidades, melhorar a tomada de decisão e rastrear o resultado dessas decisões. Essa é uma propriedade de proveniência das informações, pois todos os participantes da rede têm conhecimento de onde o ativo foi

originado e seu histórico de estados. Isso aumenta a expectativa do controle, o que pode diminuir fraude e corrupção.

69. Além disso, ainda que a hipertransparência seja um dos diferenciais de uma *blockchain*, é possível utilizar tecnologia subjacente em *blockchain*s privadas para criptografar informações e disponibilizá-las apenas para quem deva ter visibilidade, como em um cenário em que órgãos do governo colaborem com empresas e cidadãos, mas algumas informações pessoais devam ser mantidas em segredo pelas organizações públicas.

3.3.2. Integração de informações dentro e fora dos limites da administração pública – distribuído e descentralizado

70. Com o uso de uma *blockchain*, os dados são compartilhados em tempo real, além do histórico de modificações, fazendo com que não haja necessidade de reconciliação entre diferentes participantes, uma vez que os dados estão disponíveis a todos os nós e usuários da rede.

71. Dessa forma, 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 (governo hiperconectado).

3.3.3. Desintermediação e automação de transações e processos

72. A tecnologia *blockchain* introduz um novo paradigma: a possibilidade de diferentes partes transacionarem sem a necessidade de confiarem em um intermediário central. A existência de uma terceira parte confiável para resolver conflitos das transações não é mais necessária, pois agora o controle pode ser distribuído para todos os nós da rede de forma descentralizada.

73. Adicionalmente, reduz a necessidade de implementar processos complexos de reconciliação entre as partes e diminui custos, já que é possível também que contratos inteligentes da *blockchain* sejam executados automaticamente de acordo com regras pré-definidas.

74. Dessa forma, a tecnologia é uma alternativa para processos que têm elevados custos de intermediação, fazendo com que o gestor público possa rever qual é o valor agregado que o intermediário produz e se é realmente necessário.

3.3.4. Não existe ponto único de falha - disponibilidade

75. Um livro-razão contém o estado compartilhado e acordado da *blockchain*, que representa todas as transações processadas pelos nós. Cada nó neste sistema descentralizado possui uma cópia do livro-razão, que é continuamente sincronizada com a rede. Dessa maneira, não há um ponto central de vulnerabilidade que agentes maliciosos possam explorar, de modo que derrubar um nó não levará a uma quebra da cadeia de blocos. Essa arquitetura P2P típica contribui para a segurança.

76. Como todos os participantes têm uma cópia local sincronizada com a rede, isso quer dizer que, se um nó ficar 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 poderão continuar em operação mesmo que alguns nós não estejam disponíveis.

77. Além disso, o trabalho para um agente malicioso derrubar a rede como um todo é dificultado, pois terá que violar o livro-razão de cada um dos nós participantes.

3.3.5. Log imutável e integridade das informações – imutabilidade e integridade

78. 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.

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

80. É importante notar que, especificamente em uma rede permissionada, como uma entidade ou um grupo tem a prerrogativa de controlar a rede, não há verdadeira certeza se um registro ou contrato inteligente não foram alterados após o fato. Para essas redes é importante notar que a imutabilidade absoluta não existe,

pois, em teoria, a história do livro-razão pode ser alterada caso nós suficientes ajam em conluio, embora isso seja detectável por nós honestos da rede.

3.3.6. Autenticação das transações - irrefutabilidade

81. Uma das funcionalidades essenciais das tecnologias *blockchain* é o uso da criptografia de chaves públicas (ou assimétrica), que serve como uma base para a autenticação dos usuários da rede. Com o uso de um método que utiliza a chave privada do seu par de chaves e funções de *hash*, um participante é capaz de realizar assinaturas digitais sobre as transações, servindo como uma prova inegável de que é o emissor de determinada mensagem (não repúdio).

3.4 Conflitos de escolha (*trade-offs*) em um sistema com arquitetura *blockchain*

82. Como decorrência de uma arquitetura P2P distribuída, em que os nós cooperam entre si para prover serviços um ao outro, sem a necessidade, *a priori*, de um servidor central, um sistema baseado em *blockchain* enfrenta alguns *trade-offs* que devem ser avaliados cuidadosamente pela área de TI, os quais serão abordados a seguir.

83. O trilema da escalabilidade, termo cunhado por Vitalik Buterin, criador da *ethereum*, refere-se ao problema de encontrar a estratégia mais eficiente entre os três fundamentos de *blockchain*: escalabilidade, descentralização e segurança.

84. Já na teoria relacionada a sistemas distribuídos, o Teorema CAP, atribuído a Eric Brewer, é outro conhecido trilema aplicado, que representa o antagonismo entre consistência (*safety*) e progresso (*liveness*) nos sistemas tolerantes a falhas. A sigla CAP refere-se a três componentes (em inglês): consistência (*consistency*), disponibilidade (*availability*) e tolerância ao particionamento (*partition tolerance*). O Teorea CAP afirma que um sistema pode possuir no máximo duas das três propriedades citadas, em qualquer momento.

Figura 5 – Teorema CAP

3.5 Tipos de *blockchain*

86. Segundo a Comissão Europeia[Erro! Indicador não definido.], as diferentes arquiteturas adotadas por uma *blockchain* podem ser classificadas de acordo com a abertura quanto à validação das transações e à participação na realização de transações. Assim, são descritos na literatura os seguintes tipos:

86.1. Quanto à validação das transações:

a. **Não permissionada**: qualquer um dos nós que compõe a rede distribuída tem permissão para validar ou confirmar transações.

b. **Permissionada**: apenas alguns nós selecionados podem validar ou confirmar transações. Comumente encontrada em ambientes corporativos e na administração pública.

86.2. Quanto à autorização para realizar transações:

a. **Pública**: neste tipo, qualquer um dos nós que compõem a rede pode participar de transações.

b. **Privada**: em *blockchain*s privadas, apenas participantes selecionados podem participar em transações.

87. Dessa forma, podem ser enumerados quatro tipos principais de *blockchain*: *blockchain*s permissionadas públicas, *blockchain*s não permissionadas públicas, *blockchain*s permissionadas privadas e *blockchain*s não permissionadas privadas.

Tipo de *blockchain*	Explicação
Pública não permissionada	Qualquer um pode participar do mecanismo de consenso da *blockchain*. Além disso, qualquer um com conexão à internet é capaz de realizar transações e visualizar todo o *log* de transações.
Pública permissionada	Qualquer um com conexão à internet é capaz de realizar transações e visualizar o log de transações, mas apenas uma parte restrita dos nós podem participar do mecanismo de consenso.
Privada permissionada	A capacidade de realizar transações e visualizar o *log* nessa *blockchain* é restrita apenas para os nós participantes da rede. O dono da *blockchain* é quem define os usuários da rede e quais nós podem participar do mecanismo de consenso.
Privada não permissionada	Existe restrição quanto à realização de transações e visualização do log, mas o mecanismo de consenso é aberto a qualquer nó.

Figura 6 – Tipos de *blockchain*.

88. Uma outra perspectiva para classificar uma *blockchain* é de acordo com as permissões quanto às operações de leitura (quem pode acessar o livro-razão e visualizar as transações), escrita (quem pode criar transações e envia-las pela rede) e *commit* (quem atualiza o estado do livro-razão). Diferentes combinações podem ser feitas para adequar às necessidades de um determinado ecossistema.

3.6 Plataformas de *blockchain* de código aberto

89. No período inicial de desenvolvimento da tecnologia *blockchain*, os projetos de código aberto mais comuns criavam um desvio ou *fork* da plataforma *bitcoin*, ou seja, copiavam a base de código e o estado da rede em um dado momento e, a partir daí, criavam novos projetos com ajustes e customizações diversos, voltados para atender às mais variadas necessidades. No final, resultavam plataformas completamente diversas da rede do *bitcoin*, embora pequenas porções da base de código original fossem aproveitadas.

90. Uma limitação comumente citada na arquitetura do *bitcoin* diz respeito à execução de código. Tendo sido criada especificamente para suportar transações envolvendo transferência de criptomoedas, o *bitcoin* não possui uma camada arquitetural suficientemente robusta a ponto de permitir a execução de programas semelhantes a contratos inteligentes. Ao invés disso, o *bitcoin* suporta tão somente a execução de *scripts* simples.

91. Por outro lado, a execução de código autônomo e autocontido, como os contratos inteligentes, requer de preferência um ambiente de máquina virtual que suporte a chamada *Turing completude*. Tal conceito, advindo da Teoria da Computação, diz respeito em essência à capacidade de um computador ou linguagem de programação de expressar quaisquer cálculos computacionais (a exemplo não somente de expressões matemáticas, mas também estruturas de controle como condicionais e laços). No contexto da plataforma *bitcoin*, nota-se, portanto, que ela não possui tal capacidade, tendo em vista que é extremamente difícil construir um programa ou contrato inteligente utilizando apenas as instruções fornecidas pela linguagem de *script* disponibilizada.

92. Com o advento e popularização da *ethereum* – um ambiente de *blockchain* que fornece plataforma *Turing*-completa voltada para a execução de contratos inteligentes –, tornou-se possível, tanto para desenvolvedores de código aberto como para empresas, construir novos produtos com lógica de negócio mais sofisticada e de mais alto nível, sobre uma plataforma já existente, ao invés de desenvolver praticamente do zero a partir de modificações sobre a plataforma *bitcoin*.

93. Depois do *ethereum*, surgiram diversos projetos de redes abertas de blockchains. O **Erro! Fonte de referência não encontrada.**, apresenta de forma mais detalhada a rede *ethereum* e outras das principais plataformas de código aberto encontradas no mercado.

4. *Blockchain* no setor público

94. Esta seção aborda as áreas em que as tecnologias DLTs podem ser empregadas na administração pública e apresenta como os governos estão atualmente utilizando *blockchain* no Brasil e no mundo.

4.1 Quais são as áreas de aplicação em que a tecnologia pode transformar o setor público?

95. Por se tratar de uma tecnologia de propósito geral, a tecnologia *blockchain* pode levar algum tempo para alcançar adoção em massa. Porém, uma vez adotada, pode obter ganhos de produtividade em vários setores.

96. Vislumbra-se, portanto, que a tecnologia poderá ser aplicada em áreas que ainda não foram imaginadas. De todo o modo, para compreender mais facilmente quais áreas podem ser impactadas pelas tecnologias *blockchain* e DLT.

Figura 7 – Características de casos de uso com alto potencial. Fonte: Fórum Econômico Mundial

97. Nada obstante, de acordo com os casos de uso pesquisados, algumas áreas despontam como as mais exploradas. O setor público vem adotando a tecnologia distribuída para registros públicos, identidade digital, saúde e assistência médica, comércio exterior, tokenização de moeda nacional fiduciária, programas sociais e compartilhamento de informações entre órgãos públicos.

