APÊNDICE 1

APLICAÇÕES *blockchain* NO SETOR PÚBLICO DO BRASIL

TRIBUNAL DE CONTAS DA UNIÃO

REPÚBLICA FEDERATIVA DO BRASIL

TRIBUNAL DE CONTAS DA UNIÃO

MINISTROS

José Mucio Monteiro, **Presidente**

Ana Arraes, **Vice-Presidente**
Walton Alencar Rodrigues
Benjamin Zymler
Augusto Nardes
Aroldo Cedraz de Oliveira
Raimundo Carreiro
Bruno Dantas
Vital do Rêgo

MINISTROS-SUBSTITUTOS

Augusto Sherman Cavalcanti
Marcos Bemquerer Costa
André Luís de Carvalho
Weder de Oliveira

MINISTÉRIO PÚBLICO JUNTO AO TCU

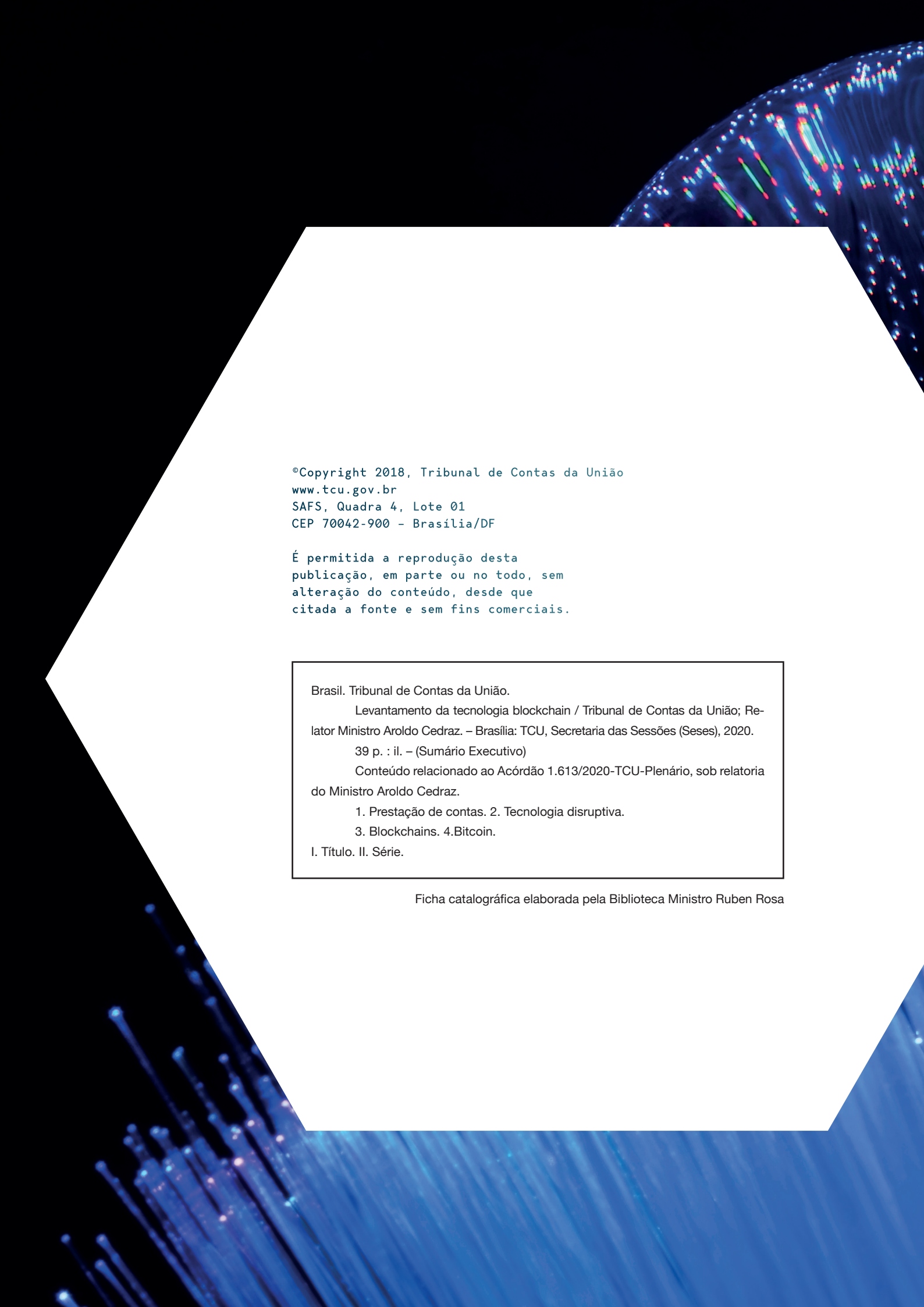
Cristina Machado da Costa e Silva, **Procuradora-Geral**
Lucas Rocha Furtado, **Subprocurador-Geral**
Paulo Soares Bugarin, **Subprocuradora-Geral**
Marinus Eduardo de Vries Marsico, **Procurador**
Júlio Marcelo de Oliveira, **Procurador**
Sergio Ricardo Costa Caribé, **Procurador**
Rodrigo Medeiros de Lima, **Procurador**

APÊNDICE 1

APLICAÇÕES *blockchain* NO SETOR PÚBLICO DO BRASIL

BRASÍLIA, 2020

TRIBUNAL DE CONTAS DA UNIÃO



©Copyright 2018, Tribunal de Contas da União
www.tcu.gov.br
SAFS, Quadra 4, Lote 01
CEP 70042-900 - Brasília/DF

É permitida a reprodução desta publicação, em parte ou no todo, sem alteração do conteúdo, desde que citada a fonte e sem fins comerciais.

Brasil. Tribunal de Contas da União.

Levantamento da tecnologia blockchain / Tribunal de Contas da União; Relator Ministro Aroldo Cedraz. – Brasília: TCU, Secretaria das Sessões (Seses), 2020.

39 p. : il. – (Sumário Executivo)

Conteúdo relacionado ao Acórdão 1.613/2020-TCU-Plenário, sob relatoria do Ministro Aroldo Cedraz.

1. Prestação de contas. 2. Tecnologia disruptiva.
3. Blockchains. 4.Bitcoin.
I. Título. II. Série.

Ficha catalográfica elaborada pela Biblioteca Ministro Ruben Rosa

1. BCONNECT (RECEITA FEDERAL DO BRASIL E SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS)

Quadro 1 – bConnect

1. Características gerais do estudo de caso					
Nível governamental envolvido	Inclui aspesctos entre outras esferas públicas ou governos estrangeiros?	Inclui aspesctos entre diversas áreas de governo ou com a iniciativa privada?	Serviço público provido/ viabilizado	Aspecto transformador	Abertura do software
Federal	Sim-países do Mercosul	Não	Troca de dados referentes ao cadastro de operadores econômicos autorizados	Resolver o problema da falta de confiança na troca de dados entre países do Mercosul, por meio da criação de uma camada de colaboração	Código aberto

2. Funcionalidades			
Funcionalidades providas	Instituições ou funções desintermediadas	Desburocratização	Combate a fraude e corrupção
Materialização de acordos bilaterais entre os países por meio de *smart contracts*	Não se aplica - solução ainda em desenvolvimento	Desponibilização de um cadastro atualizado e de forma célere contribui para a desburocratização do comércio exterior brasileiro	Não informado

3. Governança			4. Uso			
Papéis e entidades envolvidas	Tipo de blockchain	Tipo de governança	Operação atual	Capacidade esperada	Vazão suportada pela rede	Estágio
Países do Mercosul: definição nas regras de negócio e especificação técnica do projeto **Serpro:** desenvolvedor do projeto	Permissionada e privada	Descentralizada	No máximo transações por mês	Apenas países do Mercosul (quatro países)	-	Desenvolvimento

5. Arquitetura técnica				
Camada de usuário	Sistemas não-DLT	Camada API	Plataforma DLT	Detalhamento da infraestrutura DLT
Java	Sistema legados dos países	Não há	*Hyperledger*	Padrão oferecido pela plataforma *Hyperledger*

6. Custo total de propriedade		7. Benefícios	
Investimento inicial até entrada em produção	Despesas recorrentes	Benefícios quantitativos	Benefícios qualitativos
Não informado	Ainda deseconhecido	Não informados	Simplificação da atualização de cadastro de operador econômico autorizado, portanto, simplificação da importação e exportação destas empresas. Celeridade, atualização tecnológica, ineditismo

1. O bConnect corresponde a uma camada de colaboração para troca de dados entre países do Mercosul

FUNCIONALIDADES

2. A equipe da Receita Federal do Brasil (RFB) informou que, até então, por anos, não se havia chegado a um consenso de como viabilizar a troca de dados entre os países do Mercosul. Por isso, ainda se utilizava o paradigma de envio de *e-mails* para atualização de cadastros. A adoção da *blockchain* viabilizou a criação de uma camada de colaboração entre os países

3. Ainda segundo a equipe responsável, a confiança é o desafio entre os países. Por isso, a principal função é criar regras de negócio em que os países possam materializar seus acordos bilaterais de troca de informações e confiar que esses acordos serão respeitados. Isso significa que o paradigma de confiança passa a se dar pela tecnologia, de forma automática. A automatização dos acordos é viabilizada pelo uso de contratos inteligentes.

4. A solução permite disponibilizar um cadastro atualizado, de forma célere, além da fronteira brasileira, auxiliando na desburocratização do comércio exterior do país.

