ENCCLA 2020

ESTRATÉGIA NACIONAL DE COMBATE À CORRUPÇÃO E À LAVAGEM DE DINHEIRO

Blockchain no setor público: Guia de conceitos e usos potenciais

1ª Edição

Ação 08/2020 Elaborar diagnóstico sobre as possibilidades de uso de tecnologias como blockchain no setor público.

Órgão coordenador: AGU
Suplente: BNDS

Coolaboradores: ABIN, AEAL/MJSP. AJUFE, AMB, BCB, CADE, CGDF, CGM/SP, CGU, CJF, CONACI, CONJUR/MJSP, DRCI, FEBRAPAN, GNCOC, GSI/PR, MP/GO, MP/MG MP/PR, MP/RJ, MP/RN, MP/SP, MPDFT, MPF, MPM, PF, PGFN, RFB, SEGES/ME, SEPRT/ME, SF, TCE/RS, TCU

Convidados: SERPRO, SEME/PR

Sumário

Agradecimentos

Como será visto, parte substancial do texto das seções 2, 3 e 4 deste documento baseou-se, por vezes ipsis litteris, no Acórdão 1.613/2020 – Plenário, proferido pelo Tribunal de Contas da União. O uso da informação no referido formato foi acordado com o representante do TCU no Grupo de Trabalho da Ação 08/2020 da ENCCLA, ao qual se agradece pela disponibilidade e empenho em viabilizar sua adaptação, quando necessário, às particularidades da obra.

Enfatize-se que a classificação referente ao uso da tecnologia no âmbito de cada instituição pública foi definida a partir das informações fornecidas pelos próprios órgãos colaboradores do colegiado, aos quais se agradece pelo valioso empenho. Ressalte-se, ademais, que somente a partir dessa ampla colaboração é que foi possível elaborar um diagnóstico com significativa representatividade do setor público brasileiro, haja vista que participaram dos trabalhos desta Ação diferentes órgãos e entidades públicas e privadas ligados a diferentes segmentos da Administração Pública.

1. INTRODUÇÃO

O conceito de uma tecnologia descentralizada capaz de viabilizar a troca de valor entre usuários foi apresentado no artigo Bitcoin: A Peer-to-Peer Electronic Cash System[I] divulgado e escrito por um usuário da lista de discussão The Cryptography Mailing List no dia 1º de novembro de 2008[II] . Este usuário, que se identificou como Satoshi Nakamoto, acabou por criar algo muito maior que um sistema descentralizado de dinheiro eletrônico. Na verdade, desde então, começamos a repensar totalmente a forma como a economia digital opera e estamos nos preparando para efetivamente migrar de uma internet capaz de garantir a troca informações para uma rede confiável que propicia a troca de valores[III] .

No entanto, foram necessários alguns anos para que fosse enxergado o verdadeiro potencial desta tecnologia. Até 2015, o termo blockchain era pouco conhecido, o assunto das rodas de conversa de tecnologia eram os criptoativos e o seu potencial uso para o cometimento de crimes. Um dos casos mais conhecidos foi a Silk Road, um mercado negro eletrônico lançado em 2011 que prometia aos seus usuários uma forma segura e anônima de comprar e vender drogas e outros materiais ilícitos. O site foi fechado pelo FBI em 2013 e o seu criador condenado à prisão perpétua[IV] .

Um ponto de virada para a tecnologia por trás do bitcoin foi a matéria de capa da edição de 31 de outubro de 2015 da conceituada revista britânica The Economist, intitulada: The trust machine - how the technology behind bitcoin could change the world[V] . A matéria destacou o papel da blockchain para permitir o registro confiável de transações e ajudou a consolidar a ideia de que se poderia dissociar o conceito de livros-razão distribuídos da blockchain dos criptoativos como o bitcoin que gozavam de uma má reputação naquela época.

Daquele momento em diante, cresceu o movimento na indústria financeira, para adoção de tecnologias baseadas em blockchain que pudessem reduzir os custos e o tempo para efetuar transações em meio digital[VI] . E não foram apenas os bancos que se beneficiaram desta novidade. Os mais diferentes casos de uso surgiram, incluindo: registro de imóveis, automação de cadeias de suprimentos, emissão de identidades digitais e outros discutidos ao longo deste documento.