98. Neste contexto, tem-se que, dentre as diversas áreas em que a tecnologia *Blockchain* pode ser aplicada na ampliação e melhoria de serviços do Governo, cita-se:

> a. **Tributação:** a tecnologia *blockchain* permite uma maior transparência nas transações financeiras e comerciais, já que, uma vez registradas no livro-razão distribuído, tais ocorrências podem ser facilmente monitoradas, auditadas e tributadas, reduzindo a sonegação de impostos;

b. **Serviços de Saúde:** a natureza distribuída dos dados inseridos na *blockchain* propiciam que serviços universais, como prontuário eletrônico, sejam disponibilizados de uma maneira segura, transparente e de fácil acesso pelos atores que participam do processo;

c. **Identidades Digitais:** com a *blockchain*, os governos podem implementar identidades digitais para o cidadão de forma que as informações possam ser facilmente acessadas pelas autoridades, dentro de políticas de segurança estabelecidas;

d. **Gestão de Convênios e Programas:** por meio da tecnologia *blockchain*, os recursos financeiros podem ser tokenizados e repassados pelo poder público a outros entes, de forma que tais recursos podem ser adequadamente acompanhados pelos gestores públicos quanto à sua correta aplicação.

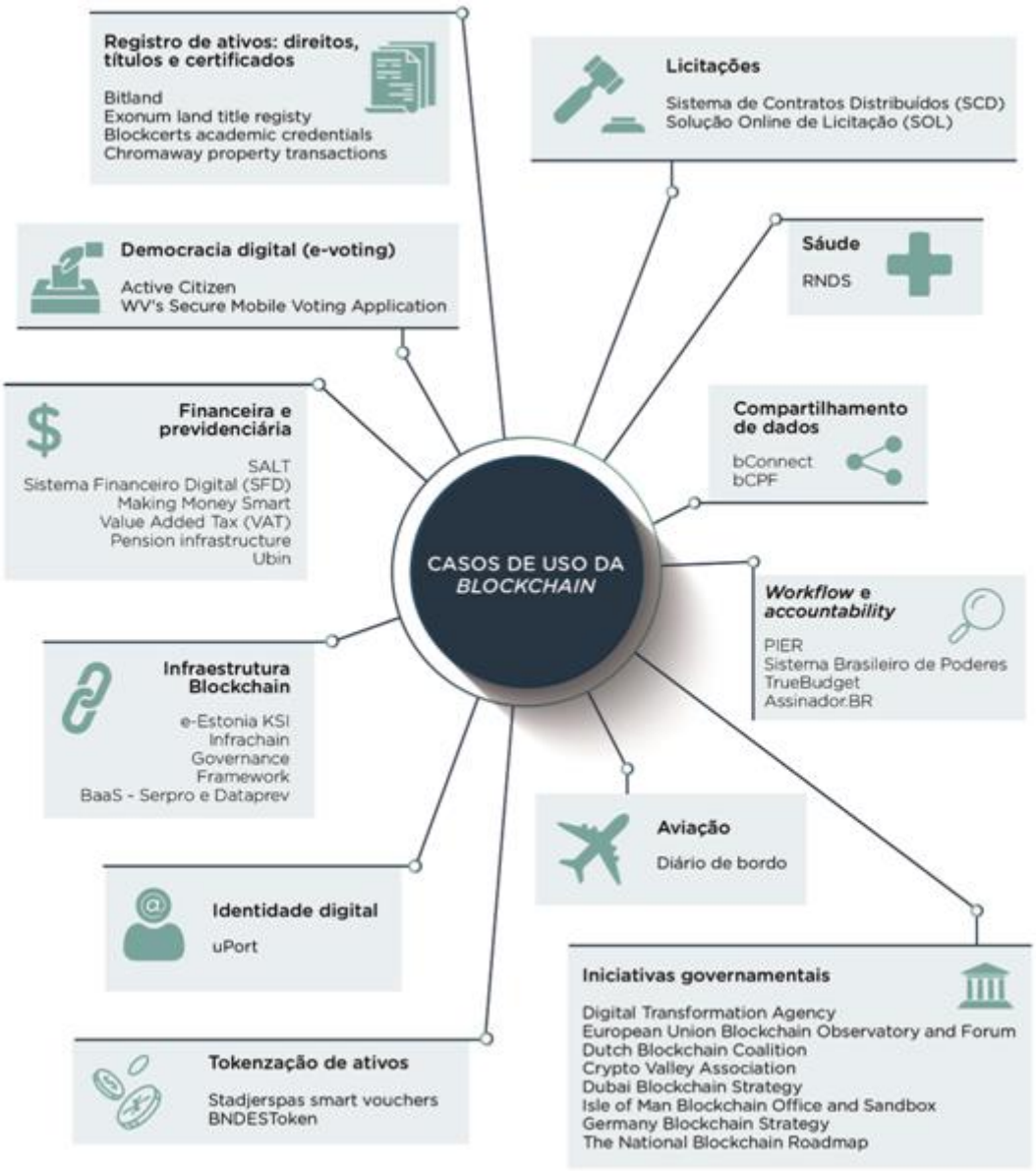

Figura 8 – Casos de uso identificados no Levantamento.

100. Além dos casos citados, tem-se o potencial para utilização das tecnologias distribuídas como alternativa para favorecer uma maior abertura de dados na APF. O **Erro! Fonte de referência não encontrada.**, apresenta uma avaliação de cenários, vantagens e desvantagens de diferentes abordagens para emprego de *blockchain* em substituição a dados abertos, baseada em um estudo realizado pela *Commonwealth Scientific and Industrial Research Organization* (CSIRO), órgão nacional de pesquisa científica da Austrália.

101. Outro potencial da tecnologia blockchain é a sua integração com a Internet das Coisas (em inglês, *Internet of Things* – IOT). Na IoT, independente do setor da economia, a tecnologia *blockchain* pode proporcionar uma forma de rastrear a história única de cada dispositivo, registrando a troca de dados entre ele e outros dispositivos, serviços web e usuários humanos. Pode também permitir que dispositivos inteligentes se tornem agentes independentes que conduzem de forma autônoma uma variedade de transações. Nesse sentido, o **Erro! Fonte de referência não encontrada.**, aborda brevemente sobre a integração dessas tecnologias.

4.2 Casos de uso identificados no Brasil – modelo (*framework*) de avaliação

102. Para assegurar que os projetos sejam comparáveis entre si, bem como com casos de outros países, foi utilizado um modelo adaptado do *framework* de avaliação utilizado pela Comissão Europeia[Erro! Indicador não definido.]. Assim, espera-se que esse modelo forneça aos gestores informações úteis para realizarem *benchmarking* de sua aplicação com outros projetos, facilitando a análise de quais tipos de problemas e como estão eles sendo resolvidos com a adoção de aplicações em *blockchain* no Brasil e ao redor do mundo. Os casos de uso analisados no país com base neste modelo estão descritos detalhadamente no **Erro! Fonte de referência não encontrada.**.

103. O *framework* adaptado consiste em avaliar projetos reais em sete dimensões que serão detalhadas a seguir. Os dados foram obtidos por meio de entrevista com os responsáveis dos órgãos e a aplicação de questionários padronizados.

Figura 9 – Framework de avaliação. Fonte: Comissão Europeia (adaptado)[Erro! Indicador não definido.].

Características gerais

104. Provê uma descrição sucinta do serviço público implementado com *blockchain*, destacando a criação de valor e o aspecto transformador obtido com a utilização do paradigma distribuído e

descentralizado. Avalia se outros entes públicos ou governos de outros países interagem com a solução, bem como informa se a aplicação é utilizada por outras organizações públicas. Também avalia o nível de abertura do software da plataforma de *blockchain* utilizada, podendo variar de código aberto a completamente proprietário.

Funcionalidade, governança e uso

105. Essa camada avalia e identifica as funcionalidades técnicas fornecidas pelo serviço baseado em *blockchain*, considerando as características relevantes e os potenciais benefícios da tecnologia, assim como as funções de negócio executadas pela aplicação *blockchain* (ex. prova de proveniência, execução automática de transações, integração de bases ou verificação de identidade etc.). Além disso, informa até que ponto instituições ou funções foram desintermediadas com o uso da solução. Também é feita análise mais ampla quanto ao nível de desburocratização alcançado, bem como se a solução provê mecanismos para o combate à fraude e à corrupção.

106. A governança da *blockchain* é avaliada quanto à descentralização, ou seja, quem tem o poder de decisão e como o projeto é controlado e direcionado. O modelo é detalhado, considerando a classificação dos tipos de *blockchain*, as entidades participantes e usuários da rede. São também identificados órgãos federais e demais entidades privadas, detalhando quais são as permissões de acesso (quem pode transacionar ou visualizar as informações etc.). É informado ainda o status do projeto, detalhando o número atual de usuários, a capacidade total, a vazão, a escalabilidade e o estágio atual em que a solução se encontra.

Arquitetura Técnica

107. Para a descrição da arquitetura técnica da *blockchain*, é utilizado um modelo em camadas de abstração. Essa estrutura hierárquica diferencia entre sistemas DLT e não DLT envolvidos. Assim, são descritos o *front-end*, as APIs e os sistemas que interagem com a aplicação (sistemas não DLT), bem como é apresentado o detalhamento da plataforma DLT utilizada.

Custos e benefícios

108. O custo total de propriedade da solução é separado entre as despesas incorridas até o momento de entrada em operação da solução e as despesas posteriores. Já os benefícios são classificados em qualitativos e quantitativos.

4.3 Ações regulatórias no Brasil

109. Em relação às implicações legais do uso de redes distribuídas e descentralizadas no país, nota-se que as primeiras instituições a criarem normas relacionadas ao tema são vinculadas ao Sistema Financeiro Nacional (SFN), além da RFB, que é autoridade tributária no Brasil. O foco desses normativos está na prevenção à lavagem de dinheiro e à evasão fiscal, o que demonstra inicialmente uma preocupação das organizações com relação ao uso indevido de criptoativos.

110. Posteriormente, ANAC e RFB positivaram o uso de tecnologias DLT como uma solução de tecnologia da informação a ser utilizada internamente em seus ambientes computacionais para prover serviços.

111. Já o Ministério da Economia, por meio da Secretaria Especial de Produtividade, Emprego e Competitividade, aprovou o Plano de Ação e o Orçamento-Programa para o ano de 2020 da Agência Brasileira de Desenvolvimento Industrial (ABDI), que prevê em seu orçamento o estímulo ao uso das tecnologias de *blockchain* para aumento da eficiência da gestão pública e a criação de uma lista de aplicações de *blockchain* para o processo de arrecadação pública, a partir de projeto-piloto.

112. A lista a seguir apresenta os normativos identificados:

Normativo	Assunto
CVM - Ofício Circular nº 11/2018/CVM/SIN	Investimento indireto em criptoativos pelos fundos de investimento.
BCB - COMUNICADO N° 31.379, DE 16 DE NOVEMBRO DE 2017	Alerta sobre os riscos decorrentes de operações de guarda e negociação das denominadas moedas virtuais.

RFB - INSTRUÇÃO NORMATIVA RFB Nº 1888, DE 03 DE MAIO DE 2019	Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB).
ANAC - RESOLUÇÃO Nº 511, DE 11 DE ABRIL DE 2019	Altera a Resolução nº 458, de 20 de dezembro de 2017, que regulamenta o uso de sistemas informatizados para registro e guarda de informações por regulados da ANAC.
RFB - PORTARIA Nº 55, DE 3 DE JULHO DE 2019	Dispõe sobre as formas e critérios de segurança da informação para o acesso a dados da Secretaria da Receita Federal do Brasil (RFB) por órgãos convenentes ou por órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional.
Ministério da Economia - PORTARIA Nº 3.237, DE 18 DE FEVEREIRO DE 2020	Aprova o Plano de Ação e o Orçamento-Programa de 2020 da Agência Brasileira de Desenvolvimento Industrial - ABDI.