5. A comunicação de dados por meio de canais bilaterais, apesar de ser distribuída por todos os nós da rede, é criptografada e, portanto, só é inteligível entre o par de países envolvidos. Os nós pertencentes aos demais países não possuem as chaves criptográficas necessárias à visualização do conteúdo dos acordos, podendo, entretanto, atuar como garantidores da integridade e imutabilidade dos acordos distribuídos pela rede.

GOVERNANÇA

6. Apenas os países do Mercosul podem trocar bases de operador econômico autorizado. Com relação à tomada de decisão, todas as partes interessadas possuem um poder de decisão igualitário. Do ponto de vista da confiança, a solução é totalmente descentralizada, pois nenhum país se submete a outro.

USO

7. A equipe da RFB considera que, dado o baixo número de usuários envolvidos (apenas os nós representantes de cada um dos países do Mercosul) e de transações a serem executadas (no máximo mil transações por mês), não são necessárias medidas para garantir escalabilidade.

ARQUITETURA TÉCNICA

8. Foi utilizada a plataforma Hyperledger. As informações da base de cadastro de operadores econômicos autorizados são armazenadas fora da rede *blockchain* (*"off--chain"*). Adicionalmente, há pontos de integração com os sistemas legados de tratamento de informações dos respectivos países. Não foram relatadas APIs específicas.

CUSTOS E BENEFÍCIOS

9. De acordo com a equipe da RFB, o desenvolvimento inicial não implicou nenhum custo conhecido, uma vez que o Serviço Federal de Processamento de Dados (Serpro) se propôs a implementar o projeto sem a cobrança de valores. Com relação aos custos recorrentes, foi informado que ainda são desconhecidos, mas que seriam realizadas estimativas brevemente.

10. Dentre os benefícios qualitativos informados, estão:

- simplificação da atualização de cadastro de operador econômico autorizado e, portanto, da importação e exportação dessas empresas;
- celeridade;
- atualização tecnológica;
- Ineditismo: outros países também estão tentando fazer algo semelhante, mas o Brasil saiu na frente

2. BCPF E BCNPJ (RECEITA FEDERAL DO BRASIL E EMPRESA DE TECNOLOGIA E INFORMAÇÕES DA PREVIDÊNCIA)

Quadro 2 – bCPF e bCNPJ

1. Características gerais do estudo de caso					
Nível governamental envolvido	Inclui aspesctos entre outras esferas públicas ou governos estrangeiros?	Inclui aspesctos entre diversas áreas de governo ou com a iniciativa privada?	Serviço público provido/ viabilizado	Aspecto transformador	Abertura do software
Federal, estadual e municipal	Não	Dataprev	Compartilhamento das bases de CPF e CNPJ	Modelo federal de compartilhamento de dados	Sim

2. Funcionalidades			
Funcionalidades providas	Instituições ou funções desintermediadas	Desburocratização	Combate a fraude e corrupção
Distribuição dos dados, regras de governança em *smart contracts*	Não se aplica no curto prazo. Porém, os dados de pessoas físicas/jurídicas têm o potencial de não mais serem intermediados pela RFB, passando a haver responsabilidade compartilhada entre os órgãos participantes da rede	Redução do tempo necessário para obtenção das informações de CPF, possibilitando a redução dos tempos de resposta dos órgãos públicos às necessidades do cidadão	O não repúdio sobre a atualização dos dados permite reduzir a incidência de fraudes. A arquitetura da solução dificulta a inclusão de dados incorretos, pois todos os participantes possuem cópias que teriam que ser fraudadas ao mesmo tempo

3. Governança			4. Uso			
Papéis e entidades envolvidas	Tipo de blockchain	Tipo de governança	Operação atual	Capacidade esperada	Vazão suportada pela rede	Estágio
Receita Federal: (fundação e gestão da rede), **Secretaria de Governo Digital** (coordenação de nós na esfera federal) e **Dataprev** (Desenvolvedora de solução)	Permissionada e privada	Centralizada, atualmente, mas será descentralizada, no futuro	12,9 tps/ Mais de 200 de nós	Há previsão de que 800 convênios entre órgãos públicos e RFB sejam contemplados	Para o bCPF, a solução tem capacidade de gerar blocos a cada 15 segundos, com 2.000 transações por bloco	Em produção

5. Arquitetura técnica				
Camada de usuário	Sistemas não-DLT	Camada API	Plataforma DLT	Detalhamento da infraestrutura DLT
Java, JavaScript e Swagger (documentação de APIs)	Base ADABAS legada, que gerencia o banco CPF/CPNJ, *PosgreSQL*	API interna + APIs para consulta de pessoas físicas e jurídicas e consultas por transações	Ethereum, com previsão de migração para Heperldger	Foram desenvolvidas regras de ACL em formato de smart contracts, através de linguagem Solidity, na plataforma Ethereum. O mecanismo de consenso utilizado foi a prova de autoridade

6. Custo total de propriedade		7. Benefícios	
Investimento inicial até entrada em produção	Despesas recorrentes	Benefícios quantitativos	Benefícios qualitativos
O custo de desenvolvimento da solução bCPF foi da ordem de R$ 200 mil, segundo o Dataprev	-	Redução em 98% do custo de propagação da base CPF	Simplicidade, segurança e alinhamento com os comandos do Decreto 8.789/2016

1. As iniciativas bCPF e bCNPJ são dois projetos com objetivo de viabilizar o consumo e a colaboração sobre a base de dados do Cadastro de Pessoas Físicas (CPF) e Jurídicas (CNPJ).

2. O processo anterior ao desenvolvimento da iniciativa era a disponibilização das bases de CPF e CNPJ através de soluções cliente-servidor, do InfoConv e por convênios. As bases eram disponibilizadas tanto pelo uso de mídias físicas enviadas por correio quanto por mecanismos de *streaming.* Dado o dispêndio de manter uma infraestrutura tecnológica de alta disponibilidade (no caso de uso de arquitetura cliente-servidor), esse processo era de elevado custo para a sociedade. Deve-se citar, ainda, a dificuldade de comunicação em municípios com problemas de acesso à internet.

3. Houve, também, motivação normativa, que levou a Receita a pesquisar sobre a tecnologia, uma vez que a *blockchain* foi percebida como capaz de "resolver originalmente o comando do Decreto 8.789/2016 (revogado e substituído por normativo com finalidade semelhante – Decreto 10.046/2019)". Ademais, as recomendações do Acórdão 1.486/2019-TCU-Plenário, Rel. Min. Marcos Bemquerer, no sentido de reduzir ou extinguir determinadas obrigações advindas de deficiências de integração entre órgãos e entidades da Administração Pública federal, em relação ao compartilhamento de bases da RFB (CPF e CNPJ), também foram fatores motivadores.

4. Assim, os projetos tiveram início em 2018, tendo entrado em produção no mesmo ano. No final de 2018, o Conselho da Justiça Federal (CJF) se tornou o primeiro órgão a aderir à rede bCPF. Em 2019, a iniciativa foi expandida para criar uma rede específica para a base CNPJ, quando foi iniciado o projeto bCNPJ. Atualmente, a solução possui, também, participação ativa de outros órgãos federais, como, por exemplo, o Conselho Nacional de Justiça (CNJ) e o Instituto Nacional do Seguro Social (INSS). A RFB tem a expectativa de que entidades de todos os Poderes e esferas possam aderir à solução baseada em *blockchain*.

5. Em 2018, foi publicada a Portaria 1.788, de 19 de novembro de 2018, que define o uso de rede permissionada *blockchain* como meio de compartilhamento de dados a ser utilizado a partir de 1° de agosto de 2019.

FUNCIONALIDADES

6. O principal serviço público provido pelos projetos bCPF/bCNPJ é o compartilhamento das bases de dados CPF e CNPJ por meio do paradigma *peer-to-peer*, que permitiu criar um modelo federativo de compartilhamento de dados. Os contratos inteligentes contêm as regras de validação das informações a serem disponibilizadas na rede e identificam as responsabilidades de cada participante sobre os campos de dados. Assim, os nós descentralizados obedecem a um pacto de gestão que é materializado por regras imutáveis gravadas na própria rede *blockchain*.

GOVERNANÇA

7. Com relação às entidades envolvidas, a RFB define os seguintes papeis:

- observadores: entidades que podem participar consumindo dados;
- colaboradores: entidades que podem participar colaborando sobre os dados – colaborar é igual a sugerir modificações;
- proprietários dos dados: são os únicos responsáveis pela modificação definitiva.

8. Atualmente, o "proprietário dos dados" é apenas a RFB, que tem a prerrogativa de escrever um dado relativo ao CPF e CNPJ nas redes bCPF e bCNPJ, respectivamente. Porém, foi percebido que, em um modelo colaborativo, poderão ser viabilizados, além da RFB, outros proprietários de dados que possam integrar a rede para publicar seus próprios dados, enquanto mantêm a posse e gestão das informações. No papel "observador", poderão estar todos os órgãos da Administração Pública federal.

9. Já o conceito de "colaborador sobre o dado" refere-se a nós que podem escrever na rede com informações de suas próprias bases. A transformação da colaboração em aceitação definitiva sobre o dado na *blockchain*, no entanto, caberia apenas ao respectivo proprietário. Essa colaboração seria, então, consumida, processada pelos sistemas legados do proprietário dos dados e, caso este proprietário concordasse que a colaboração fizesse sentido e que deveria modificar o cadastro daquele lado, o proprietário faria uma publicação de alteração do dado. Desta forma, todos os nós da rede seriam informados da modificação do dado e atualizariam sua estrutura.