Por isso, apesar de a tecnologia blockchain ter nascido em um ambiente de contracultura[VII], que buscava a ruptura do status quo quanto ao controle exercido por um órgão central, ela apresenta um modelo de consenso distribuído, onde a imutabilidade, a segurança, a integridade e a privacidade são garantidas por meio de criptografia, o que torna possível a construção de soluções para o Estado que garantam a transparência, a confiança e a rastreabilidade necessárias para inibir a corrupção e a lavagem de dinheiro.

2. AFINAL, O QUE É BLOCKCHAIN?

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

2.1 Conceito

De uma forma geral, uma blockchain é um software que funciona como um livro-razão (também denominado ledger) distribuído por diversos terminais de uma rede (os "nós"). 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 de transações requer a manipulação de todos os blocos anteriores[VIII].

Todavia, é importante ressaltar que há várias outras definições, embora bastante próximas, para o termo blockchain, oriundas das mais variadas fontes internacionais, tais quais o National Institute of Standards and Technology – NIST, a Comissão Europeia[IX] e a OCDE[X].

Sob um aspecto técnico, blockchain é uma estrutura de dados que armazena transações organizadas em blocos, os quais são encadeados sequencialmente, servindo como um sistema de registros distribuído pelos "nós" da rede. Cada bloco é dividido em duas partes: cabeçalho e dados. O cabeçalho consiste em um número único que referencia um bloco, seu horário de criação e possui uma indicação para o hash (algo similar a uma "impressão digital", legível por uma sequência única de letras e números) 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)[XI].

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[XII].

Denomina-se transação 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.

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.

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, daí a possibilidade de múltipla checagem de sua autenticidade.

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[XIII] . A figura abaixo resume o funcionamento genérico de como uma transação é realizada em uma blockchain:

Figura 1 – Funcionamento genérico de uma blockchain. Fonte: Acórdão 1.613/2020 – Plenário TCU.

2.2 Componentes da tecnologia blockchain

As implementações da tecnologia blockchain incluem tipicamente os componentes detalhados na Figura 2.

2.2.1 Livro-razão distribuído (Ledger)

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 pelos nós da rede ponto-a-ponto (sem autoridades centralizadoras). Logo, o livro-razão distribuído é replicado e imutável[XIV].