Tabela 1 – Lista de normativos relativos à tecnologia *blockchain* no Brasil.

4.4 Iniciativas e casos de uso de outros países

113. Governos de todo o mundo estão conduzindo projetos-piloto usando as tecnologias *blockchain* e DLT. Para elaboração deste relatório foram pesquisados diversos casos de uso de países estrangeiros em diversas fontes, tais como: notícias na internet e sítios eletrônicos de outros governos, publicações especializadas e artigos acadêmicos. Todos eles estão descritos no Apêndice II – Aplicações e iniciativos *blockchain* em outros países.

5 Desafios e oportunidades das tecnologias *blockchain* e DLT

114. Com base na análise das principais características da tecnologia *blockchain*, nas entrevistas com especialistas e nos casos de uso visitados, a equipe de levantamento identificou os seguintes desafios (itens 6 a 11) e oportunidades (itens 1 a 5) relativos às tecnologias descentralizadas:

[1] Agilidade e baixo custo em projetos experimentais

115. Ainda que a experimentação de projetos em *blockchain* precise de um grau elevado de conhecimento de tecnologias distribuídas e programação de contratos inteligentes, devido à natureza *opensource* das principais plataformas corporativas de *blockchain* e redes não permissionadas, a administração pública pode realizar projetos piloto para explorar a tecnologia e validar requisitos de forma ágil, sem a necessidade de efetuar altos desembolsos para uma solução completa.

[2] DLTs promovem um governo hiperconectado

116. As tecnologias descentralizadas e distribuídas criam confiança em informações e processos com grandes grupos heterogêneos, sem a necessidade de confiar em uma única autoridade central. Isso viabiliza a integração e a execução satisfatória de processos quando há um desnível muito grande entre informações que prestadores de serviço e consumidores detém sobre determinada transação. No nível mais básico, isso implica serviços públicos aprimorados nos processos de registro e troca de informações (peça 37).

117. Em outras palavras, a tecnologia *blockchain*/DLT pode ser usada como uma camada comum e confiável para compartilhamento de informações entre diferentes esferas de governo (municipal, estadual e federal), países e com a indústria e a sociedade. Além do mais, a procedência dessas informações pode ser verificada *on-line*, de modo que o uso compartilhado e confiável de informações poupa tempo e reduz custos para a administração pública.

[3] Blockchain alinha-se ao combate à fraude e à corrupção

118. A utilização da tecnologia *blockchain*/DLT pode ser considerada tanto como um controle preventivo como detectivo no combate à fraude e à corrupção. A utilização das tecnologias distribuídas permite a criação de trilhas de auditoria para rastrear as operações de governo, além de favorecer a abertura de dados. Assim, o fato de que cada participante da rede mantém seu próprio registro atualizado das transações aumenta a transparência e reduz as oportunidades de fraude, dificultando a ocorrência de delitos e comportamentos antiéticos.

119. Além disso, como o *hash* de uma transação é vinculado aos *hashes* de todas as transações anteriores, as transações passadas podem ser verificadas e investigadas, de modo que as tentativas de adulteração são perceptíveis para os participantes da rede. Assim, a tecnologia também funciona como um controle detectivo, possibilitando o rastreio e a identificação de atividades ilegais.

120. O gerenciamento de dinheiro público é uma área em que soluções *blockchain* podem ajudar a minimizar fraudes e aumentar transparência e a responsabilidade dos entes envolvidos (peça 37). Por exemplo, com a utilização de contratos inteligentes é possível estabelecer que repasses de determinado programa de governo sejam efetivamente realizados somente se a transação é legítima, considerando parâmetros como valor, beneficiários, temporalidade, área de aplicação do recurso, entre outros.

121. Sendo assim, nota-se o potencial da tecnologia *blockchain* para prevenir e detectar desvios simultaneamente em decorrência de suas características inerentes da tecnologia (transparência, imutabilidade e irrefutabilidade), promovendo assim a cultura da prestação de contas nos serviços públicos e na realização das despesas governamentais. Todas essas vantagens reunidas aumentam a confiança nos dados mantidos pelo governo, especialmente nos casos em que cidadãos desconfiam sobre a veracidade das informações.

[4] Blockchain para otimizar serviços digitais prestados ao cidadão

122. Os processos intraorganizacionais enfrentam desafios de governança e desconfiança entre organizações que impedem a sua otimização. Além disso, a falta de um entendimento comum da lógica do processo pode ser um complicador na prestação de serviços que dependam da colaboração de vários órgãos.

123. A tecnologia *blockchain* permite que os processos sejam executados de maneira distribuída, sem delegar confiança às autoridades centrais nem exigir confiança mútua entre os participantes. Dessa maneira, a capacidade de realizar transações sem a necessidade de uma terceira parte confiável tem o potencial de desintermediar funções e instituições de governo.

124. Portanto, os serviços digitais que envolvem diferentes órgãos do governo podem ser beneficiados pela arquitetura descentralizada da *blockchain*. Especificamente, um modelo de processo que compreende tarefas executadas por várias partes pode ser coordenado e automatizado por meio de contratos inteligentes em uma rede *blockchain*. As vantagens mais importantes dos contratos inteligentes são que eles contêm um registro transparente e à prova de violações das transações em que nenhum terceiro é necessário para garantir a confiança.

125. Contratos inteligentes podem ser implementados para otimizar serviços digitais em que: há trabalho manual para verificar dados objetivos ou quantificáveis; partes não se conhecem ou não confiam uma na outra; existe interesses conflitantes; exigem confiança e transparência; os dados podem ser verificados automaticamente em fontes confiáveis. Além disso, a tecnologia *Blockchain* também pode ajudar os governos a reduzirem erros e o custo de processos que exigem muita interferência humana.

126. Por fim, considerando os recursos atualmente gastos na verificação e reconciliação dos dados coletados pela administração pública, espera-se uma substancial economia de custo e tempo, as quais podem ser obtidas via *blockchain* de maneira descentralizada e em tempo real, reduzindo assim a redundância de controles (peça 37).

[5] Redefinição do papel do governo na prestação de serviços digitais

127. No futuro, a função de autoridade centralizada exercida pelo governo pode se tornar menos relevante no contexto das tecnologias *blockchain*, ou seu papel pode mudar para fornecer uma plataforma e governança para serviços descentralizados, em vez de estar no centro de todas as transações[Erro! Indicador não definido.]. Essa será uma oportunidade para que processos colaborativos sejam redefinidos, possibilitando o surgimento de novos arranjos institucionais que façam uso extensivo de transações digitais inovadoras, propiciando que plataformas *blockchain* mantidas pelo governo conectem diferentes partes interessadas e criem valor público para desenvolvimento da economia.

128. O governo poderá desempenhar o papel de um administrador confiável que inicia e opera um registro, determina as regras de transação e audita os aplicativos para garantir o funcionamento adequado. No papel de gestor dos dados, o governo provavelmente permanecerá responsável pela configuração, operação e manutenção das aplicações e poderá ser responsabilizado em caso de falha ou quando tiverem

problemas de qualidade dos dados. Como tal, a tecnologia descentralizada exigirá uma reintermediação dos papéis do governo[Erro! Indicador não definido.].

129. Assim, há a possibilidade de reduzir ainda mais as atribuições do governo. Em um possível cenário, a administração pública possivelmente não precisará mais fornecer, por conta própria, processos de armazenamento e troca de informações que facilitam as atividades econômicas na sociedade, uma vez que isso poderá ser fornecido totalmente pelo protocolo *blockchain*. Nessa situação, o governo deverá manter um papel de supervisão no que diz respeito às transações que ocorrem nessa infraestrutura (peça 37).

[6] Projetos blockchain no âmbito da APF ainda estão em estágio de experimentação

130. A despeito de todo esforço empreendido por várias organizações, no âmbito da Administração Pública Federal, os projetos *blockchain* analisados durante esta auditoria ainda estão em experimentação, ou em estado inicial de produção, envolvendo um pequeno número de participantes. De fato, não há no momento da escrita deste relatório, nenhuma aplicação *blockchain* que está sendo utilizada em larga escala no âmbito da APF. Logicamente, esta situação poderá ser modificada à medida que a tecnologia amadureça, os projetos tenham o crescimento esperado em número de transações e participantes e as experiências de casos de sucesso sejam compartilhadas entre as organizações.

[7] Aplicações blockchain no âmbito da APF não envolvem diretamente o cidadão brasileiro

131. As iniciativas *blockchain* na APF ainda não alcançaram diretamente o cidadão brasileiro. As aplicações observadas, em sua maioria, são voltadas à colaboração entre entidades públicas e privadas, sem a participação da pessoa física. Em outros países, verifica-se a interação dos cidadãos diretamente em aplicações *blockchain*. A visibilidade pública e a possibilidade de interação direta do cidadão, além de ter efeito positivo na prestação dos serviços digitais, aumenta o controle social. Assim, entende-se que as aplicações que utilizam a tecnologia *blockchain* na APF podem e devem ser um instrumento de participação direta do cidadão brasileiro nas mais diversas questões, promovendo uma maior transparência e a diminuição da burocracia estatal.

[8] Plataformas blockchain permissionadas ainda não estão consolidadas

132. As plataformas de *blockchain* permissionadas, como *quorum* e *Hyperledger*, entre outras, ainda são relativamente novas, a despeito de terem tido uma evolução rápida. Tais ferramentas ainda não estão consolidadas e, em alguns casos, componentes importantes poderão ser alterados ou evoluídos, causando descontinuidade das tecnologias adotadas nas aplicações já desenvolvidas.

133. Há notícias, por exemplo, da troca de mecanismos de consenso entre versões de uma determinada plataforma e, vale lembrar, tal mecanismo é componente central de uma plataforma *blockchain*. Assim, nota-se que as plataformas permissionadas ainda estão em consolidação, o que envolve risco de manutenções custosas, ou mesmo descontinuidade, em aplicações já desenvolvidas ou em desenvolvimento.

134. Outro ponto que merece atenção é que as plataformas permissionadas não têm especificações mundialmente reconhecidas acerca da tecnologia *blockchain*. A despeito do esforço da comunidade europeia e do *International Telecommunication Union* (ITU) na padronização e disseminação do conhecimento sobre *blockchain*, ainda não há um consenso sobre os termos e padronizações em torno das ferramentas de mercado. De fato, plataformas observadas definem termos próprios e tecnologias próprias em suas implementações. A falta de padronização e especificação pode levar ao efeito *vendor lock-in*, onde a adoção de uma plataforma ou produto torna o cliente refém desta escolha.

[9] Falta de interoperabilidade entre plataformas blockchain

135. No momento da escrita deste relatório, as plataformas de *blockchain* permissionadas, a princípio, não são interoperáveis, o que significa dizer que os dados persistidos em uma plataforma não são intercambiáveis entre plataformas *blockchain*. Isto dificulta sobremaneira a colaboração entre aplicações *blockchain*, impedindo muitas vezes que um processo de negócio possa ser executado pela colaboração entre órgãos que usam diferentes plataformas *blockchain* em suas aplicações. Esta lacuna tem sido suprida pelo desenvolvimento de APIs e pelo registro de dados *off-chain*.