10. O tipo de *blockchain* utilizado é permissionada e privada, sendo uma rede fechada apenas para órgãos do governo. No que concerne à responsabilidade pela tomada de decisões, o modelo de governança atual é centralizado, mas a RFB tem a expectativa de que venha a ser descentralizado futuramente.

USO

11. O sistema atual conta com um total de duzentos nós na rede. A princípio, a maioria dos nós só consome dados que a Receita transmite para atualizar as bases CPF e CNPJ. Os blocos transmitidos têm tamanho variável entre 0,1 MB e 1 MB. Em termos de vazão, a equipe do projeto acredita, ainda, que o volume é pequeno, não tendo alcançado a capacidade de até 50.000 transações por dia. Contudo, a expectativa é que o volume cresça, pois há previsão de oitocentos convênios entre órgãos públicos e RFB a serem contemplados pelo uso da solução bCPF.

12. Como estratégia para garantia de escalabilidade, foi citada pela Empresa de Tecnologia e Informações da Previdência (Dataprev) a utilização de recursos de nuvem (Go-

vCloud), disponível tanto para os nós da RFB quanto para os participantes que optarem pela contratação da empresa para sustentação do nó.

ARQUITETURA TÉCNICA

13. Tecnicamente, o emprego da tecnologia *blockchain* consiste em apenas uma camada sobre os sistemas legados, que teve baixo custo de desenvolvimento. As atualizações cadastrais a serem realizadas pelos nós colaboradores consistirão em eventos de modificação ("deltas"), que são, por sua vez, enviados a sistemas legados, de forma que, a qualquer momento, a rede pode ser reiniciada sem nenhum impacto significativo.

14. Há uma Interface de Programação de Aplicativos (*Application Programming Interface* – API) interna à aplicação responsável por consumir o que é propagado no livro-razão e atualizar um banco de dados relacional (*PostgreSQL*), que acompanha o *container* de instalação. O banco de dados relacional, por sua vez, permite que o consumo subsequente dos dados (ex.: migração para bases legadas) seja feito por meio de ferramentas de *Extract-Transformation-Load* (ETL). Assim, a instalação inicial do container é feita por um funcionário da própria Dataprev, que instala a base original a partir de uma mídia física, gravando-a na base *PostgreeSQL*, com uma marca d'água para garantir integridade.

15. Adicionalmente, são disponibilizadas pela Dataprev APIs para consultas de pessoas físicas e jurídicas (bCPF e bCNPJ), não havendo utilização de oráculos.

16. A plataforma de *blockchain* utilizada é a *Ethereum,* com contratos inteligentes escritos na linguagem padrão da plataforma (*Solidity*). Porém, há planos para migrar a plataforma para *Hyperledger.*

17. Com relação ao desenvolvimento de contratos inteligentes, a RFB pondera que há necessidade de padronização da forma de codificação, para facilitar o entendimento entre atores de diferentes instituições.

CUSTOS E BENEFÍCIOS

18. O investimento inicial foi considerado nulo pela equipe da RFB, uma vez que o projeto foi concluído com recursos da própria Dataprev. Porém, vale ressaltar que foi dito não ter ocorrido mensuração do custo do servidor da RFB dedicado ao trabalho de pesquisa e prospecção.

19. Em termos de benefícios quantitativos, foi reportada a redução em 98% do custo de propagação da base CPF (de R$ 20.000,00 para R$ 500,00), em relação à solução antiga.

20. Ainda assim, os participantes da rede precisam contratar os serviços junto à Dataprev, que pratica um modelo comercial em que há um custo mensal de sustentação da solução diferenciado entre o nó fundador da rede, que necessita de

mais recursos, e o nó observador, que é um participante da rede com infraestrutura sustentada pela Dataprev.

21. Dentre os benefícios qualitativos, foram citados a simplicidade e segurança. Há maior resiliência do serviço, maior confiabilidade das informações, devido à consistência entre os participantes, maior segurança no compartilhamento das informações, evitando atualizações indevidas. Além disso, a frequência de atualização foi reduzida para diária, aumentando a confiabilidade e celeridade dos dados fornecidos.

22. Existem, também, ganhos indiretos, uma vez que o aprendizado com esses projetos influenciou várias outras iniciativas dentro do governo, que podem se beneficiar da arquitetura descentralizada e distribuída das Tecnologias de Registros Distribuídos (*Distributed Ledger Technologies* – DLTs).

3. SALT (BANCO CENTRAL DO BRASIL

Quadro 3 – SALT

1. Características gerais do estudo de caso					
Nível governamental envolvido	Inclui aspesctos entre outras esferas públicas ou governos estrangeiros?	Inclui aspesctos entre diversas áreas de governo ou com a iniciativa privada?	Serviço público provido/ viabilizado	Aspecto transformador	Abertura do software
Federal	Não	Não	Manutenção do sistema de liquidação de reservas, em caso de inoperância do Bacen	Consenso do sistema de liquidaçãi sem necessidade de agente central	Sim

2. Funcionalidades			
Funcionalidades providas	Instituições ou funções desintermediadas	Desburocratização	Combate a fraude e corrupção
Liquidação descentralizada de transações	Sistema do próprio Bacen	A liquidação descentralizada não exige mais um agente público operando na rede	Um único agente poderia apresentar informações fraudulentas. Com a utilização de uma rede baseada em consenso, é necessário corromper a moaioria dos seus agentes para fraudar os dados

3. Governança			4. Uso			
Papéis e entidades envolvidas	Tipo de blockchain	Tipo de governança	Operação atual	Capacidade esperada	Vazão suportada pela rede	Estágio
Instituições financeiras: implementam a rede e fazem parte do consenso **Bacen:** desenvolve o sistema e inicia a operação	Permissionada e privada	Centralizada	-	-	O sistema não entrou em produção, mas estima-se que deva ser capaz de processar milhares de transações por dia	Prova de conceito

5. Arquitetura técnica				
Camada de usuário	Sistemas não-DLT	Camada API	Plataforma DLT	Detalhamento da infraestrutura DLT
Javascript e - *Angular JS*	Plataforma RTGS centralizada	Não há	*Quorum*	Consenso Raff, mas, em produção, seria necessário um método de consenso resistente a falhas bizantinas

6. Custo total de propriedade		7. Benefícios	
Investimento inicial até entrada em produção	Despesas recorrentes	Benefícios quantitativos	Benefícios qualitativos
Custo com alocação de servidores	Custo com alocação de servidores	Menor tempo de interrupção no sistema de liquidação de transações	Maior resiliência no sistema financeiro

1. O Sistema Alternativo de Liquidação de Transações (SALT) consiste em uma proposta de plataforma de contingência a ser utilizada em caso de pane do "Sistema de Transferência de Reservas". O objetivo é que essa solução seja totalmente independente de um Banco Central, sendo capaz de funcionar apenas com a colaboração dos participantes do sistema financeiro. Fazendo uso das virtudes de DLT, como a ausência de entidade central e garantia de integridade dos dados por criptografia, a equipe projetou um sistema que permite o funcionamento do Sistema Financeiro Nacional (SFN) sem a participação do banco, caso ocorra falha completa dos sistemas de TI da entidade reguladora.

2. O projeto foi iniciado no final de 2016, quando, inicialmente, o Banco instituiu um grupo de estudos voltado para avaliar e analisar as plataformas *blockchain* atuais, com o objetivo de melhor entender tanto a aplicabilidade quanto as limitações da tecnologia. De acordo com publicação do próprio banco, "um livro-razão confiável e imutável pode ser uma ferramenta ideal para atacar soluções para situações que podem se beneficiar de descentralização completa e resiliência a falhas individuais, vindo a ser um bom candidato para um grande conjunto de problemas previamente inexplorados" (tradução livre).

3. O SALT foi considerado pelo grupo de estudo um candidato ideal: os requisitos funcionais foram considerados simples e havia disponibilidade das partes. Ex.: bancos comerciais no alcance do Banco Central do Brasil (Bacen).

4. A solução de contingência desenvolvida inclui uma rede *blockchain* permissionada em que instituições financeiras (IFs) e Bacen são nós validadores, utilizando a internet como infraestrutura de comunicação. Os nós compartilham um livro-razão distribuído que contém o estado das reservas de cada instituição e são capazes de continuar executando transações entre si por meio de contratos inteligentes, na total ausência de supervisão do Bacen.

FUNCIONALIDADES

5. O aspecto transformador é a criação de um sistema de liquidação distribuído que trabalhe com mecanismo de consenso independente de um agente central. Com isso, torna-se possível a liquidação descentralizada de transações, de forma resiliente, uma vez que o sistema permite a manutenção do sistema de liquidação de reservas, em caso de inoperância do Bacen.

6. Em termos de desintermediação e desburocratização, a principal instituição a ser desintermediada é o próprio Bacen, uma vez que a liquidação descentralizada de transações não requer a presença de um agente público operando na rede.

7. Do ponto de vista do combate a fraude e corrupção, a solução mitiga o risco de um agente central apresentar informações fraudulentas.

GOVERNANÇA

8. As principais entidades envolvidas incluem as IFs, que implementam a rede e fazem parte das verificações de consenso, e o próprio Bacen, responsável pelo desenvolvimento do sistema e início de sua operação.