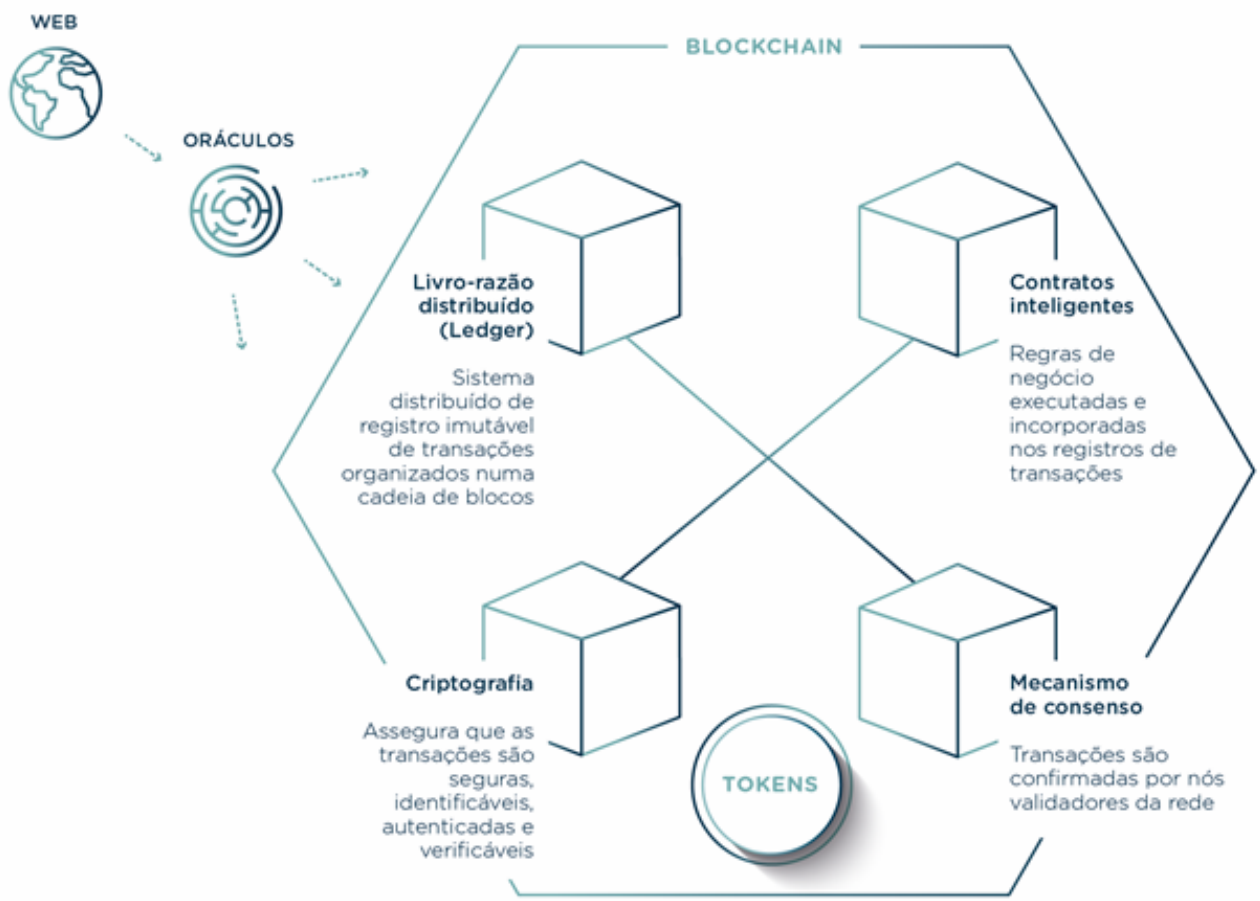


Figura 2 – Componentes da tecnologia blockchain. Fonte: Acórdão 1.613/2020 – Plenário do TCU

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.

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.

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 aceito pelas partes, eliminando a necessidade de intermediários[XV].

2.2.2 Mecanismos de consenso

O problema de se chegar ao consenso em um meio não confiável em que os nós da rede podem falhar (por questões técnicas ou ataques maliciosos) é geralmente conhecido como Problema dos Generais Bizantinos[XVI]. Considerando que as primeiras aplicações de blockchain são redes públicas e anônimas, como

garantir que os usuários dessas redes se comportem de forma honesta? Deve haver uma forma coordenada em que todas as transações sejam validadas e os nós participantes cheguem a um acordo em relação ao estado da rede.

Daí surgem os chamados mecanismos de consenso, que são as regras e procedimentos pelos quais os nós de uma rede distribuída concordam em validar transações. 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 os 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.

2.2.3 Contratos Inteligentes

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.

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.

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[XVII].

Assim, 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.

Além disso, a utilização de contratos inteligentes pode prover 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 (embora exista o custo de desenvolvimento da solução);

g. Confiança: as características citadas acima levam à maior confiança entre as partes envolvidas no contrato (embora seja necessário confiar na tecnologia).

2.2.4 Criptografia

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 guia, tendo em vista que existem diversos livros e publicações especializados que já tratam sobre o tema.

2.2.5 Tokens

Segundo o estudo do ITU[XVIII] , token é uma representação digital de valor em uma DLT cuja posse e segurança é baseada em criptografia. 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[XIX].

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[XX] . 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.

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.

Segundo algumas entidades internacionais, os tokens podem ser categorizados como:

a. Tokens de pagamento (payment tokens): são sinônimos de criptoativos, 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 investimento30. Security Tokens também são tokens que representam um ativo sob o ponto de vista de valores mobiliários[XXI]. 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.

Ressalta-se que os primeiros sistemas de blockchain, tais como bitcoin e outros criptoativos derivados do bitcoin, foram projetos voltados exclusivamente para realizarem transferências de valores em ativos 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[XXII].