[10] Poucos profissionais com conhecimento sobre a tecnologia blockchain no âmbito da APF

136. Por ser uma tecnologia relativamente nova, o número de profissionais e servidores com domínio sobre os aspectos técnicos e conceitos que envolvem *blockchain* ainda é baixo, pelo menos nas organizações estatais visitadas no âmbito desta auditoria. Consta-se que o domínio ainda está sob a tutela de entusiastas da tecnologia *blockchain* em alguns órgãos e empresas específicas da APF. Nesse sentido, destacam-se as iniciativas do BNDES de disseminar o conhecimento e fomentar o ecossistema das tecnologias distribuídas no país, por meio da realização de workshops e treinamentos, a exemplo do Fórum *Blockchain*Gov.

137. Além disso, há poucos programadores disponíveis no mercado com conhecimento suficiente para escrever código de contratos inteligentes, o que pode ser um limitador na adoção dessa tecnologia pelo governo.

[11] A criação de um sistema de identidade digital pode viabilizar o uso massivo da tecnologia blockchain

138. De acordo com o *The European Union Blockchain Observatory & Forum*, um dos requisitos mais importantes na construção de uma sociedade digital é a disponibilização de uma identidade digital viável para todos os cidadãos, empresas, órgãos públicos ou, cada vez mais, máquinas e outros agentes autônomos. A organização refere-se à ideia da criação de uma identidade auto-soberana baseada em *blockchain*, que, em vez dos indivíduos manterem suas informações de identificação com terceiros, os próprios indivíduos seriam capazes de guardar suas informações de identificação autenticadas.

No paradigma da auto-soberania, os governos podem, por exemplo, emitir certificados assinados digitalmente para seus cidadãos ou residentes, atestando o nome, o endereço, a data de nascimento, o local de nascimento da pessoa, a residência, a permissão de dirigir, as propriedades imobiliárias, o título de eleitor e assim por diante. Sob esse paradigma, os indivíduos seriam, pelo menos, em teoria, responsáveis por proteger seus próprios dados pessoais.

6. Inventário de riscos

139. Com o surgimento de uma nova tecnologia emergente, novos riscos também são observados e devem ser tratados. Assim, foi estruturada uma lista contendo possíveis controles associados aos riscos identificados, bem como as referências de critérios (normas e boas práticas), com o intuito de auxiliar as áreas de tecnologia da informação das organizações quando forem implementar projetos de *blockchain* e DLTs.

140. Os riscos foram levantados e consolidados com base nas respostas aos questionários enviadas pelos auditados, no julgamento técnico da equipe de fiscalização, na consulta a normas e padrões internacionais, como descrito nos documentos ABNT NBR ISO/IEC 27002:2013, Cobit 2019, e normativos brasileiros específicos para a Administração Pública Federal, bem como em publicações especializadas do Gartner e da *Information Systems Audit and Control Association* (ISACA), entre outros documentos. A equipe de *blockchain* do BNDES também colaborou com sugestões para melhorar a matriz que a equipe do Levantamento elaborou. Informa-se que os riscos foram agrupados em cinco áreas para facilitar o entendimento e estão descritos detalhadamente no **Erro! Fonte de referência não encontrada.**:

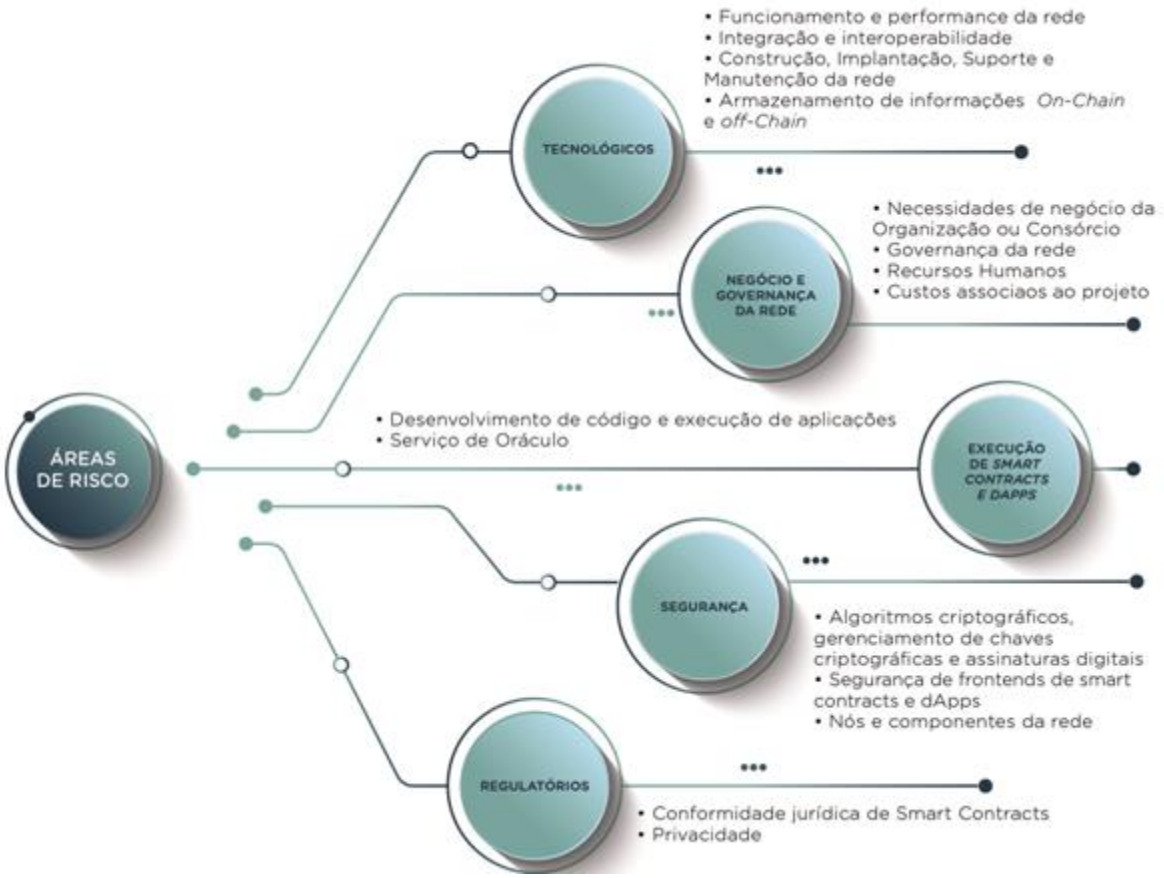

Figura 10 – Áreas de riscos relativos às tecnologias DLTs e *blockchain*.

7. Fatores críticos de sucesso para uma aplicação *blockchain*/DLT

141. Para facilitar as chances de sucesso, a equipe do levantamento elencou seis fatores que as áreas de tecnologia da informação devem levar em consideração antes de implementar projetos de soluções distribuídas. Dessa forma, os seguintes fatores críticos de sucesso devem ser considerados pelos gestores na implementação de uma aplicação distribuída:

[1] Conhecimento da tecnologia

142. Por ser uma tecnologia inovadora, ainda não existem muitos profissionais com habilidades e conhecimento sobre DLTs. Por isso, o desenvolvimento de uma aplicação *blockchain* requer capacitação da equipe de TI ou recrutamento de recursos humanos com a competência necessária para operar redes distribuídas *peer-to-peer* e escrever contratos inteligentes.

143. A organização deve conhecer a tecnologia e ter domínio sobre as principais características antes de iniciar um projeto descentralizado, além de estar ciente dos riscos que o uso de uma nova tecnologia pode introduzir.

[2] É necessário justificar o uso (mensurar o impacto para o negócio e para o cidadão)

144. A adoção de uma solução DLT não deve ser por modismo ou entusiasmo tecnológico. Não se deve utilizar uma solução DLT em um serviço centralizado que funciona bem atualmente e com custo controlado. Assim, a organização (ou consórcio) deve saber explicar o porquê de estar adotando o modelo descentralizado e distribuído das tecnologias *blockchain*/DLT em determinado caso de uso e como isso impacta no seu negócio e melhora os serviços públicos para o cidadão.

145. Deve-se avaliar bem o problema que se quer resolver para entender se é o caso de utilizar uma solução distribuída. Não só isso, espera-se também que os profissionais do projeto estejam cientes dos riscos relacionados ao uso da tecnologia para que possam gerenciá-los de forma efetiva.

146. Além disso, o novo paradigma requer uma avalição minuciosa sobre o impacto no negócio: quais pessoas, instituições e processos serão afetados? Quais são os ganhos em termos de eficiência e redução de custos que a aplicação pode trazer e qual é a relação custo-benefício quando comparada a outras tecnologias disponíveis? Como a solução está agregando valor pela perspectiva do cidadão e dos usuários dos serviços? Todas essas perguntas devem ser respondidas de forma clara e objetiva.

147. Outro ponto de atenção diz respeito ao propósito inicial da tecnologia: a realização de transações sem a necessidade de confiar em uma autoridade central. Assim, a desintermediação é uma propriedade desejável dessa tecnologia quando utilizada nos serviços públicos. Caso existam instituições intermediárias ou funções administrativas que podem ser eliminadas (ou ter sua importância reduzida), elas devem ser explicitadas como benefícios da solução.

148. Existem ferramentas disponíveis na internet que auxiliam as áreas de tecnologia a justificarem o uso e realizarem o *design* da solução *blockchain*, em especial cita-se o modelo "Canvas de aplicações *blockchain*", constante do **Erro! Fonte de referência não encontrada.**.

[3] Integração com o ambiente computacional e de negócio

149. Soluções baseadas em *blockchain* quase sempre requerem pontos de integração e/ou interoperabilidade com sistemas legados. Mecanismos de notificação e tratamento de eventos podem ser implementados para fins de atualização de bases de dados legadas e automatização de processos de negócio. Camadas de software adicionais baseadas em APIs podem ser necessárias para encapsular tanto os sistemas legados como também a solução *blockchain*.

150. Em situações de existência de bancos de dados legados, faz-se necessário levar em consideração os possíveis cenários de replicação de dados (a exemplo de cópia ou movimentação de dados da base legada para a *blockchain* e vice-versa), bem como definir quais dados serão armazenados *on-chain* e *off-chain*. Tal definição deve levar em conta, principalmente, os requisitos de confidencialidade, integridade, transparência, rastreabilidade e não repúdio das informações.

[4] Implementação gradual

151. As tecnologias *blockchain*/DLT ainda estão amadurecendo nas organizações. Portanto, é aconselhável a iniciação da implantação de uma solução distribuída com uma abordagem experimental, permitindo uma evolução contínua e gradual.

152. Isso requer a realização de projeto piloto e provas de conceito com escopo reduzido para validar o funcionamento da solução e conhecer eventuais obstáculos da tecnologia. A execução de uma fase de experimentação antes de partir para a implementação em larga escala é facilitada pelo fato de estarem disponíveis diversas plataformas de código aberto. Assim, o gestor público pode rapidamente construir um protótipo e validar os requisitos de seu caso de uso sem a necessidade de realizar desembolsos elevados.

[5] Os benefícios são potencializados com mais colaboração

153. As tecnologias *blockchain* movem o poder de uma autoridade central para o consenso baseado em rede. Isso quer dizer que, quantos mais participantes, mais resiliente é uma rede. Além disso, quanto mais entidades fazem uso e contribuem com as informações armazenadas em uma *blockchain*, mais valor aquela rede possui.