9. Com relação à estrutura de governança adotada, é centralizada no Bacen, papel resultante da responsabilidade do órgão pela implantação do serviço.

USO

10. A solução concluiu a etapa de prova de conceito, mas ainda não entrou em produção, devido a questões de priorização estratégica do próprio órgão. Como consequência, a equipe técnica afirmou não ser capaz de precisar numericamente a demanda de uso. Porém, estima que o sistema deva ser capaz de processar alguns milhares de transações por dia". Essa informação tem como base experimentos já feitos por terceiros na plataforma em utilização. A equipe acredita que a estimativa atenderia à demanda esperada em uma futura implantação em produção.

11. A preocupação com vazão e escalabilidade é mitigada pelo fato de que o sistema deverá ser voltado apenas para ordens de pagamento, que obrigatoriamente precisam passar pelo Bacen. Hoje, essas transações possuem um número baixo de ocorrências.

ARQUITETURA TÉCNICA

12. No início do projeto, a equipe identificou que a transparência intrínseca das redes *blockchain* infringe os requisitos de privacidade entre IFs. A simples abordagem de armazenar saldos no livro-razão e aprovar transações assinadas com base em lógica de negócio codificada não seria suficiente, uma vez que revelaria dados financeiros sensíveis a todos os participantes. Criptografar dados sensíveis também não seria uma solução viável: sem acesso a todos os dados, contratos inteligentes nas plataformas disponíveis não podem decidir se uma transação é válida. Esse dilema mostrou ser um desafio maior do que o esperado.

13. Diferentes plataformas foram testadas. Os protótipos foram construídos utilizando as plataformas *BlockApps* (baseada em *Ethereum*), *Hyperledger Fabric, Corda e Quorum*.

14. A plataforma escolhida foi a *Quorum*, que é otimizada, por exemplo, para suporte a informações privadas e implementação de canais privados, o que atende a um dos requisitos do projeto SALT: a privacidade entre participantes, segundo a qual uma instituição não pode enxergar o saldo de outra nem as transações entre outras duas instituições.

15. Foi citado que, durante o desenvolvimento da solução, a equipe se deparou com um trilema: continuidade na ausência do regulador, privacidade e garantia de saldos. Em todas as plataformas testadas na época, apenas dois desses três requisitos eram atingidos.

16. Contratos inteligentes são utilizados para controlar os saldos e liquidar as transações. Na camada de apresentação, são utilizadas as tecnologias *JavaScript* e *AngularJS*.

17. Com relação a sistemas *off-chain*, foi apontado que o sistema deve ser capaz de se sincronizar com uma plataforma centralizada *Real-time Gross Settlement* (RTGS). Até o momento, não foi necessária a construção de APIs ou o uso de oráculos.

18. O mecanismo de consenso empregado é *Raft*, mas foi apontado que, em produção, seria necessário um mecanismo resistente a falhas bizantinas.

CUSTOS E BENEFÍCIOS

19. Considerando que o sistema ainda não entrou em produção, o único custo foi referente aos salários dos analistas internos envolvidos no desenvolvimento. Para despesas recorrentes, estimam o custo equivalente a um servidor com dedicação integral ou dois, em dedicação parcial.

20. Os benefícios reportados foram os seguintes:

- quantitativo: menor tempo de interrupção no sistema de liquidação de transações, embora essa redução não tenha sido especificada numericamente;

- qualitativo: maior resiliência no sistema financeiro.

4. PIER (BANCO CENTRAL DO BRASIL)

Quadro 4 – PIER

1. Características gerais do estudo de caso					
Nível governamental envolvido	Inclui aspesctos entre outras esferas públicas ou governos estrangeiros?	Inclui aspesctos entre diversas áreas de governo ou com a iniciativa privada?	Serviço público provido/ viabilizado	Aspecto transformador	Abertura do software
Federal	Não	CVM, Susep e instituições financeiras	Registro da interação entre instituições financeiras e órgãos regulatórios	Imutabilidade e auditabilidade das informações trocadas	Sim

2. Funcionalidades			
Funcionalidades providas	Instituições ou funções desintermediadas	Desburocratização	Combate a fraude e corrupção
Troca de informações entre IFs e órgãos reguladores acerca do processo decisório (escolha de diretores) de IFs/Rastreabilidade e maior agilidade no processo/ Não repúdio	Autenticidade baseada na comunicação mediante oficio	Maior agilidade no processo, que antes era operacionalizado por e-mail, suscetível a falhas humanas	Evita que uma pessoa inapropriada ou má intencionada atue na direção de uma instituição financeira

3. Governança			4. Uso			
Papéis e entidades envolvidas	Tipo de blockchain	Tipo de governança	Operação atual	Capacidade esperada	Vazão suportada pela rede	Estágio
Bacen, CVM e Susep validam a indicação de diretores indicados por instiuições financeiras	Permissionada e privada	Descentralizada	3 nós: Bacen, CVM e Susep 30 a 100 transações por mês	Não há demanda por alto desempenho em vazão. O processo é espaçado e esporádico	Em modelos similares	Prova de conceito

5. Arquitetura técnica				
Camada de usuário	Sistemas não-DLT	Camada API	Plataforma DLT	Detalhamento da infraestrutura DLT
Angular JS	Olinda - entrega dados de banco de dados via *web services*	Não há	*Quorum*	Smart contracts escritos na linguagem *Solidity*/ Mecanismo de consenso

6. Custo total de propriedade		7. Benefícios	
Investimento inicial até entrada em produção	Despesas recorrentes	Benefícios quantitativos	Benefícios qualitativos
Custo de pessoal: quatro analistas durante oito meses no desenvolvimento do projeto	Custo de pessoal: um analista em tempo parcial para manutenção do projeto	Redução de tempo no processo de solicitação e resposta entre as entidades envolvidas, de dias para segundos	Auditabilidade das informações trocadas. Menor risco de erros em relação à troca de informações por *e-mail*

1. A Plataforma de Integração de Informações das Entidades Reguladoras (PIER), projeto iniciado no segundo semestre de 2017, foi desenvolvida pelo Departamento de Tecnologia da Informação (Deinf) do Bacen.

2. Antes da plataforma PIER, os processos autorizativos, como, por exemplo, a indicação de diretores para IFs, eram feitos por *e-mail*. As mensagens de *e-mail* eram trocadas entre as IFs e os órgãos que regulam o sistema financeiro, por exemplo, Bacen, Comissão de Valores Mobiliários (CVM), Superintendência de Seguros Privados (Susep) e Superintendência Nacional de Previdência Complementar (Previc). A demora na autorização dos órgãos reguladores, os riscos envolvidos na operação e a baixa rastreabilidade e auditabilidade das informações trocadas foram as grandes motivações para o desenvolvimento da PIER.

3. PIER permite que dados sejam trocados em plataforma *blockchain*, otimizando os processos autorizativos, como a verificação de penalidades e sanções de um indicado a dirigente no sistema financeiro perante as demais entidades reguladoras.

FUNCIONALIDADES

4. O principal serviço provido pela PIER é a transparência e resposta célere às solicitações de IFs nos processos autorizativos, envolvendo o Bacen, a CVM e a Susep.

5. No início do processo, estruturas de dados (metadados) e capacidades de consulta e resposta foram acordadas entre órgãos reguladores e IFs. Tais estruturas definiram quais informações seriam trocadas entre IFs e quais serviços de consulta e resposta seriam oferecidos mutuamente entre as entidades envolvidas. Os acordos foram registrados na *blockchain* utilizada na PIER.

6. Após a definição das estruturas de dados e dos serviços de consulta e resposta, os respectivos eventos são registrados em *blockchain*. Com isso, a solução provê rastreabilidade e auditabilidade, já que os registros em *blockchain* são feitos de forma imutável e com indicação clara dos atores envolvidos e papéis desempenhados por cada um.

7. Com o suporte a canais privados entre os participantes, a PIER permite que os dados sensíveis sejam mantidos em sigilo, de modo que os outros nós da blockchain/DLT enxergam somente o hash das informações, para fins de validação do livro-razão.

GOVERNANÇA

8. A governança da solução é feita de forma descentralizada, por um comitê formado pelos órgãos reguladores envolvidos.

USO

9. Até setembro de 2019, 170 requisições foram trocadas entre IFs e órgãos de controle. O tempo médio de instalação de um novo nó na PIER é de dois dias. Segundo técnicos do Bacen, a escalabilidade não é um problema para a PIER até o momento, dado que o número de transações é baixo.

ARQUITETURA TÉCNICA

10. Olinda é um *broker* desenvolvido no âmbito do Bacen. A ferramenta permite a extração de dados de bancos de dados relacionais de forma agnóstica, ou seja, não importa qual seja o banco de dados relacional. Olinda consegue expor esses dados via *web services*. A ferramenta Olinda é pré-requisito para o funcionamento da PIER.

11. Uma aplicação em *frontend* em *AngularJS* é usada para acesso às funcionalidades da PIER.

12. A rede Quorum (uma derivação da Ethereum) foi utilizada para implementação da PIER, pois, na época do início do desenvolvimento, era uma das poucas soluções que permitiam o uso de canais privados entre nós.

CUSTOS E BENEFÍCIOS

13. O desenvolvimento do projeto se deu exclusivamente com profissionais da instituição, sendo contabilizado o desembolso com salário para quatro analistas, durante oito meses, no desenvolvimento do projeto, além do salário de um analista que dá manutenção ao sistema em tempo parcial.