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.

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")x.

2.2.6 Oráculos

Blockchains e contratos inteligentes funcionam de forma independente do mundo externo e sem necessidade de uma autoridade central. Contudo 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.

Um oráculo, no contexto de blockchains, 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.

Importante ressaltar que oráculos são serviços que não fazem parte do mecanismo de consenso da blockchain5.Em outras palavras, são serviços que verificam ocorrências do mundo físico e enviam essas informações a contratos inteligentes, desencadeando mudanças de estado na blockchain.

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.

2.3 Tipos de blockchain

Segundo a Comissão Europeiaix, 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 tipos a seguir.

Quanto à validação das transações:

Não permissionada	Permissionada
Qualquer um dos nós que compõe a rede distribuída tem permissão para validar ou confirmar transações.	Apenas alguns nós selecionados podem validar ou confirmar transações. Comumente encontrada em ambientes corporativos e na administração pública.

Quanto à autorização para realizar transações:

Pública	Privada
Neste tipo, qualquer um dos nós que compõem a rede pode participar de transações.	Em blockchains privadas, apenas participantes selecionados podem participar em transações.

Dessa conjugação, surgem quatro tipos principais, segundo a Figura 3:

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 3 – Tipos de blockchain. Fonte: Acórdão 1.613/2020 – Plenário do TCU

3. BLOCKCHAIN NO SETOR PÚBLICO DO BRASIL

A utilização da tecnologia blockchain/DLT pode ser considerada tanto 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 operações de governo, além de favorecer a abertura de dados. Assim, o fato de que vários participantes da rede mantêm seu próprio registro atualizado das transações aumenta a transparência e reduz as oportunidades de fraude, dificultando a ocorrência de delitos e comportamentos antiéticos.

Além disso, como o hash de uma transação é vinculado aos hashes de todas as transações anteriores, estas podem ser verificadas e investigadas, de modo que tentativas de adulteração passam a ser perceptíveis para os participantes da rede. Assim, a tecnologia também possibilita o rastreamento e a identificação de atividades ilegais.

O gerenciamento de dinheiro público é uma área em que soluções blockchain podem ajudar a minimizar fraudes e aumentar a transparência e a responsabilidade dos entes envolvidos. 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.