154. No contexto da administração pública, é preciso cooperação e colaboração dos diversos entes para alcançar sucesso com um projeto descentralizado. Assim, deve-se estruturar a governança da rede com o intuito de identificar os principais papéis e responsabilidades relacionados com o problema do caso de uso e garantir que haja mecanismos na solução para incentivar a participação das partes interessadas. Isso permite também que haja redução de custos em razão da natureza descentralizada do projeto.

[6] Estrutura de governança do consórcio adequada

155. Os projetos de *blockchain* são, por natureza, colaborativos. Isso significa sair de um modelo em que normalmente uma única organização é responsável por administrar os dados para um modelo de negócio em que as decisões do projeto são tomadas por um consórcio de entidades. Assim, criar uma estrutura de governança para organizações colaborativas é fundamental para o sucesso nos projetos de tecnologias distribuídas.

156. A liderança do consórcio deve definir responsabilidades entre os diferentes níveis de participantes na rede: comitê de governança, usuários, nós colaboradores, operadores técnicos, entre outros atores. Mais ainda, redes complexas podem ter a necessidade de definir classes de participantes que podem votar em relação a um assunto específico da rede, bem como definir se o mecanismo de governança a ser adotado será interno (*on-chain*) ou externo (*off-chain*) à rede *blockchain*.

157. Deve-se garantir que todos os grupos de partes interessadas estejam representados e determinar como as decisões são tomadas em relação às mudanças na aplicação *blockchain*. Outras questões acessórias também devem ser endereçadas como, por exemplo, determinar se os direitos dos membros iniciais serão diferentes dos membros posteriores, de forma que uma rede descentralizada opere de forma sustentável.

8. Modelo de avaliação da necessidade de utilização da tecnologia *blockchain*/DLT

158. Primeiramente, assim como ocorre com toda nova tecnologia inovadora, a escolha pela adoção de uma *blockchain*/DLT deve ser pautada em uma análise detalhada do problema, não devendo ser feita por impulso ou modismo. Uma solução de tecnologia distribuída pode ser uma alternativa indicada para resolver um problema, mas é preciso ressaltar que em muitos casos as tecnologias convencionais poderão ser mais apropriadas. Dessa forma, uma organização pública deve ser capaz de analisar se existem benefícios técnicos e econômicos que justifiquem o investimento.

159. Assim, como identificar se o desafio que a entidade pública enfrenta pode se beneficiar de uma solução descentralizada e distribuída? Para facilitar a escolha ou não por utilizar uma solução *blockchain* e decidir se uma solução *blockchain*/DLT se aplica ao caso de uso da instituição, a equipe do presente levantamento propõe um modelo de avaliação, 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 DLT. As perguntas de 5 a 7 se referem ao caso especial de uma *blockchain*. A imagem abaixo representa o fluxograma mencionado, seguido pelo detalhamento de cada uma das perguntas:

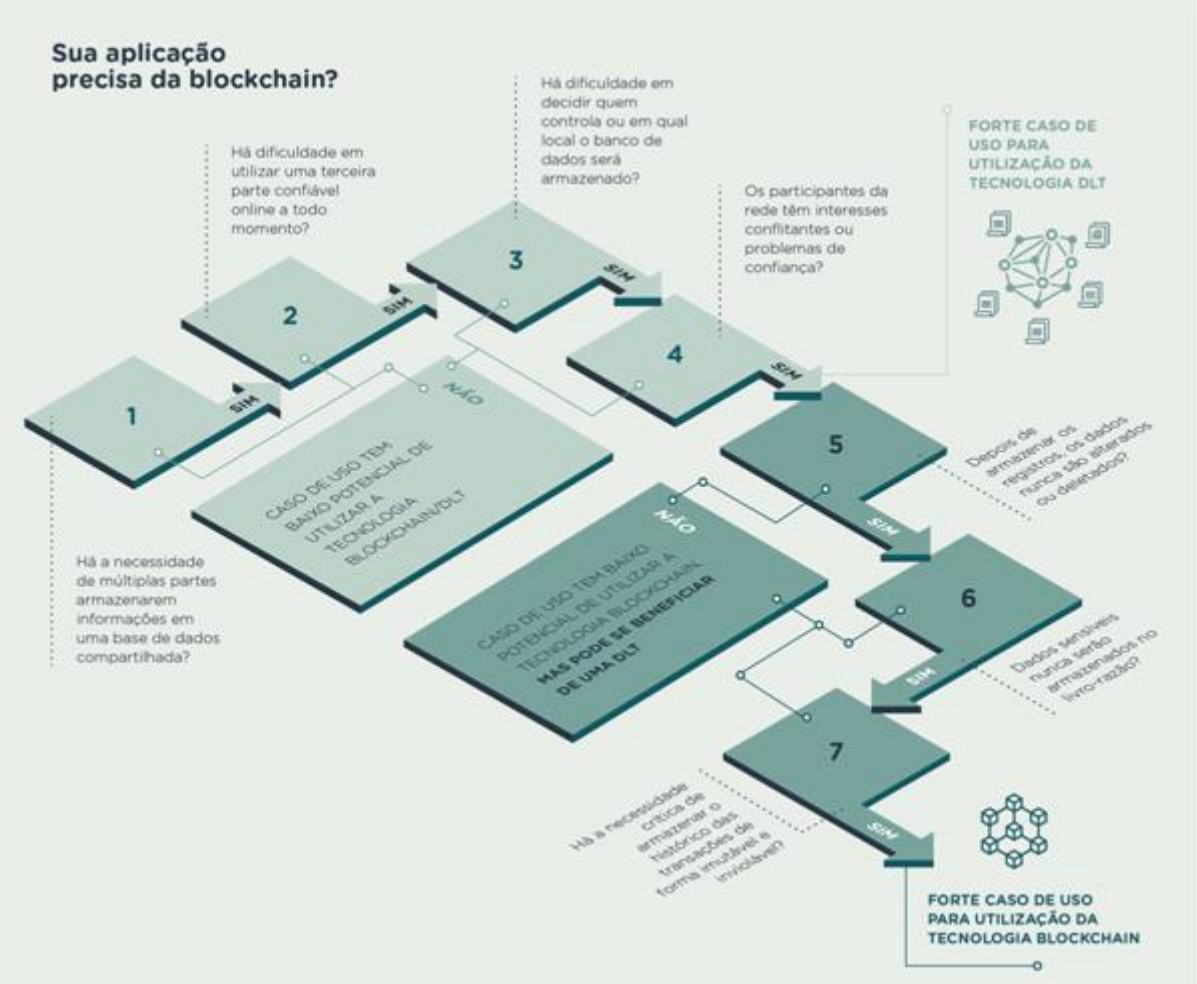

Figura 11 – Árvore de decisão quanto à necessidade de utilizar a tecnologia *blockchain*/DLT.

[1] Há a necessidade de múltiplas partes armazenarem informações em uma base de dados compartilhada?

160. 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, o gestor deve avaliar outros tipos convencionais de banco de dados.

[2] Há dificuldade em utilizar uma terceira parte confiável online a todo momento?

161. 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 ou em qual local o banco de dados será armazenado?

162. Nos sistemas tradicionais, existe desconfiança sobre quem armazena os dados, uma vez que eles podem ser facilmente manipulados. A arquitetura distribuída pode resolver o problema em que não há acordo sobre qual participante armazenará as informações. Além disso, uma vez que agora todos participantes armazenam as mesmas informações, o livro-razão é facilmente auditado pelos nós, aumentando a segurança como um todo. A adoção de uma arquitetura distribuída *blockchain* ou DLT 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?

163. 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 o 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 apagados?

164. Em uma *blockchain*, os dados são armazenados de forma somente escrita. Ou seja, novas informações são apenas apensadas, não havendo alteração dos dados que já foram gravados no livro-razão.

[6] Dados sensíveis nunca serão armazenados no livro-razão?

165. Como os dados são armazenados de forma transparente em toda a rede, a utilização de uma *blockchain* não faz sentido para aplicações que precisem manter sigilo dos dados. Os nós com acesso à rede poderão visualizar e rastrear todo o histórico de transações. Logo, uma *blockchain* deve ser utilizada para o armazenamento de dados que não são sensíveis.

[7] Há a necessidade crítica de armazenar o histórico das transações de forma imutável e inviolável?

166. A imutabilidade e a integridade são benefícios essenciais em virtude de os blocos serem encadeados e armazenados de forma e distribuída por nós que seguem as mesmas regras.

167. Assim, uma *blockchain* é útil quando há a necessidade de armazenar de forma consistente e inviolável todos os detalhes de transações que foram validadas de acordo com as regras pré-determinadas pela rede, incluindo o *timestamp* e as partes envolvidas.

9. Impactos advindos da tecnologia *blockchain* na atividade de fiscalização e auditoria

168. *Blockchain* poderá impactar nas atividades do TCU tanto por exigir conhecimento sobre possível objeto de auditaria como no modo como a Corte realiza suas fiscalizações. Dito de outra forma, *blockchain* tem o potencial de impactar não só os sistemas de informação dos jurisdicionados, mas também mudar o papel e os conhecimentos exigidos do auditor. Em um ambiente governamental com rápida mudança, o

órgão fiscalizador precisa se adaptar e estar preparado para desenvolver suas atividades em ambientes complexos que utilizam intensamente tecnologias inovadoras.

169. A análise feita nesta seção é baseada na literatura acadêmica, bem como em publicações e sites profissionais referentes à tecnologia *blockchain*. Não se pretende avaliar como as tecnologias descentralizadas afetarão as normas profissionais de auditoria no âmbito do TCU, mas apenas fazer reflexões de como poderá impactar a área de auditoria em um cenário de adoção crescente da tecnologia.

[1] Auditoria contínua e em tempo real

170. 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.

171. 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. A coleta contínua de evidências aprimora a auditoria, reduzindo o intervalo de tempo entre a ocorrência do evento e o procedimento de auditoria.

172. 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.

[2] Mudança de paradigma de auditoria baseada em amostra para auditoria baseada em todo o universo de dados

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

174. 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.

175. 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, dependendo do caso de uso, precisam ser considerados e endereçados. Por exemplo, como as informações na transação podem ser criptografadas, as chaves para descriptografar devem estar acessíveis para a função de auditoria. Além do mais, a regulamentação pode definir requisitos específicos, que precisam ser auditáveis na *blockchain*.

[3] Auditoria automatizada

176. Os mecanismos de governança, gerenciamento de riscos e controle estão às vezes associados à *blockchain*, não a um sistema ou organização específicos. Isso possibilita que os auditores possam 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.

177. 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), levando a níveis mais baixos de corrupção.

[4] Novos conhecimentos exigidos para o auditor

178. 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.

179. No que diz respeito às DLTs e *blockchain*, isso exige que o profissional adquira habilidade e proficiência sobre diversos conceitos técnicos 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.

180. O uso crescente de contratos inteligentes, possivelmente, exigirá o entendimento da linguagem de programação técnica para verificar se os acordos, 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.

181. *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.

182. 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, o que requer habilidades interpessoais.

[5] Auditores devem ter percepção da ocorrência de novos tipos de riscos e fraudes

183. 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. Além disso, o risco de conluio de participantes em uma rede permissionada e vulnerabilidades em contratos inteligentes são novos pontos de atenção do auditor.

[6] Compliance by Design

184. O termo *compliance by design* surge da necessidade de validar controles antes da 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.