14. Os benefícios reportados foram os seguintes:

- quantitativo: redução do tempo de reposta nos processos administrativos. Anteriormente, a comunicação por meio de ofícios costumava levar dias;
- qualitativos: auditabilidade das informações trocadas entre as entidades reguladores; e menor risco de erro, por não haver intervenção manual.

5. SISTEMA DE CONTRATOS DISTRIBUÍDOS (BANCO DO BRASIL, BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL, CAIXA ECONÔMICA FEDERAL E SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS)

Quadro 5 – Sistema de Contratos Distribuídos

1. Características gerais do estudo de caso					
Nível governamental envolvido	Inclui aspesctos entre outras esferas públicas ou governos estrangeiros?	Inclui aspesctos entre diversas áreas de governo ou com a iniciativa privada?	Serviço público provido/ viabilizado	Aspecto transformador	Abertura do software
Federal, mas poderá estender para Estadual e Municipal	Não	Não	Compartilhamento de informações padronizadas sobre processos públicos de compra	Empresas públicas poderão passar a compartilhar informações diretamente, de maneira mais célere e padronizada	Código aberto

2. Funcionalidades			
Funcionalidades providas	Instituições ou funções desintermediadas	Desburocratização	Combate a fraude e corrupção
Compartilhamento de informações relativas a processos de compra	je, os participantes da rede contratam o serviço de terceiros, para levantar informações relevantes das bases públicas dos contratos governamentais. O SCD eliminará esta necessidade	Agilização dos processos de compra Compartilhamento dos contratos Comparação de preços com base histórica	Auditoria facilitada. Possível exposição dos contratos no portal da transparência. Automatização da gestão do ciclo de vida das contratações, reduzindo a possibilidade de má-fé na gestão

3. Governança			4. Uso			
Papéis e entidades envolvidas	Tipo de blockchain	Tipo de governança	Demanda atual	Capacidade esperada	Vazão suportada pela rede	Estágio
Empresas públicas, órgãos de controle e Serpro (desenvolvedor)	Permissionada e privada	Descentralizada	Volume transacional é baixo	Espera-se a participação de todas as empresas públicas. Poderá suportar milhares de registros por dia	Hyperledger Fabric tem publicado um volume transacional de 3.500 tps	Pré-produção

5. Arquitetura técnica				
Camada de usuário	Sistemas não-DLT	Camada API	Plataforma DLT	Detalhamento da infraestrutura DLT
React JS para *front-end web*	Bancos de dados e índices NoSQL. Sistemas legados de cada órgão	APIs para integração com sistemas legados e diretórios de usuários	*Hyperledger Fabric*	Consenso BFT e *KAFKA/ ZooKeeper*. Está sendo estudado o uso do Raft, *CouchDB NodeJs* nos *chaincodes*

6. Custo total de propriedade		7. Benefícios	
Investimento inicial até entrada em produção	Despesas recorrentes	Benefícios quantitativos	Benefícios qualitativos
Não está em produção. Cada organização custeia a sua própria equipe	Ainda não há despesas recorrentes	Espera-se redução do tempo gasto no processo de precificação de um item, em função de dias para minutos e, consequentemente, a redução do número de pessoas dedicadas a esta tarefa	Potencial de uso dos dados armazenados na rede para análises preditivas. Melhora na qualidade dos dados, maior precisão na precificação do item. A longo prazo, espera-se uma menor intervenção manual, tornando-se menos suscetível a erros e desvios

1. O objetivo deste projeto consiste no desenvolvimento de um sistema a ser utilizado para compartilhar informações sobre contratações feitas por empresas públicas que, por lei, podem reaproveitar etapas da contratação (consulta pública, oferta pública, contratação) de outras empresas públicas, mas que hoje não conseguem pôr em prática de maneira eficiente.

FUNCIONALIDADES

2. A principal funcionalidade a ser provida é a possibilidade de compartilhamento de informações sobre processos públicos de compra, como a consulta pública, a oferta pública e as aquisições de bens ou contratações de serviços. A carga inicial foi de apenas contratos de TI, porém a intenção é incluir todos os tipos de contratos.

3. Até então, as empresas públicas compartilham essas informações por *e-mail* e/ou alguns sítios específicos, sem a abrangência necessária. Havia, também, problemas de disponibilidade e padronização das informações neles armazenadas, uma vez que os normativos atuais não prescrevem adequadamente quais campos devem ser armazenados, dificultando, portanto, a consulta de informações. Diante dessas limitações, decidiu-se pela construção de um novo sistema, baseado em *blockchain*, como alternativa às manutenções evolutivas no sistema Comprasnet.

4. Com a nova solução, as entidades poderão compartilhar essas informações diretamente entre elas, de maneira oficial, padronizada e com histórico, em tempo real e com baixo custo. Para garantir a confiabilidade dos dados, a aplicação prevê que informações inconsistentes registradas no livro-razão sejam substituídas por uma transação de correção, sendo que o registro mais novo passa a ser considerado o registro válido.

5. Contratos inteligentes são utilizados para registro das informações de maneira controlada, uma vez que somente a empresa pode fazer o registro em seu próprio nome, bem como para verificação da coerência das informações. O projeto prevê a padronização dos itens que serão objeto dos contratos de compra, permitindo, ainda, um “de/para” do padrão com os sistemas legados.

6. Do ponto de vista de desintermediação, como atualmente os participantes da rede necessitam contratar serviço de terceiros para conseguir levantar informações relevantes das bases públicas dos contratos governamentais, com a implementação do Sistema de Contratos Distribuídos (SCD), não haverá mais necessidade dessas contratações.

7. Do ponto de vista de desburocratização, foram citados os seguintes impactos

- agilização dos processos de compra;
- · compartilhamento dos contratos;
- comparação de preços com a base histórica.

8. Do ponto de vista de combate a fraudes, o sistema garante a auditabilidade, com possibilidade de exposição dos contratos no portal da transparência, para visualização por qualquer cidadão. Além disso, pretende-se que toda a gestão do ciclo de vida das contratações seja realizada por meio de contratos inteligentes, o que reduzirá a possibilidade de erros humanos e má-fé na execução da gestão.

9. A equipe do projeto acredita que a solução tem o potencial de vir a ser utilizada por toda a Administração federal, além de estados e municípios. Órgãos que porventura não tenham capacidade ou disponibilidade para instalar um nó na rede poderão consultar informações por meio de API a ser disponibilizada pelo Serpro.

GOVERNANÇA

10. Como entidades que podem participar da rede, foram citadas:

- empresas públicas: compartilhando e consultando processos de compra;
- órgãos de controle (ex.: TCU): auditando contratos;
- Serpro: provendo infraestrutura para as empresas públicas que desejarem aderir à rede.

11. A estrutura de governança é descentralizada, estando o poder de decisão centrado nos membros fundadores. Os membros fundadores decidem quem pode entrar no consórcio e como se dará a evolução do sistema.

12. Participaram do desenvolvimento da rede: Banco do Brasil (BB), Banco Nacional de Desenvolvimento Econômico e Social (BNDES), Caixa Econômica Federal (CEF) e Serpro, embora, devido a mudanças internas recentes, o BNDES tenha precisado deixar a rede. Os três participantes remanescentes são os membros fundadores da rede e exercem o mesmo papel no acordo de parceria técnica, contribuindo com o desenvolvimento e gerenciamento da própria infraestrutura.

ARQUITETURA TÉCNICA

13. Na camada de apresentação, é utilizado o *framework ReactJS*.

14. A plataforma de *blockchain* empregada é o *Hyperledger Fabric*. Nessa plataforma, o suporte pode ser contratado com diversas empresas, com modelos de negócio diferentes.

15. O código dos contratos inteligentes (*"chain code"*) é escrito em *NodeJS* e contém toda a lógica de negócio do sistema.

16. Atualmente, são utilizados como mecanismos de consenso pBFT e KAFKA/*ZooKeeper*. Entretanto, a equipe do projeto está estudando o uso de *Raft*.

17. Os processos de contratação são executados em sistemas específicos das instituições participantes. As tecnologias *off-chain* envolvidas variam entre as instituições. São utilizados bancos de dados *NoSQL*. A solução se integra aos sistemas legados de gestão de contratos de cada órgão. São armazenados índices para agilizar a busca por informações no sistema.

18. Atualmente, APIs são utilizadas para alimentar a DLT com informações dos sistemas legados de gestão de contratos. O acesso às informações pelos usuários das organizações também deverá ocorrer mediante o uso dos sistemas de cada entidade.

USO

19. Com relação à demanda de uso, a equipe desenvolvedora espera a participação de todas as empresas públicas, embora não tenha traduzido em termos numéricos tal demanda. Com relação à vazão esperada, assume como premissa que o volume transacional é baixo, mesmo comparando o cenário de milhares de contratações por semana frente à capacidade das plataformas atuais. Foi citado como exemplo o fato de que a plataforma de *blockchain* utilizada tem publicado um volume transacional na ordem de 3.500 transações por segundo, sendo a previsão de registros da ordem de milhares por dia entre todas as empresas.

20. A equipe do projeto não vê necessidade de estabelecimento de estratégias para garantia de escalabilidade, uma vez que "quase todo o processo é executado *off-chai*n, sendo compartilhado somente o registro da consulta pública, oferta pública e contratação, reduzindo muito o número de interações necessárias com a *blockchain*".