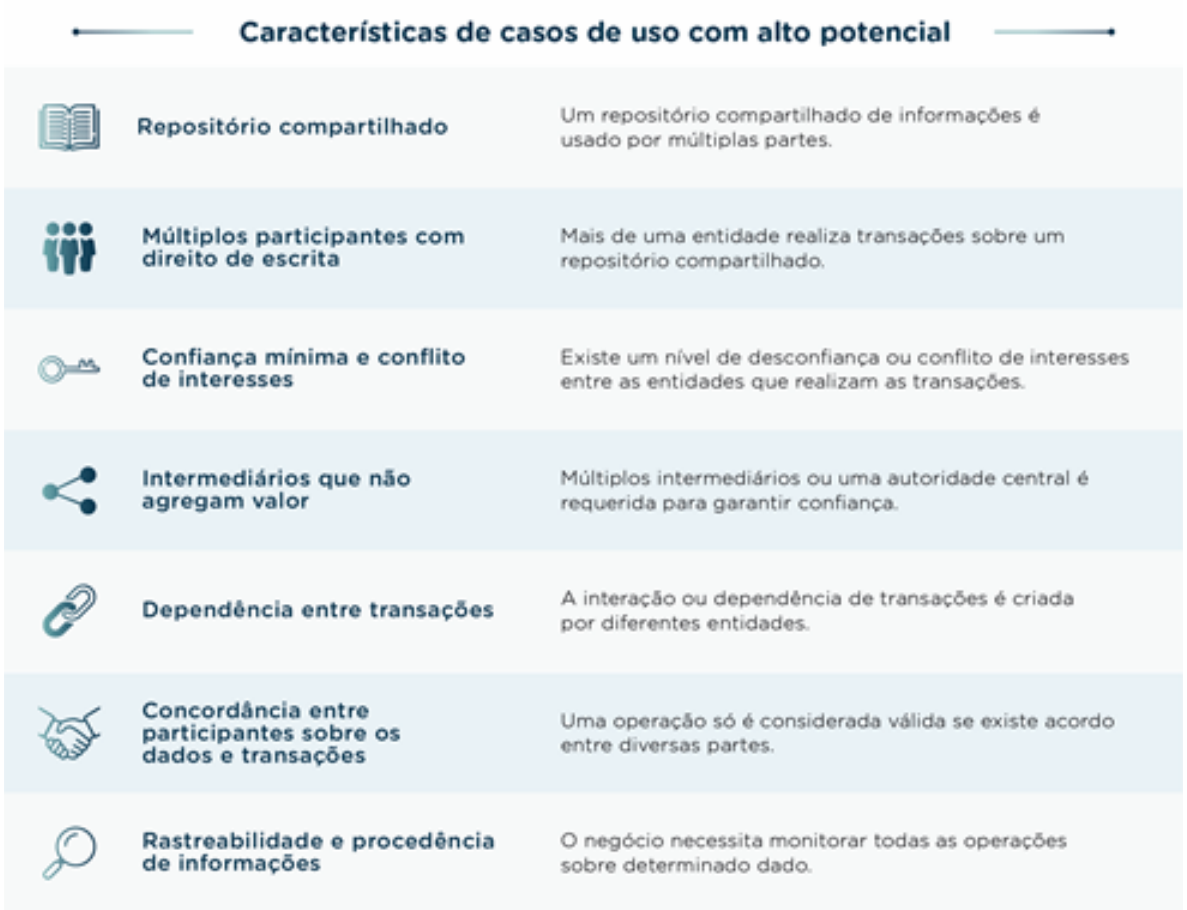
Sendo assim, nota-se o potencial da tecnologia blockchain para prevenir e detectar desvios simultaneamente em decorrência de suas características inerentes, já abordadas, promovendo assim a cultura da accountability nos serviços públicos e na realização das despesas governamentais. Todas essas vantagens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

Esta seção aborda as áreas em que as DLTs podem ser empregadas na administração pública, a utilização atual da blockchain no Brasil e seu potencial futuro.

3.1 Em que áreas a tecnologia pode transformar o setor público?

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

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 DLTs, a Figura 4 apresenta possíveis características genéricas de casos de uso com alto potencial:



Nada obstante, de acordo com os casos 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.

Neste contexto, tem-se que, dentre as diversas áreas de aplicação na ampliação e melhoria de serviços do Governo, citam-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.

Além dos casos citados, tem-se potencial para utilização das tecnologias distribuídas como alternativa para favorecer a maior abertura de dados no setor público.

3.2 Blockchain nas organizações públicas colaboradoras

Um dos objetivos do presente guia, consistente no diagnóstico do uso de tecnologias como a blockchain na Administração Pública, fora atingido por meio de informações providas pelos colaboradores designados pelos próprios órgãos, de modo a permitir um panorama, ainda que incipiente, sobre o atual estágio de uso e conhecimento de tais plataformas, que pode ser subdividido, basicamente em três níveis:

a) Utilização e operação plenas: BNDES (Trubudget[XXIV] e BNDESToken[XXV]); SERPRO (SCD); Receita Federal (b-CPF; b-CNPJ[XXVI]; b-Connect - Mercosul[XXVII]); Banco Central (PIER); TCU (Acórdão nº 1.613/2020-Plenário e participação b-CPF/b-CNPJ).

b) Estudos e utilização em estágios iniciais: AGU (Labra); CADE (participação b-CPF/b-CNPJ); CGDF (participação b-CPF/b-CNPJ); CGE-PR (Projeto Harpia); CGU; MJSP (participação b-CPF/b-CNPJ); Polícia Federal; PGFN.

c) Não utilização: AMB; MPF; MPGO; AJUFE; ABIN; CGM-SP; MPM; MPSP; MPMG; MPPR; SEPRT-ME.