185. 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 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 antes de serem executadas.

[7] Necessidade de validar informações off-chain

186. 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. 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.

187. 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*.

[8] Novos desafios e oportunidades

188. Um desafio que o auditor precisará lidar é 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. 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 realização de testes de auditoria.

189. 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.

190. 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. Já o uso de IA junto com contratos inteligentes poderá prever irregularidades e outros desvios.

10. Conclusão

191. Uma *blockchain* é a tecnologia que foi criada inicialmente para suportar a plataforma das moedas virtuais, como o *bitcoin*. Essa tecnologia, além resolver o problema da escassez na internet, permitiu uma nova forma de abordagem para as relações de troca de informações e de confiança para representar situações da vida real no mundo digital.

192. O aspecto descentralizador das tecnologias *blockchain* e DLT pode acelerar a transformação digital, uma vez que a possibilidade de realizar transações autenticadas sem a necessidade de uma autoridade central facilita a implementação de serviços públicos digitais orientados pela perspectiva do cidadão. As transações registradas no livro-razão são públicas e imutáveis, de modo que tentativas de violação das informações são facilmente rastreadas. Isso aumenta a transparência e reduz o tempo e os custos para verificar a conformidade dos dados e transações.

193. Em um mundo em que contratos inteligentes substituem controles manuais e em que cidadãos e empresas não precisam de intermediários para registrar e consultar informações, nota-se que a automação da confiança provida por soluções *blockchain* poderá ser um instrumento poderoso no desafiador processo de transformação digital.

194. Dentre as diversas áreas em que a tecnologia *blockchain* pode ser aplicada na ampliação e melhoria de serviços do Governo, elencam-se o processo tributário, a universalização de serviços de saúde, a criação de identidades digitais auto-soberanas, a gestão de convênios, o acompanhamento de repasses financeiros e a prevenção à fraude e à lavagem de dinheiro.

195. No Brasil, o presente trabalho analisou onze projetos de aplicações que fazem uso inovador de tecnologias distribuídas. O **Erro! Fonte de referência não encontrada.**, apresenta as informações de cada um desses projetos, obtidas por meio de visita da equipe de Levantamento às organizações. Essas informações auxiliarão gestores a avaliarem a necessidade de se utilizar a tecnologia *blockchain* em suas organizações públicas a partir da experiência de outras organizações do país.

196. Nada obstante, considerando o atual cenário mundial do uso de tecnologias *blockchain* e DLT, constatou-se que ainda falta o amadurecimento regulatório no país para o aproveitamento de todo o potencial dessas tecnologias digitais para aumentar a produtividade e impulsionar a economia. Nesse sentido, citam-se os exemplos de países como a Ilha de Man e a Suíça (**Erro! Fonte de referência não encontrada.**), que podem ser referências para o governo brasileiro criar ações específicas de incentivo às empresas *startups* de *blockchain*, bem como criar ambiente de leis flexíveis para realizar testes práticos de inovação com empresas privadas (*sandbox* regulatórios), permitindo assim o amadurecimento do arcabouço legislativo brasileiro relacionado à *blockchain*.

197. Merecem destaque também as iniciativas da União Europeia e de países como Dubai, Austrália, Alemanha, Estônia e Holanda, que estabeleceram o incentivo e o uso estratégico de *blockchain* e DLTs, com o intuito de aproveitar todo o potencial dessas tecnologias digitais para aumentar a produtividade e impulsionar a economia da nação.

198. Portanto, os aspectos abordados nas seções 3 e 4 do presente relatório permitem compreender o panorama geral sobre o estado da arte da tecnologia *blockchain* e os principais casos de uso no setor público do Brasil e no mundo, ou seja, como a tecnologia está sendo utilizada e quais áreas podem ser beneficiadas pela aplicação da tecnologia.

199. A seção "5 – Desafios e oportunidades das tecnologias *blockchain* e DLT", aborda aspectos das tecnologias distribuídas no entendimento da equipe do presente Levantamento. Em síntese, vislumbra-se que as aplicações *blockchain* utilizadas pela administração pública podem promover uma maior transparência e compartilhamento das informações. O uso de contratos inteligentes possibilitará a redução de erros e fraudes nas operações de governo. Pela ótica do cidadão, espera-se uma diminuição na burocracia dos serviços e uma interação mais direta com sistemas do governo, sem a necessidade de agentes intermediários que não agregam valor na prestação de serviços públicos.

200. Importante destacar também a visão dos especialistas entrevistados no que tange às implicações de soluções *blockchain* no governo:

> *Blockchain* pode agregar valor à administração pública em razão de suas propriedades de imutabilidade, transparência, rastreabilidade, confiabilidade e resiliência operacional. No nível mais básico, isso implica serviços públicos aprimorados nos processos de registro e troca de informações. Além disso, O gerenciamento de dinheiro público é uma área em que soluções *blockchain* podem ajudar a minimizar fraudes e aumentar transparência e a responsabilidade dos entes envolvidos. Isso aumenta muito a transparência em termos de processamento de dados e processos – importante em um ambiente governamental – e dificulta o uso indevido ou a falsificação de informações. Considerando os recursos atualmente gastos na verificação e reconciliação dos dados coletados pelas administrações públicas, a substancial economia de custo e tempo que podem ser obtidas via *blockchain*, de maneira descentralizadas e em tempo real são muito interessantes (peça 37).
>
> O compartilhamento de dados entre órgãos públicos, além da garantia da confiabilidade da informação, traz um grande potencial para desburocratizar as ações de governo para a sociedade. A partir do momento que uma informação já está na *blockchain*, o cidadão não precisa comparecer fisicamente nas organizações públicas, pois tem a garantia de onde a informação veio e o status dela. Além de poder dar ao cidadão maior transparência e controle sobre o uso de suas informações (peça 38).
>
> *Blockchain*/DLT propicia o consenso sobre as informações que o governo detém. As tecnologias tradicionais, com diferentes bases dispersas em diferentes órgãos ou até mesmo dentro do mesmo órgão, geram cenários onde não se sabe ao certo em qual informação confiar. *Blockchain* também oferece um framework que facilita a colaboração entre os órgãos e propicia, por meio dos contratos inteligentes, a automação de processos. Sendo, por tanto, ideal para promoção da transformação digital dos serviços públicos que envolvam diversos entes (peça 39).

201. Outros aspectos relevantes são a necessidade de compreender os riscos inerentes à tecnologia *blockchain* e avaliar a pertinência do projeto *blockchain* de uma organização auditada, ou seja, avaliar se realmente a solução distribuída atende aos requisitos de negócio e não está sendo adotada sem estudo de viabilidade. Nesse sentido, a equipe do presente trabalho, com base na análise da documentação e dos casos de usos estudados, elaborou um Modelo de avaliação da necessidade baseado em árvore de decisão e uma Matriz de riscos da tecnologia *blockchain*, presentes respectivamente na seção 8 e no **Erro! Fonte de referência não encontrada.**deste relatório, incluindo sugestões de controle para mitiga-los.

202. Dessa forma, as seções 5 a 8 visam subsidiar os gestores públicos com informações sobre a tecnologia, de modo que possam identificar possíveis casos de uso onde a tecnologia pode ser adotada na sua organização, bem como maximizar os benefícios e chances de sucesso com projetos de tecnologias distribuídas no governo de modo que agreguem valor aos cidadãos, além de evitar contratações *blockchain* quando não forem viáveis ou com risco elevado, gerando economia ao evitar possíveis despesas desnecessárias;

203. Com relação aos impactos advindos da tecnologia *blockchain* na atividade de fiscalização e auditoria, tem-se a possibilidade de ter que auditar tanto o código de contratos inteligentes como as transações dentro de uma *blockchain*. Em resumo, com a possibilidade de o TCU participar como nó de auditoria em uma *blockchain*, fazendo com que possua uma cópia local do livro-razão sincronizada com a rede distribuída, o acesso aos dados em tempo real será facilitado, de modo que a Corte poderá realizar auditoria sobre todo o universo de dados. Além disso, com a possibilidade de os auditores participarem de forma colaborativa ainda na etapa de concepção e planejamento de projetos de *blockchain*, bem como examinar contratos inteligentes antes deles entrarem em produção, espera-se que esta Corte de Contas possa atuar mais preventivamente na validação de controles e na verificação de irregularidades, em especial no combate à fraude e à corrupção.

204. Em um cenário com abundância no acesso aos dados, requerem-se novos conhecimentos dos auditores. Assim, será desejável que os profissionais de auditoria tenham certa experiência em avaliar se a organização auditada utilizou boas práticas no desenvolvimento de contratos inteligentes. Outras tecnologias que podem ser integradas ao uso de *blockchain* e DLTs, como inteligência artificial, IoT e *analytics*, também deverão ser melhor compreendidas pelos profissionais de auditoria. O conhecimento necessário dessas tecnologias permitirá que os auditores automatizem mais seus processos de trabalho, ampliando os resultados obtidos na atividade de fiscalização.

205. Dessa forma, a seção 9 teve o intuito de internalizar o conhecimento no âmbito do TCU, provendo à atividade de controle externo uma visão geral sobre as possibilidades abertas para auditar soluções de TI descentralizadas e distribuídas, além de aumentar a competência e capacidade do Tribunal em como avaliar os potenciais e riscos de novas tecnologias inovadoras que possam surgir, com base nas lições aprendidas e boas práticas identificadas neste trabalho. Nesse sentido, a Sefti enviará posteriormente memorandos à Secretaria-Geral de Controle Externo (Segecex) e ao Instituto Serzedello Corrêa (ISC) do TCU com informações relevantes identificadas neste trabalho, a fim de que avaliem a conveniência e oportunidade da adoção de medidas nas suas áreas de atuação, em decorrência dos aspectos da nova tecnologia que possam afetar a atividade de fiscalização.

206. Por fim, como benefício alcançado, este trabalho como um todo promove a cultura da inovação e fomenta o ecossistema de tecnologias descentralizadas no país, em prol da transformação digital. Nessa esteira, apresenta-se um framework da tecnologia *blockchain* com o intuito de auxiliar na implementação da tecnologia *blockchain*.