21. Nada obstante, a preocupação atual é com disponibilidade. A equipe tem estudado como garantir uma arquitetura que mitigue pontos de falha, como o uso do serviço de ordenação do *Raft*.

CUSTOS E BENEFÍCIOS

22. O custo reportado pela equipe do BB se refere ao valor total gasto em licenciamento de *software*/suporte técnico para o conjunto de projetos em andamento. O custo individual por projeto não está disponível, uma vez que existem vários projetos em andamento que tratam da tecnologia *blockchain*.

23. Para o Serpro, desenvolvedor do projeto, não houve investimento por parte da empresa em capacitação, contratação de hardware ou com licença de *software.* A pesquisa e gerência de projeto são executadas pelas equipes das organizações, que contam com cerca de cinco ou seis pessoas ao todo por organização. No entanto,

nenhuma pessoa está alocada em tempo integral ao projeto. Cada organização custeia sua própria equipe. O custo total (direto e indireto) com pessoal, incluindo viagens, foi da ordem de R$ 750 mil, em 2018, para o Serpro.

24. Dentre os benefícios quantitativos, foram citados melhores preços nas contratações, devido à base histórica de contratos entre empresas públicas, além da redução do tempo gasto no processo de precificação de um item, de dias para minutos, e, consequentemente, do número de pessoas dedicadas a essa tarefa.

25. Como benefício qualitativo, está o potencial de uso dos dados armazenados na rede para análises preditivas. Espera-se, também, melhora na qualidade dos dados e mais precisão na precificação do item. A longo prazo, espera-se que todo o processo de gestão de contratos se beneficie, tornando-se uma atividade que requeira menos intervenção manual e esteja menos suscetível a erros e desvios.

6. SISTEMA FINANCEIRO DIGITAL (BANCO DO BRASIL)

Quadro 6 – Sistema Financeiro Digital

1. Características gerais do estudo de caso					
Nível governamental envolvido	Inclui aspesctos entre outras esferas públicas ou governos estrangeiros?	Inclui aspesctos entre diversas áreas de governo ou com a iniciativa privada?	Serviço público provido/ viabilizado	Aspecto transformador	Abertura do software
Federal	Não	Não	Liquidação financeira, descentralizada, entre instituições financeiras diferentes em poucos segundos	Sistema de pagamentos *online* mediante *smartphones*	Código aberto

2. Funcionalidades			
Funcionalidades providas	Instituições ou funções desintermediadas	Desburocratização	Combate a fraude e corrupção
Liquidação financeira descentralizada com uso de infraestrutura blockchain	Câmaras de compensação que fazem o serviço de intermediador nas liquidações financeiras entre instituições	Simplificação nas relações de consumo entre PFs e PJs por simplificar a forma de pagamento	Nenhum aspecto identificado

3. Governança			4. Uso			
Papéis e entidades envolvidas	Tipo de blockchain	Tipo de governança	Operação atual	Capacidade esperada	Vazão suportada pela rede	Estágio
BCB é o órgão regulador. **Instituições Financeiras** podem participar da rede blockchain de forma direta ou indireta	Permissionada e privada	Descentralizada – todas as instituições financeiras possuem um poder de decisão igualitário	Menor que 2400 transações por segundo	O SFD será capaz de atender à demanda por transferências financeiras executadas hoje por DOC e TED	2.400 transações por segundo	Em desenvolvimento

5. Arquitetura técnica				
Camada de usuário	Sistemas não-DLT	Camada API	Plataforma DLT	Detalhamento da infraestrutura DLT
Aplicativos móveis de Internet Banking com acesso aos contatos do cliente e *QR Code.* Piloto em *React Native*	Integração com o sistema do Banco do Brasil – EVT – para contabilidade	Não informado	*Hyperledger*	*Smart contracts* escritos em *JavaScript (NodeJS).* Mecanismo de consenso BFT

6. Custo total de propriedade		7. Benefícios	
Investimento inicial até entrada em produção	Despesas recorrentes	Benefícios quantitativos	Benefícios qualitativos
O projeto está em desenvolvimento há 2 anos, com 5 funcionários dedicados	Contrato anual de suporte da plataforma blockchain	Menor tempo no processamento das transações financeiras e possibilidade de redução de tarifas bancárias e custos com numerários. Maior disponibilidade do serviço de transferências e pagamentos, 24 horas por dia, 7 dias por semana	Melhor experiência para os clientes bancários nas transferências de valores e pagamentos Menor necessidade de impressão de cédulas (redução de custos com numerários). Simplificação de transferências de valores via QR Codes. Redução no uso de boletos bancários, TEDs e DOCs

1. O Sistema Financeiro Digital (SFD) propõe a estruturação de uma rede permissionada baseada em *blockchain*, interligando diversas IFs, sobre a qual serão realizadas transferências de valores e pagamentos de forma simplificada, por meio de aplicativo *mobile banking* (aplicativo de celular específico para clientes dos bancos participantes), modernizando o sistema financeiro e oferecendo uma experiência intuitiva para os clientes.

2. Com uso intenso de tecnologia das chamadas *fintechs*, empresas (*startups*) dedicadas à inovação e otimização dos serviços do sistema financeiro, a forma como as transferências de valores e os pagamentos ocorrem tem se transformado. Em um mundo cada vez mais digital, a exigência dos clientes desses serviços vai além de horários e dias pré-estabelecidos para efetivação de transferências e pagamentos.

3. Nesse cenário, alternativas aos serviços tradicionais de pagamento e transferência, como Transferências Eletrônicas Disponíveis (TEDs), Documentos de Ordem de Crédito (DOCs), boletos e cartões de crédito, para citar alguns, têm surgido, em geral, oferecidas por centenas de fintechs no Brasil e no mundo.

4. Segundo o BB, é inevitável que o sistema bancário brasileiro, mais especificamente os serviços de transferência de valores e pagamento, sejam impactados por esse movimento mundial. Em razão disto, o BB tem se preparado para manter sua competitividade no mercado financeiro brasileiro. O SFD é, em alguma medida, uma resposta a essa transformação e à competição das *fintechs* e grandes empresas internacionais no mercado de transferência de valores e pagamento.

FUNCIONALIDADES

5. A transferência de valores de forma “imediata” (alguns segundos) e simplificada entre clientes bancários, apenas com o uso do número de telefone como referência aos dados bancários, por meio do *mobile banking* de cada instituição financeira ou de uma aplicação com essa funcionalidade específica, substitui as TEDs e os DOCs atuais.

6. No SFD, lotes de transações são liquidados de uma única vez. Um lote de liquidação é executado a cada 200 milissegundos. Ressalta-se que há garantia de sigilo bancário, tendo em vista que as transações não são visíveis a outros bancos e os detalhes de pessoas físicas são criptografados.

7. Há a simplificação de pagamentos a pessoas jurídicas por transferência “imediata” de valores entre contas correntes, onde *QR Codes* podem ser utilizados para pagamento em estabelecimentos comerciais presenciais, comércio eletrônico, além de disponibilidade dos serviços supracitados nos sete dias da semana, 24 horas por dia.

GOVERNANÇA

8. CEF e Sistema de Cooperativas de Crédito (Sicoob) são parceiros no desenvolvimento do projeto. Contatos constantes com o Bacen também foram relatados pelo BB.

9. As IFs pioneiras avaliam e deliberam sobre a entrada de novos participantes na rede.

USO

10. O SFD está preparado para atender mais de 2.400 transações por segundo. Atualmente, a demanda atual é menor que essa.

ARQUITETURA TÉCNICA

11. A aplicação cliente móvel foi desenvolvida em *React Native*. Há integração com os sistemas legados do BB para contabilidade (sistema EVT). A plataforma de *blockchain* utilizada é o *Hyperledger Fabric*, utilizando mecanismo de consenso baseado em pBFT e contratos inteligentes escritos em *NodeJS.*

CUSTOS E BENEFÍCIOS

12. As despesas do projeto estão relacionadas à alocação integral de cinco funcionários pelos dois anos de desenvolvimento. Além disso, há desembolso com contratação do suporte e manutenção da plataforma de *blockchain.*

13. Como benefícios, pretende-se reduzir o custo de numerário (papel-moeda), que, somente em 2017, foi de, aproximadamente, R$ 89 bilhões. Espera-se, ainda, reduzir o tempo das transações financeiras e as tarifas.