É importante ressaltar que existem iniciativas nacionais no setor público que não estão citadas acima uma vez que a inclusão neste trabalho não foi validada pelas organizações responsáveis. Algumas dessas iniciativas estão descritas no Acórdão TCU nº 1.613/2020-Plenário[XXVIII].

Todavia, em que pese haver órgãos e entidades que já incorporaram a blockchain a suas rotinas, ainda não parecer haver uso consolidado e seletivo em larga escala no que se refere ao combate à corrupção ou à lavagem de dinheiro, tratando-se mais de uma consequência natural da estrutura da tecnologia do que propriamente uma ferramenta de uso direcionado. E esta é uma realidade que traz inúmeras reflexões para o futuro, no âmbito da ENCCLA.

3.3 Potencial para o futuro

O uso da blockchain habilita novos modelos federativos e colaborativos sobre o dado e abre caminho para diversas inovações que poderão surpreender a sociedade por muito tempo. Vencido o desafio histórico da confiança entre interlocutores sem a necessidade de intermediários, diversos desdobramentos se tornaram possíveis para romper as barreiras da gestão da informação, pois um grande desafio tecnológico era compartilhar a gestão do dado de forma segura.

Para ativos virtuais, a blockchain surge como potencial de um modelo de troca de recursos rápido que vai impulsionar toda a economia, desde o seu nível mais local até o nível mundial. Formas inovadoras de distribuição ou troca de riqueza se tornaram viáveis com um modelo digital auditável e confiável. Espera-se que, com o tempo, as tecnologias atuais possam ser mais interoperáveis e mais escaláveis e que possamos atingir a chamada Internet do valor - uma Internet em que seja simples e intuitivo trocar não apenas informação, mas também ativos digitais.

Como fundamento para serviços ao cidadão, a blockchain surge como uma infraestrutura relevante para viabilizar uma identidade soberana e descentralizada. No modelo de identidade soberana, passa o indivíduo a inverter a sua relação para com aqueles que detinham e gerenciavam seus dados de identificação. Se, em um primeiro momento, o cidadão se cadastrava perante o Estado e este centralizava os seus dados, no momento intermediário - que é o estado atual -, as informações passam a estar replicadas e até até desatualizadas tanto nos diversos órgãos do Estado como em diversos entes privados. No momento que se aproxima, a pessoa passará a ser gestor dos seus dados, sendo capaz de ofertar e atualizar seus dados quando achar conveniente, invertendo-se, assim, a relação da posse do dado.

Todas estas inovações são decorrentes do potencial colaborativo e federativo oferecido. Não mais se precisa pensar necessariamente em um modelo centralizado para alcançar os objetivos de estado que, em muitos cenários, já se mostrou caro, inseguro e ineficaz. Agora, é possível pensar em um modelo baseado na confiança. Confiança em quê? Confiança na tecnologia, passando-nos submeter a este ente etéreo e tecnológico chamado blockchain para nos interconectar.

A realidade tem mostrado, no entanto, que diversas barreiras dificultam o desenvolvimento de projetos em blockchain, tais como questões tecnológicas, educacionais, regulatórias, de padronização e interoperabilidade, entre outras[XXIX]. A Figura 5 apresenta uma proposição de agrupamento de ações que podem promover o desenvolvimento do ecossistema brasileiro.

Figura 5. Fonte: Serviços governamentais para cidadãos do futuro[xxx].

Os benefícios poderão ser maximizados se houver um ecossistema adequado ao desenvolvimento de novos projetos e o estabelecimento de modelos sustentáveis de negócios. Conforme discutido ao longo deste documento, o setor público possui inúmeras oportunidades de uso da tecnologia para os serviços que provê e precisa se organizar para aproveitá-las, gerando externalidades positivas para tal ecossistema com um todo.

Um exemplo concreto de ação sendo executada pelo setor público é o grupo de trabalho de blockchain do Comitê Geral de Governança de Dados (CCGD). Dentre outras atribuições, o GT, criado em julho de 2020, objetiva fomentar a criação de uma infraestrutura de blockchain, utilizando uma ou mais plataformas tecnológicas e atendendo ao Decreto nº 10.332, de 28 de abril de 2020.

trabalho de blockchain do Comitê Geral de Governança de Dados (CCGD). Dentre outras atribuições, o GT, criado em julho de 2020, objetiva fomentar a criação de uma infraestrutura de blockchain, utilizando uma ou mais plataformas tecnológicas e atendendo ao Decreto nº 10.332, de 28 de abril de 2020.