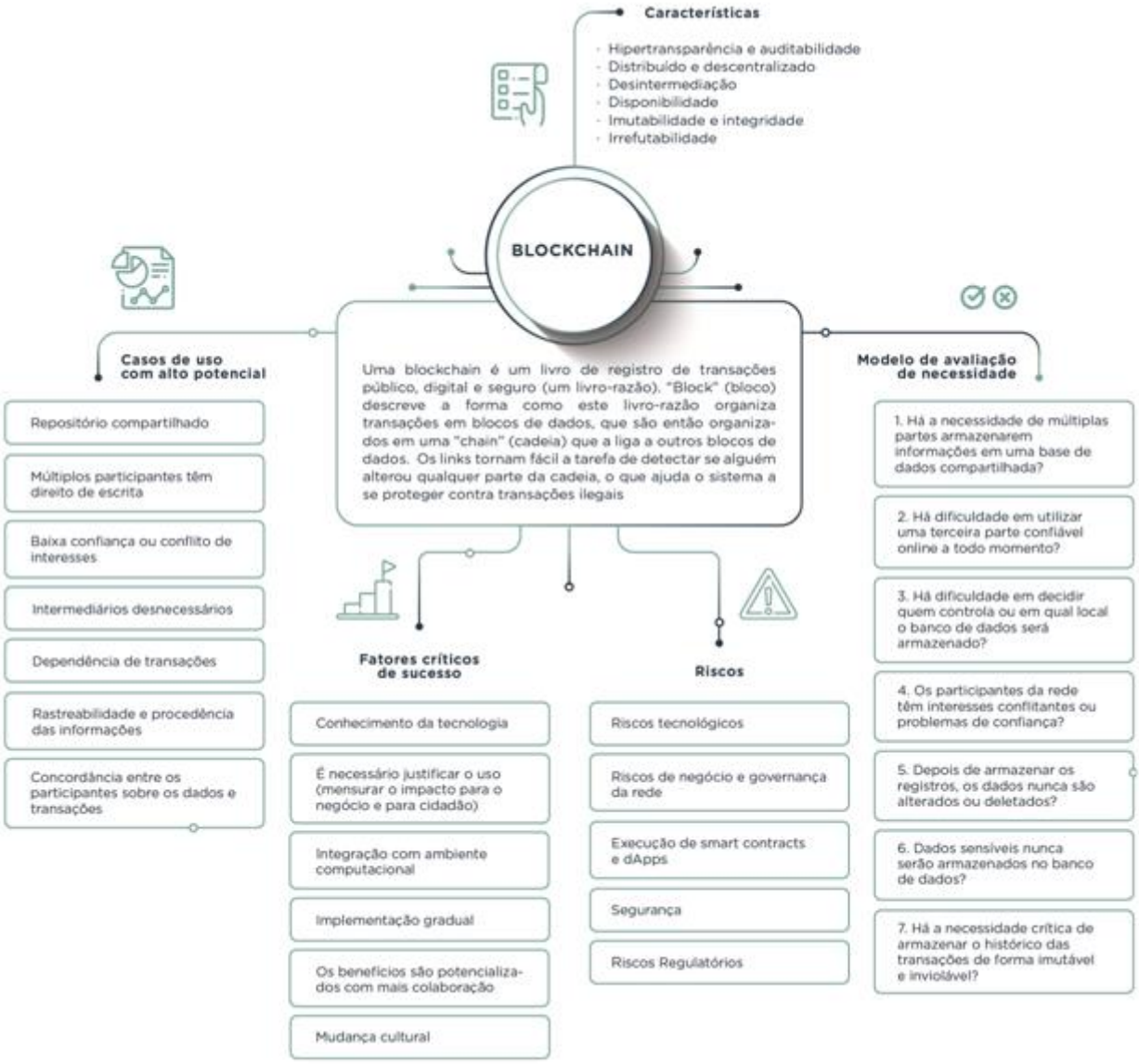

Figura 12 – *Framework* para implementar a tecnologia blockchain.

11. Proposta de encaminhamento

207. Ante o exposto, submetem-se os autos à consideração superior propondo:

207.1.1. recomendar à Secretaria Especial de Desburocratização, Gestão e Governo Digital (SEDGG) do Ministério da Economia, à Secretaria de Coordenação e Governança das Empresas Estatais do Ministério da Economia, à Câmara dos Deputados, ao Senado Federal, ao Tribunal de Contas da União, ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público que avaliem a conveniência e a oportunidade de orientarem os órgãos e entidades federais sob sua supervisão para que, ao considerarem o uso da tecnologia *Blockchain*/DLT em suas organizações, atentem para:

207.1.2. a necessidade de realizar um estudo de viabilidade sobre a utilização das tecnologias blockchain e *Distributed Ledger Technology* (DLT), considerando os recursos humanos disponíveis e os requisitos de negócio da organização, se for o caso, inicialmente com a condução de um projeto-piloto para validação do caso de uso, com o intuito de verificar a real necessidade de se utilizar uma solução desse tipo, podendo ser aplicados, por exemplo, o modelo de árvore de decisão e o modelo canvas, apresentados no presente Levantamento, para auxiliar o referido estudo;

207.1.3. os desafios, riscos, oportunidades e fatores críticos de sucesso das tecnologias *blockchain* e *Distributed Ledger Technology* (DLT) identificados no presente Levantamento;

207.1.4. a necessidade de incluir medidas anticorrupção e pró-transparência, ainda na fase de desenho da solução *blockchain* pretendida, considerando o potencial da tecnologia para favorecer a abertura de dados e reduzir fraudes e desvios;

207.2. encaminhar cópia da deliberação que vier a ser adotada, bem como do relatório, do voto, do relatório da unidade técnica e dos seus respectivos *Apêndice*s:

i. ao Banco Central do Brasil (BCB);

ii. ao Banco do Brasil (BB);

iii. ao Banco Nacional do Desenvolvimento Econômico e Social (BNDES);

iv. à Caixa Econômica Federal (Caixa);

v. à Empresa de Tecnologia e Informações da Previdência (Dataprev);

vi. à Receita Federal do Brasil (RFB);

vii. ao Serviço Federal de Processamento de Dados (Serpro);

viii. à Empresa de Petróleo Brasileiro S.A. (Petrobras);

ix. à Agência Nacional de Aviação Civil (Anac);

x. ao Instituto Nacional de Tecnologia da Informação (ITI);

xi. ao Ministério da Saúde (MS);

xii. à Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI) da Câmara dos Deputados;

xiii. à Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT) do Senado Federal;

xiv. à Associação Brasileira de Criptomoedas e Blockchain (ABCB);

207.3. encaminhar o relatório para a Controladoria-Geral da União (CGU) e Associação dos Membros dos Tribunais de Contas do Brasil (Atricon) para avaliarem a conveniência e oportunidade da adoção de medidas nas suas áreas de atuação, em decorrência dos aspectos da nova tecnologia, que possam afetar a atividade de fiscalização;

207.4. autorizar a Secretaria de Fiscalização de Tecnologia da Informação (Sefti) a divulgar as informações consolidadas constantes deste levantamento, preferencialmente por intermédio de ficha-síntese, sumário executivo e infográfico;

207.5. levantar o sigilo deste relatório, por conter informações relevantes às organizações públicas e à sociedade;

207.6. arquivar o presente processo, com fulcro no art. 169, inciso V, do Regimento Interno do TCU."

É o Relatório.

VOTO

Trata-se de levantamento com o objetivo de identificar áreas de aplicação de **blockchain** e de livros-razão distribuídos (**Distributed Ledger Technology** - DLT) no setor público, seus principais riscos e fatores críticos de sucesso, além dos desafios para o controle.

2. Chamamos de livro-razão uma estrutura de dados imutável, em que transações são registradas e mantidas. Caso esses registros sejam replicados em todos os nós de determinada rede, temos um livros-razão distribuído.

3. **Blockchain** pode ser definido como um **software** que funciona como um livro-razão distribuído. O que distingue, então, esse livro-razão dos bancos de dados ou **softwares** tradicionais é a resistência à adulteração, pois a alteração dos dados de um bloco requer a manipulação de todos os blocos anteriores. Como os dados estão replicados e distribuídos, entende-se que essa alteração é muito difícil.

4. Essa é uma característica essencial, pois o livro-razão é acessível e público a todos que façam parte da rede, assim os participantes podem ver o histórico das transações em tempo real. Como resultado, a rastreabilidade das operações possibilita a qualquer usuário auditar todas as transações, com plena convicção de que os registros se mantêm íntegros, aumentando a confiança na rede e reduzindo comportamentos fraudulentos.

5. Ainda que a transparência seja um dos diferenciais de uma **blockchain**, é possível utilizar a tecnologia em **blockchains** privadas com o uso de criptografia e disponibilizá-las apenas para quem o acesso é conferido, mantendo, em certa medida, requisitos de privacidade.

6. As principais características da tecnologia **blockchain** são: hipertransparência, auditabilidade, integração de informações dentro e fora dos limites da administração pública, de forma distribuída e descentralizada; desintermediação; automação de transações e processos; disponibilidade, pois não existe ponto único de falha; e integridade das informações.

7. Abstenho-me, neste voto, de ir além nos conceitos e aspectos mais técnicos da tecnologia, abordados com elevada qualidade e profundidade no relatório do levantamento e em seus apêndices.

8. Devo ressaltar que, por se tratar de tecnologia com potencial disruptivo devido à capacidade de digitalizar, proteger e rastrear transações sem a necessidade de uma terceira parte confiável, o **blockchain** deverá ter um efeito transformador na sociedade e nos serviços públicos. O momento, então, é propício para que o TCU conheça melhor o assunto, uma vez que, embora a tecnologia esteja avançando sobre novos nichos, os projetos de **blockchain** no setor público ainda se encontram restritos a iniciativas isoladas.

9. Enquanto isso, o Gartner estima que até 2023 a tecnologia **blockchain** suportará o movimento global e o rastreamento de dois trilhões de dólares por ano. Por ora, o mercado financeiro debate formas de regular e medir as transações que fazem uso dessa tecnologia, como, por exemplo, as realizadas com o uso de **bitcoin**. Nessa linha, a Receita Federal do Brasil (RFB), ao publicar a IN 1888/2019, disciplinou a obrigatoriedade de prestação de informações relativas a criptoativos.

10. De maneira incipiente, o setor público tem adotado a tecnologia distribuída para registros públicos, identidade digital, assistência médica, comércio exterior, tokenização de moeda nacional fiduciária, programas sociais e compartilhamento de informações entre órgãos públicos. Além disso, percebe-se potencial de adoção em áreas relacionadas à:

    - tributação: a tecnologia **blockchain** permite uma maior transparência nas transações financeiras e comerciais, reduzindo a sonegação de impostos;

    - serviços de Saúde: a natureza distribuída dos dados inseridos na **blockchain** propiciam que serviços universais, como prontuário eletrônico, sejam disponibilizados de uma maneira segura, transparente e de fácil acesso pelos atores que participam do processo;

    - identidades Digitais: com a **blockchain**, os governos podem implementar identidades digitais para o cidadão de forma que as informações possam ser facilmente acessadas pelas autoridades, dentro de políticas de segurança estabelecidas;

    - gestão de Convênios e Programas: por meio da tecnologia **blockchain**, os recursos financeiros podem ser tokenizados e repassados

pelo poder público a outros entes, de forma que tais recursos podem ser adequadamente acompanhados pelos gestores públicos quanto à sua correta aplicação.

11. Acrescento à lista trazida pela Sefti os serviços cartoriais, herança patrícia para conferir confiança a uma sociedade desconfiada de tudo, com boas razões. Uma seara, portanto, em que o **blockchain** há de transformar usos e costumes, trazendo agilidade às transações entre particulares.

12. De certa forma, trata-se de uma tendência contraintuitiva do ponto de vista governamental, de natureza inerentemente centralizadora, afinal é o próprio poder público que atua como a terceira parte confiável nos exemplos citados acima. Compartilhar o controle das mídias e dos registros em uma arquitetura mais eficiente e aberta exigirá amadurecimento de processos e gestores. Reconheço, também, que os desafios agregados por ela também são relevantes, pois trata-se de um movimento ainda não consolidado, com poucos profissionais capacitados.

13. Diante disso, o relatório apresenta um inventário de riscos com cinco dimensões: tecnológica, governança da rede, execução, segurança e regulação. Esta última inclui as questões referentes à privacidade (peça 55, p. 29).