7. SISTEMA BRASILEIRO DE PODERES (BANCO DO BRASIL E PETROBRAS)

Quadro 7 – Sistema Brasileiro de Poderes

1. Características gerais do estudo de caso					
Nível governamental envolvido	Inclui aspesctos entre outras esferas públicas ou governos estrangeiros?	Inclui aspesctos entre diversas áreas de governo ou com a iniciativa privada?	Serviço público provido/ viabilizado	Aspecto transformador	Abertura do software
Federal, Estadual e Municipal	Não	Não	Designação de permissões (poderes) para a movimentação de contas bancárias por grandes corporações ou por governos	Processo passa a ser digital, sem intermendiários e *on-line*, com visibilidade e audtabilidade	Código aberto

2. Funcionalidades			
Funcionalidades providas	Instituições ou funções desintermediadas	Desburocratização	Combate a fraude e corrupção
Registro da cadeia de poderes	Bancos, empresas com contas nestes bancos, TSE e prefeituras	Digitização do processo, remoção de intermediários e redução do tempo necessário para o registro de poderes	Redução no tempo necessário para cancelar permissões de movimentação de conta-corrente por funcionários demitidos

3. Governança			4. Uso			
Papéis e entidades envolvidas	Tipo de blockchain	Tipo de governança	Operação atual	Capacidade esperada	Vazão suportada pela rede	Estágio
Bancos: detêm contas utilizadas por PJs ou governos, além destas empresas e governos. TSE: concede poderes a novos prefeitos	Permissionada	Centralizada	-	Baixa, na casa de milhares por dia.	A rede escala facilmente para contemplar todas as IFs no Brasil, além de empresas e governos	Pré-produção

5. Arquitetura técnica				
Camada de usuário	Sistemas não-DLT	Camada API	Plataforma DLT	Detalhamento da infraestrutura DLT
AngularJS	*MongoDB:* persistência dos registros ainda não finalizados *Redis:* cache de informações	Não se aplica	*Hyperledger Fabric*	Consenso *Raft*, utilizando *NodeJs* nos *chaincodes*

6. Custo total de propriedade		7. Benefícios	
Investimento inicial até entrada em produção	Despesas recorrentes	Benefícios quantitativos	Benefícios qualitativos
-	Ainda não há despesas recorrentes	Redução do gasto com pessoal que hoje somente valida documentos de poderes	Redução do tempo de execução deste processo de 8 dias úteis em média para 3hs

1. O Sistema Brasileiro de Poderes consiste em uma rede de *blockchain* criada em parceria pelo BB e pela Petrobrás, com o objetivo de digitalizar o processo de registro de poderes, substituindo os processos manuais baseados em papel, que definem, por exemplo, quem tem poderes para movimentar as contas de uma instituição.

2. A rede poderá ser expandida para o controle de poderes de quaisquer empresas clientes de todos os bancos participantes da rede.

3. Também poderá ser utilizada para registro de poderes de prefeitos sobre contas municipais, na virada após as eleições.

FUNCIONALIDADES

4. A principal função executada pela solução é o registro da cadeia de poderes, que nada mais são do que permissões para movimentar as contas correntes de pessoas jurídicas (empresas ou governos estaduais/municipais).

5. Na rede, serão registrados:

- as pessoas (outorgantes e outorgados);
- os poderes;
- os documentos de poderes: cada documento de poder equivale a um contrato privado, hoje registrado em cartório.

6. Para que as mesmas garantias sejam atendidas, os contratos serão assinados digitalmente, com certificados ICP Brasil.

7. A solução faz uso de contratos inteligentes, com foco em garantir que o processo de registro de poderes e todas as informações registradas estejam de acordo com o especificado.

8. Do ponto de vista da desburocratização, a solução tem o potencial de digitalizar o processo, removendo intermediários (tais como cartórios) e reduzindo o tempo necessário para o registro de poderes, de oito dias para três horas, em média, com possibilidade de que o processo ocorra em tempo real.

9. Do ponto de vista do combate a fraude e corrupção, no cenário atual, funcionários que perderam o direito de acesso a contas, muitas vezes devido a demissão por justa causa e, até mesmo, cometimento de fraude, ainda mantêm plenos poderes por alguns dias, devido ao tempo necessário para execução do processo atual, manual, baseado em papel e dependente de cartórios, trazendo sérios riscos de desvio de recursos.

GOVERNANÇA

10. Dentre as entidades envolvidas, foram citados:

- bancos que detêm contas utilizadas por pessoas jurídicas e/ou governos;
- empresas com contas nesses bancos;
- governos com contas nesses bancos;
- Tribunal Superior Eleitoral (TSE), que possui a prerrogativa de conceder poderes a prefeitos recém-eleitos.

11. A estrutura de governança é centralizada, estando o poder de decisão centrado nos membros fundadores.

USO

12. O sistema ainda está em fase de "aceleração para produção" e, portanto, ainda não foi definida a demanda de uso atual.

13. Com relação ao número de usuários e transações, a solução poderá escalar, de modo a contemplar todas as IFs do Brasil, além de empresas e governos.

14. Para registro de poderes, em que grande parte das empresas faz atualizações semanalmente, espera-se ter um volume transacional baixo, mesmo incluindo todos os grupos esperados. A equipe também tem a percepção de que, além das empresas de grande porte, a maioria não tem interesse em ser um nó na rede (devido ao custo) e, portanto, deverão utilizar APIs de suas IFs ou ferramentas de autoatendimento de pessoa jurídica para acesso à rede, reduzindo o número de nós presentes.

ARQUITETURA TÉCNICA

15. O projeto utiliza *AngularJS* na interface de referência, mas, dado que o *back-end* está exposto dentro das instituições, elas podem utilizar mecanismos de acesso diferentes para conexão com seus sistemas internos.

16. Com relação a sistemas *off-chain*, o banco de dados *MongoDB* é utilizado para persistência de estado dos registros ainda não finalizados e o Redis, para cache de informações.

17. A plataforma DLT empregada é o *Hyperledger Fabric*.

18. O código dos contratos inteligentes (*"chain code"*) é escrito em *NodeJS.*

19. O mecanismo de consenso utilizado é o *Raft.*

20. Até o momento, não foram necessários APIs ou oráculos.

CUSTOS E BENEFÍCIOS

21. Há custo relativo a dois analistas do BB e cinco analistas da Petrobrás. Quase todo o pessoal é compartilhado com outros projetos. Também não há estimativas de despesas recorrentes.

22. Ademais, há desembolso com licenciamento de *software*/suporte técnico da plataforma *blockchain* para atender ao conjunto de projetos em andamento.

23. Dentre os benefícios quantitativos estimados, foi citada a redução do gasto com pessoal, que, hoje, só valida os documentos de poderes vindos de grandes corporações. Esse custo está estimado atualmente em R$ 90 milhões por ano.

24. Como benefício qualitativo, foi citada a redução do tempo do atual processo de registro de poderes.

8. BNDESTOKEN (BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL)

Quadro 8 – BNDESToken

1. Características gerais do estudo de caso					
Nível governamental envolvido	Inclui aspesctos entre outras esferas públicas ou governos estrangeiros?	Inclui aspesctos entre diversas áreas de governo ou com a iniciativa privada?	Serviço público provido/ viabilizado	Aspecto transformador	Abertura do software
Federal e Estadual	Sim	Sim, uma vez que a solução pode ser utilizada por órgãos governamentais e agentes externos (fornecedores)	Financiamentos do BNDES	Processo passa a utilizar um token digital, sem a utilização de papel moeda até a aprovação da prestação de contas	Código aberto

2. Funcionalidades			
Funcionalidades providas	Instituições ou funções desintermediadas	Desburocratização	Combate a fraude e corrupção
Liberação de criptoativo a tomadores de empréstimos; transferência de criptoativos dos tomadores a fornecedores; resgate de criptoativos	Alguns bancos podem ser desintermediados, uma vez que os recursos financeiros não passam pelos bancos dos tomadores de empréstimos	Implementação do *compliance by design* e o acesso sistêmico aos dados de transferência entre os participantes podem reduzir os custos de auditoria e acompanhamento do BNDES e até de outras instituições que monitoram o Banco	Aumento da transparência e acompanhamento tempestivo dos desembolsos diretamente na blockchain, com a possibilidade do desenvolvimento de soluções de terceiros para acompanhamento das transações na DLT

3. Governança			4. Uso			
Papéis e entidades envolvidas	Tipo de blockchain	Tipo de governança	Demanda atual	Capacidade esperada	Vazão	Estágio
BNDES: geração e destruição de criptoativos e liberação de desembolsos; **Tomador de Empréstimo:** realiza transferência para fornecedor **Fornecedor:** solicita resgate de criptoativos	Não-Permissionada e pública (Ethereum)	Centralizada, mas está em estudos a descentralização	Baixa. O piloto em produção aguarda definições organizacionais da Ancine	Capacidade da rede Ethereum – 10 a 30 TPS	O volume deve ser pequeno e plenamente atendível pela rede Ethereum	Foi realizada uma prova de conceito com o Estado do Espírito Santo. Há um piloto em produção no contexto de programas da Ancine.

5. Arquitetura técnica				
Camada de usuário	Sistemas não-DLT	Camada API	Plataforma DLT	Detalhamento da infraestrutura DLT
Metamask (e navegadores compatíveis), HTML/ JavaScript, com bibliotecas Web3 para acessar a *blockchain*	Não há	Não se aplica	*Ethereum*	*Ethereum* público com programação de contratos inteligentes em *Solidity.*

6. Custo total de propriedade		7. Benefícios	
Investimento inicial até entrada em produção	Despesas recorrentes	Benefícios quantitativos	Benefícios qualitativos
A solução tem sido implementada com recursos internos.	Não há	Redução do custo de acompanhamento das operações de financiamento	Maior transparência e tempestividade no acompanhamento das operações; aprimoramento na triagem de incidentes; acompanhamento online automático e proativo do nível de *compliance* do cliente

1. O projeto BNDESToken tem o intuito de criar uma DLT e um criptoativo lastreado em real para as operações de concessão de crédito/transferência de recursos do BNDES para entidades públicas e privadas tomadoras de financiamento.

2. A utilização do BNDESToken como criptoativo permite o acompanhamento tempestivo, pela sociedade, das operações financeiras do BNDES, podendo, também, desintermediar operações.

FUNCIONALIDADES

3. A principal função executada pela solução é o uso de um criptoativo lastreado em real para o registro das operações de liberação, transferência e resgate nas operações de crédito do BNDES com pessoas jurídicas.