4. BLOCKCHAIN, O DIREITO BRASILEIRO E CONSIDERAÇÕES FINAIS

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 nacional. 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.

Posteriormente, diversas organizações positivaram o uso de tecnologias DLT como solução de tecnologia da informação a ser utilizada internamente em seus ambientes computacionais para prover serviços.

Normativo	Conteúdo
CONSTITUIÇÃO FEDERAL DE 1988, Art. 218.	Art. 218. O Estado promoverá e incentivará o desenvolvimento científico, a pesquisa, a capacitação científica e tecnológica e a inovação.
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.
DECRETO Nº 10.332, DE 28 DE ABRIL DE 2020	Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências.
PORTARIA RFB Nº 879, DE 20 DE MAIO DE 2020.	Altera a Portaria RFB nº 1.639, de 22 de novembro de 2016, que estabelece procedimentos para disponibilização de dados de que trata o Decreto nº 8.789, de 29 de junho de 2016 (que estabelece procedimentos para disponibilização de dados de que trata o Decreto nº 8.789, de 29 de junho de 2016).

No âmbito jurisprudencial (STF), é importante mencionar o recrudescimento das discussões quanto à possibilidade de se disponibilizar o conteúdo de comunicações privadas que se utilizam de aplicativos de qualquer natureza, inclusive quanto a eventual necessidade de ordem judicial para tanto (v.g. ADI 5.527), o que pode levar ao aprofundamento dos debates envolvendo a colisão entre intimidade da vida privada e interesse público no combate a atividades ilícitas. Referida ação direta de inconstitucionalidade fora ajuizada com o intuito de questionar dispositivos da Lei nº 12.965/14, também conhecida como marco civil da internet.

Diante desse panorama, ainda que concebido de forma sintética, percebe-se que o regime jurídico-administrativo brasileiro tem buscado conformar os mais diversos e inovadores mecanismos e plataformas às suas premissas, sempre com vistas a resguardar a supremacia do interesse público. Na seara do combate à corrupção, em especial, é importante refletir constantemente sobre o papel que o Direito deve desempenhar no estabelecimento de regras e técnicas que permitam conjugar flexibilidade e efetividade diante de novos

e cada vez maiores desafios, sem olvidar da salutar demarcação dos limites necessários à preservação de garantias fundamentais.

São essas, portanto, as inescapáveis repercussões da tecnologia da informação e comunicação sobre a vida em sociedade, às quais o Estado brasileiro não está alheio. Daí porque a continuidade da temática será bem-vinda à ENCCLA.

NOTAS E REFERÊNCIAS:

I https://bitcoin.org/bitcoin.pdf

II https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

III https://trustoverip.org

IV https://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced

V https://www.economist.com/leaders/2015/10/31/the-trust-machine

VI https://www.bloomberg.com/news/features/2015-09-01/blythe-masters-tells-banks-the-blockchain-changes-everything

VII https://www.wired.com/1993/02/crypto-rebels/

VIII CANADÁ. Chamber Of Digital Commerce. Canadian Blockchain Census 2019: Part I: Measuring Canada's Blockchain Ecosystem. 2019. Disponível em: <https://www.blockchainresearchinstitute.org/wp-content/uploads/2019/10/Chamber-BlockchainCensus-2019.pdf >. Acesso em: 8 nov. 2019.

IX The European Union Blockchain Observatory & Forum. Blockchain for Government and Public Services. 2018. Disponível em: <https://www.eublockchainforum.eu/sites/default/files/reports/eu_observatory_blockchain_in_government_services_v1_2018-12-07.pdf>. Acesso em: 5 set. 2019.

X OECD. The Tokenisation of Assets and Potential Implications for Financial Markets. Disponível em: <https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.pdf>. Acesso em: 11 fev. 2020.