14. Considerando esse conjunto de riscos, a Sefti consolidou um denso modelo de suporte à tomada de decisão para que o gestor possa avaliar se a tecnologia **blockchain**/DLT deve ser adotada em aplicações sob sua responsabilidade (peça 55, p.32-34). Transcrevo as perguntas que amparam a avaliação proposta, em que um elevado número de respostas "sim" sugere maiores ganho com a adoção da tecnologia:

> - "Há a necessidade de múltiplas partes armazenarem informações em uma base de dados compartilhada?
> - Há dificuldade em utilizar uma terceira parte confiável online a todo momento?
> - Há dificuldade em decidir quem controla ou em qual local o banco de dados será armazenado?
> - Os participantes da rede têm interesses conflitantes ou problemas de confiança?
> - Depois de armazenar os registros, os dados nunca são alterados ou apagados?
> - Dados sensíveis nunca serão armazenados no livro-razão?
> - Há a necessidade crítica de armazenar o histórico das transações de forma imutável e inviolável?"

15. Entre os fatores críticos de sucesso apontados pela Sefti, destaco a importância de mensurar o impacto para o negócio e para o cidadão, a integração com o ambiente computacional e de negócio, a

necessidade de colaboração e a estrutura de governança do consórcio, uma vez que decisões do projeto são tomadas por um consórcio de organizações.

16. Do ponto de vista do controle, o par **blockchain/Distributed Ledger Technology** apresenta-se como um aliado. Soluções distribuídas contribuem para a governança e a transparência das organizações, fornecendo aos interessados acesso imediato e irrestrito a dados. A integração das atividades de auditoria com a operação de processos controlados por DLTs possibilitaria, por exemplo, um monitoramento contínuo dos gastos públicos, de histórico inviolável.

17. É fato que técnicas de auditoria contínua, processos de avaliação do universo de dados em vez de amostra e automação de avaliação de atos administrativos são uma realidade no TCU há algum tempo. Ainda assim, mostra-se oportuna a incorporação dessa nova capacidade ao arsenal técnico disponível ao controle, considerando que a adoção das tecnologias discutidas nestes autos na gestão pública se encontra em expansão.

18. Lembro que a característica descentralizadora das tecnologias **blockchain** e DLT pode acelerar a transformação digital do Estado, uma vez que a possibilidade de realizar transações autenticadas sem a necessidade de uma autoridade central facilita a implementação de serviços públicos digitais orientados ao cidadão.

19. Nessa linha, sempre devemos olhar com atenção as ações tomadas por nações protagonistas em inovação. Austrália, Alemanha, Estônia e Holanda têm incentivado o uso estratégico de **blockchain** e DLTs, com o intuito de aproveitar o potencial dessas tecnologias digitais para aumentar a produtividade e impulsionar a economia. Recentemente, a China reforçou seu protagonismo ao anunciar o lançamento de criptomoeda própria.

20. Oportuno então o presente levantamento, preparando o TCU para atuar diante de um contexto em transformação.

21. Reconheço os benefícios do presente trabalho ao analisar as oportunidades, ganhos e riscos da tecnologia, bem como propor um **framework** abrangente da **blockchain**, sem furtar-se de sugerir caminhos mais seguros para a sua implementação.

Atuando assim, o TCU contribui para promover a cultura da inovação e fomentar o ecossistema de tecnologias descentralizadas no país, contribuindo para acelerar a transformação digital que esse país tanto precisa.

22. Nesse aspecto, e por se tratar de uma tecnologia relativamente recente, é importante que a Sefti, como fez no presente trabalho, continue atenta às contribuições das organizações com mais experiência na sua aplicação e, em especial, ao eventual conhecimento desenvolvido pelos órgãos governantes superiores, na sua função reguladora, de modo que os modelos desenvolvidos se mantenham atualizados.

23. Quanto aos encaminhamentos, propõe a Sefti recomendação à Secretaria Especial de Desburocratização, Gestão e Governo Digital (SEDGG) do Ministério da Economia e a outros órgãos governantes superiores que orientem sobre importância de realizar estudos ou atentem para desafios, riscos, oportunidades e fatores críticos de sucesso das tecnologias **blockchain** e **Distributed Ledger Technology** identificados no presente Levantamento, antes de adotar as citadas tecnologias.

24. Embora reconheça a necessidade de um planejamento bem fundamentado, creio que a medida sugerida pode mostrar-se ineficaz em grande parte, tendo em vista que a maioria absoluta das organizações públicas não tem condições técnicas de implementar a tecnologia, ou mesmo de identificar oportunidades de fazê-lo.

25. Opto, então, por limitar o alcance, com vistas a evitar a multiplicação de ofícios, mas reforçar a medida, ao determinar aos órgãos governantes superiores que avaliem, entre seus supervisionados, aqueles que deverão ser informados das conclusões presentes nestes autos, orientando-os com relação ao referido conteúdo.

26. Devido à excelência do trabalho, ao possível aproveitamento da pesquisa e das conclusões contidas nestes autos por outras organizações e à ausência de informações sensíveis, o sigilo que recai por padrão em processos dessa natureza deve ser levantado.

27. Por fim, considero que a disponibilização do conteúdo produzido nas mídias apropriadas e em eventos como a Sefti tem feito ao longo dos anos

será um canal eficaz de disseminação de informações e alcance dos resultados almejados de transformação de cultura na Administração Pública Federal, sem prejuízo da realização de evento específico para tratar dos assuntos abordados no presente levantamento.

28. Assinto às demais propostas, com os ajustes de forma pertinentes.

Ante o exposto, VOTO por que o Tribunal adote a minuta de Acórdão que ora submeto à apreciação deste Colegiado.

TCU, Sala das Sessões Ministro Luciano Brandão Alves de Souza, em 24 de junho de 2020.

AROLDO CEDRAZ
Relator

ACÓRDÃO Nº 1613/2020 – TCU – Plenário

1. Processo TC 031.044/2019-0.
2. Grupo I – Classe de Assunto: V - Levantamento de Auditoria.
3. Interessados/Responsáveis: não há.
4. Órgãos/Entidades: Agência Nacional de Aviação Civil (Anac); Banco Central do Brasil (BCB); Banco do Brasil S.A.; Banco Nacional de Desenvolvimento Econômico e Social (BNDES); Caixa Econômica Federal (CEF); Empresa de Tecnologia e Informações da Previdência (Dataprev); Instituto Nacional de Tecnologia da Informação (Inti); Petróleo Brasileiro S.A.; Secretaria Especial da Receita Federal do Brasil (RFB); Secretaria Especial de Desburocratização, Gestão e Governo Digital; Serviço Federal de Processamento de Dados (Serpro).
5. Relator: Ministro Aroldo Cedraz.
6. Representante do Ministério Público: não atuou.
7. Unidade Técnica: Secretaria de Fiscalização de Tecnologia da Informação (Sefti).
8. Representação legal: não há.

9. Acórdão:

VISTOS, relatados e discutidos estes autos de Levantamento de Auditoria com o objetivo de identificar as áreas de aplicação do **blockchain** no setor público, os principais riscos e fatores críticos de sucesso, além dos desafios para auditoria e controle;

ACORDAM os ministros do Tribunal de Contas da União, reunidos em sessão do Plenário, ante as razões expostas pelo relator, em:

9.1. encaminhar cópia da presente deliberação, bem como do relatório, do voto, do relatório da unidade técnica e dos seus respectivos apêndices:

i. ao Banco Central do Brasil (BCB);
ii. ao Banco do Brasil (BB);
iii. ao Banco Nacional do Desenvolvimento Econômico e Social (BNDES);
iv. à Caixa Econômica Federal (Caixa);
v. à Empresa de Tecnologia e Informações da Previdência (Dataprev);
vi. à Receita Federal do Brasil (RFB);
vii. ao Serviço Federal de Processamento de Dados (Serpro);
viii. à Empresa de Petróleo Brasileiro S.A. (Petrobras);
ix. à Agência Nacional de Aviação Civil (Anac);
x. ao Instituto Nacional de Tecnologia da Informação (ITI);
xi. ao Ministério da Saúde (MS);
xii. à Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI) da Câmara dos Deputados;
xiii. à Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT) do Senado Federal;
xiv. à Associação Brasileira de Criptomoedas e Blockchain (ABCB);
xv. ao Tribunal de Contas da União (TCU);
xvi. à Câmara dos Deputados (CD);
xvii. ao Senado Federal (SF);
xviii. à Casa Civil da Presidência da República;

9.2. encaminhar o Relatório para a Controladoria-Geral da União (CGU) e Associação dos Membros dos Tribunais de Contas do Brasil (Atricon) para avaliarem a conveniência e oportunidade da adoção de medidas nas suas áreas de atuação, em decorrência dos aspectos da nova tecnologia que possam afetar a atividade de fiscalização;

9.3. determinar à Secretaria Especial de Desburocratização, Gestão e Governo Digital (SEDGG) do Ministério da Economia, à Secretaria de Coordenação e Governança das Empresas Estatais do Ministério da Economia, ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público que, caso identifiquem órgãos e entidades sob sua supervisão que considerem o uso da tecnologia Blockchain/DLT, informe-os que atentem para:

9.3.1. a necessidade de realizar um estudo de viabilidade sobre a utilização das tecnologias **blockchain** e **Distributed Ledger Technolog**y (DLT), considerando os recursos humanos disponíveis e os requisitos de negócio da organização, se for o caso, inicialmente com a condução de um projeto-piloto para validação do caso de uso, com o intuito de verificar a real necessidade de se utilizar uma solução desse tipo, podendo ser aplicados, por exemplo, o modelo de árvore de decisão e o modelo canvas, apresentados no presente Levantamento, para auxiliar o referido estudo;

9.3.2. os desafios, riscos, oportunidades e fatores críticos de sucesso das tecnologias **blockchain** e **Distributed Ledger Technology** (DLT) identificados no presente Levantamento;

9.3.3. a necessidade de incluir medidas anticorrupção e pró-transparência, ainda na fase de desenho da solução **blockchain** pretendida, considerando o potencial da tecnologia para favorecer a abertura de dados e reduzir fraudes e desvios;

9.4. retirar o sigilo do restante deste processo;

9.5. autorizar à Secretaria de Fiscalização de Tecnologia da Informação (Sefti) a divulgar e compartilhar as informações constantes deste levantamento de auditoria, realizando, caso entenda como oportuno e conveniente, evento específico;

9.6. arquivar o presente processo, com fundamento nos art. 169, inciso V, do Regimento Interno do TCU.

10. Ata n° 23/2020 – Plenário.
11. Data da Sessão: 24/6/2020 – Telepresencial.
12. Código eletrônico para localização na página do TCU na Internet: AC-1613-23/20-P.
13. Especificação do quórum:
13.1. Ministros presentes: José Mucio Monteiro (Presidente), Walton Alencar Rodrigues, Benjamin Zymler, Augusto Nardes, Aroldo Cedraz (Relator), Raimundo Carreiro, Ana Arraes, Bruno Dantas e Vital do Rêgo.
13.2. Ministros-Substitutos presentes: Augusto Sherman Cavalcanti, Marcos Bemquerer Costa, André Luís de Carvalho e Weder de Oliveira.

(Assinado Eletronicamente)
JOSÉ MUCIO MONTEIRO
Presidente

(Assinado Eletronicamente)
AROLDO CEDRAZ
Relator

Fui presente:

(Assinado Eletronicamente)
CRISTINA MACHADO DA COSTA E SILVA
Procuradora-Geral