XI Australian Governament. National blockchain roadmap. Disponível em: https://www.industry.gov.au/sites/default/files/2020-02/national-blockchain-roadmap.pdf. Acesso em: 11 mar. 2020.

XII CHICARINO, et al. O uso de Blockchain para Privacidade e Segurança em Internet das Coisas. Livro de minicursos do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg'17), Brasília-DF. 2017. p. 99–148. Disponível em: <https://sbseg2017.redes.unb.br/wp-ontent/uploads/2017/04/20171107-SBSeg2017-Livro_de_Minicursos.pdf>. Acesso em 21 nov. 2019.

XIII Data Foundation. Bringing Blockchain Into Government: a path forward for creating effective federal blockchain initiatives. 2019. Disponível em: <https://www.datafoundation.org/bringing-blockchain-into-government>. Acesso em: 8 nov. 2019

XIV GREVE, Fabíola, et al. Blockchain e a Revolução do Consenso sob Demanda. In Minicursos do XXXVI do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuıdos (SBRC), São Carlos-SP. 2018. 52 p. Disponível em: <http://www.sbrc2018.ufscar.br/wp-content/uploads/2018/04/Capitulo5.pdf>. Acesso em: 11 dez. 2019.

XV MAJASKI, Christina. Distributed Ledgers. Disponível em: https://blockchaincanvas.files.wordpress.com/2017/05/blockchain-canevas-ven-2016-sajida-zouarhi-cc-by-nc-sa-1-0.pdf. Acesso em: 12 mar. 2020.

XVI Byzantine fault. In: Wikipédia. Disponível em: <https://en.wikipedia.org/wiki/Byzantine_fault>. Acesso em 9 out. 2019.

XVII SZABO, N. Smart Contracts: Building Blocks for Digital Markets, 1996. Disponivel em: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. Acesso em: 12 set. 2019.

XVIII ITU Focus Group on Application of Distributed Ledger Technology. Disponível em: <https://www.itu.int/en/ITU-T/focusgroups/dlt/>. Acesso em: 3 ago 2020.

XIX ALEMANHA. Bundesministerium der Finanzen. Blockchain Strategy of the Federal Government: We Set Out the Course for the Token Economy. Disponível em: <https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/blockchain-strategy.pdf?__blob=publicationFile&v=3>. Acesso em: 11 dez. 2019.

XX VOSHMGIR, S. Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy. [S.l.]: [s.n.], 2019.

XXI MITRA, R. Utility Tokens vs Security Tokens: Learn The Difference – Ultimate Guide. Disponivel em: <https://blockgeeks.com/guides/utility-tokens-vs-security-tokens/>. Acesso em: 25 set. 2019.

XXII Symbiont. Smart contract vs “token”-based systems. Disponível em: <https://medium.com/symbiont-io/smart-contract-vs-token-based-systems-ccdd99af41e3>. Acesso em: 11 nov. 2019.

XXIII ITU-T FOCUS GROUP ON APPLICATION OF DISTRIBUTED LEDGER TECHNOLOGY (FG DLT). Technical Report FG DLT D2.1: Distributed ledger technology use cases. 2019. Disponível em: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d21.pdf>. Acesso em: 9 dez. 2019.

XXIV Trubudget - www.bndes.gov.br/trubudget

XXV BNDESToken - https://github.com/bndes/ (existem algumas versões do projeto, contemplando diferentes cenários de uso). Uma boa referência conceitual é: https://bit.ly/2Th8rHu.

XXVI https://repositorio.enap.gov.br/bitstream/1/4727/1/Relato_1_lugar__Ronald.pdf

XXVII https://www.serpro.gov.br/menu/imprensa/Releases/serpro-desenvolve-rede-blockchain-para-a-receita-federal

XXVIII https://portal.tcu.gov.br/imprensa/noticias/tcu-avalia-tecnologias-da-informacao-blockchain-e-livros-razao-distribuidos-para-o-setor-publico.htm

XXIX https://www.eublockchainforum.eu/reports

XXXhttps://www.jota.info/coberturas-especiais/inova-e-acao/servicos-governamentais-para-cidadaos-do-futuro-15102019