4. Em vez de fazer a liberação de recursos em reais, o banco libera um *token*, numa *blockchain* pública (*Ethereum*), para o cliente. A ideia é que o cliente utilize o *token* para adquirir produtos e serviços de seus fornecedores. Estes, por sua vez, realizam o resgate do *token* no BNDES, que faz o depósito da quantia correspondente (uma unidade do BNDESToken equivale a R$ 1,00) na conta corrente dos fornecedores. O processo é totalmente transparente para qualquer cidadão. Mais ainda, qualquer pessoa que se dispuser a rodar um nó da *Ethereum* poderá, até mesmo, validar as transações que compõem o processo, resultando em algo ainda mais poderoso do que a transparência, dado que o cidadão passa a tomar parte na própria validação do processo.

5. Na DLT, são registrados:

- as liberações de recursos aos tomadores de recursos, que podem ser tanto governos estaduais/municipais quanto entidades privadas;
- as transferências de recursos entre os tomadores de empréstimos e fornecedores de serviços/insumos do projeto;
- os resgates realizados pelos fornecedores, ou seja, a conversão de criptoativo em real após a aprovação da prestação de contas dos serviços prestados.

6. Por conta da falta de transparência nos endereços *Ethereum*, desenvolveu-se um processo de cadastro para identificação do dono do endereço, de forma que as pessoas jurídicas participantes do processo utilizam o e-CNPJ como instrumento de garantia de identidade.

7. A solução faz uso de contratos inteligentes, com foco em garantir o processo de criação, transferência e destruição de criptoativos.

8. Do ponto de vista da desburocratização, a solução tem o potencial de digitalizar o processo, com possibilidade de remover os bancos dos fornecedores como intermediários.

9. Todavia, o objetivo maior do projeto BNDESToken é o aumento da transparência das operações de crédito do BNDES, uma vez que sociedade e órgãos de controle podem acompanhar tempestivamente tais operações, dado que a solução é implementada sobre uma *blockchain* aberta e não-permissionada, com todas as garantias de imutabilidade, autenticidade e integridade que tal tecnologia fornece.

GOVERNANÇA

10. A estrutura de governança é centralizada, com o poder de decisão exercido pelo BNDES.

USO

11. O BNDES realizou uma prova de conceito da solução com o governo do Espírito Santo, que atuou como cliente em uma operação simulada de empréstimo para licitação da construção de uma rodovia.

12. O piloto atual em execução é de um programa de incentivo fiscal da Agência Nacional do Cinema (Ancine) para produção de filmes, em que o banco participa com operações não reembolsáveis.

13. A equipe do BNDES informou que o sistema está em produção. Todavia, em decorrência de mudanças organizacionais que estão acontecendo na Ancine, ainda não houve liberação de recursos para projetos daquela autarquia.

ARQUITETURA TÉCNICA

14. O processo exige que a empresa tenha um certificado ICP-Brasil, o e-CNPJ. Cliente e fornecedores precisam assinar uma declaração utilizando seu certificado ICP-Brasil (e-CNPJ). Nessa declaração, a pessoa jurídica se responsabiliza por um endereço *Ethereum* que será utilizado para realizar as transações. A declaração é armazenada pelo BNDES e seu *hash* a é registrado na *blockchain*, permitindo a auditabilidade do processo. A intenção é que o acesso à declaração seja automático, mas isso ainda não foi implementado.

15. Não há solução nova *off-chain* utilizada, porém alguns dados do cadastro de clientes e fornecedores são buscados através de integração e apresentados na interface. No futuro, há a intenção de registrar na *blockchain* um *hash* do comprovante de depósito na conta corrente do fornecedor, armazenando o comprovante em si fora da *blockchain*.

16. O processo que é executado dentro do contexto da *blockchain* é relativamente isolado. No futuro, haverá integrações em suas pontas. Porém, as informações relevan-

tes da parte automatizada pela *blockchain* ficam, hoje em dia, armazenadas nela própria (com exceção da declaração citada anteriormente).

17. Os requisitos de carga e escalabilidade do BNDESToken são adequados à performance fornecida pela rede *Ethereum.*

CUSTOS E BENEFÍCIOS

18. A utilização do BNDESToken aumentará a confiança do cidadão no processo público, tendo em vista que:

- a solução estende a transparência do uso dos recursos do BNDES até para o evento de uso do recurso pelo cliente na aquisição de produtos e serviços do fornecedor, o que é inovador, considerando toda a estrutura do mercado bancário atual;

- as partes do processo que são executadas em *blockchain* são totalmente auditáveis pelos cidadãos, viabilizando uma forma de monitoramento inédita de um processo público;

- o cidadão tem acesso ao código executável do contrato inteligente (que é obrigatoriamente público na *Ethereum*), podendo auditar todo o processo.

19. Em relação aos custos, a solução tem sido implementada com recursos internos, inclusive tendo ocorrido desembolsos com treinamentos da equipe.

9. TRUBUDGET (BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL)

Quadro 9 – TruBudget

1. Características gerais do estudo de caso					
Nível governamental envolvido	Inclui aspesctos entre outras esferas públicas ou governos estrangeiros?	Inclui aspesctos entre diversas áreas de governo ou com a iniciativa privada?	Serviço público provido/ viabilizado	Aspecto transformador	Abertura do software
Federal	Sim, KfW (Banco de Desenvolvimento da Alemanha)	Sim. O software tem sido desenvolvimento pelo KfW (Banco de Desenvolvimento Alemão), que é um dos doadores do Fundo Amazônia.	Acompanhamento de liberação e recebimento de recursos repassados ao Fundo da Amazônia	Envolvimento numa rede única dos doadores de recursos, intermediários e beneficiários das doações	Sim

2. Funcionalidades			
Funcionalidades providas	Instituições ou funções desintermediadas	Desburocratização	Combate a fraude e corrupção
Disponibilização de informações referentes à liberações e recebimentos de recursos no Fundo da Amazônia, em tempo real, para todos os envolvidos	Não há potencial de desintermediação	Há potencial, principalmente se a solução for expandida para redução de custo de acompanhamento e auditoria	As informações estão disponíveis em tempo real para todos os envolvidos, inclusive doadores que, por natureza, têm grande interesse de garantir o adequado uso dos recursos. Outras instituições poderiam tomar parte na rede, aumentando ainda mais esse potencial

3. Governança			4. Uso			
Papéis e entidades envolvidas	Tipo de blockchain	Tipo de governança	Demanda atual	Capacidade esperada	Vazão	Estágio
KfW: Doador, desenvolve a solução e participa da rede **BNDES:** Gerencia o fundo, realiza os repasses configura o workflow e participa da rede **Beneficiários:** Recebem e aplicam os recursos e usam a ferramenta (já configurada)	Permissionada e privada	Descentralizada	Ainda em fase piloto	Ainda em piloto	Baixo volume de transações	Piloto

5. Arquitetura técnica				
Camada de usuário	Sistemas não-DLT	Camada API	Plataforma DLT	Detalhamento da infraestrutura DLT
React	A ferramenta foi integrada com o SAP do BNDES	Não há	*Multichain*	O Multichain é um *fork* permissionado do Bitcoin, cujo algoritmo de consenso não envolve criptomoedas, sendo um algoritmo próprio, baseado no pBFT

6. Custo total de propriedade		7. Benefícios	
Investimento inicial até entrada em produção	Despesas recorrentes	Benefícios quantitativos	Benefícios qualitativos
Plataforma MultChain cedida pelo KfW Pessoal - Custos referentes a cinco empregados em tempo parcial	Pessoal - Custos referentes a cinco empregados em tempo parcial	No momento não há	Maior confiança dos doadores na aplicação dos recursos Aumento da expectativa de controle no emprego dos recursos doados

1. O TruBudget é uma solução em DLT desenvolvida pelo KfW, Banco de Desenvolvimento do governo da Alemanha, que tem por objetivo acompanhar, de forma mais tempestiva e transparente, a utilização dos recursos financeiros doados por aquela instituição aos vários projetos apoiados em todo o mundo. O KfW é o segundo maior doador do Fundo da Amazônia.

2. O TruBudget é um *workflow* configurável cujos dados são todos gravados em uma *blockchain* permissionada, chamada *Multichain*.

3. Até o momento, há dois nós na rede *Multichain*, o BNDES e o KfW. A Noruega, responsável por 94% dos recursos financeiros doados ao Fundo da Amazônia, também foi convidada para participar do Projeto TruBudget, mas ainda está avaliando a proposta.

FUNCIONALIDADES

4. A concepção do TruBudget é envolver numa rede os possíveis diversos doadores de recursos, intermediários e beneficiários. Esse compartilhamento confiável de informações só é possível desta forma.

5. A configuração realizada até o momento para o piloto com o Fundo Amazônia abrange dois passos do processo de concessão e acompanhamento do uso de recursos do fundo. Basicamente, na DLT, o:

- BNDES registra a liberação de um recurso à entidade recebedora;
- beneficiário registra o recebimento deste mesmo recurso.

6. Todos os dados da solução são armazenados na plataforma *Multichain.*

7. Atualmente, a DLT tem dois nós, um no BNDES e outro no KfW. Com apenas dois nós, a vantagem de usar a *blockchain* sobre um sistema centralizado no próprio KfW, que seria dar garantias ao BNDES de que os dados não serão manipulados de alguma forma, é menor. Porém, uma rede que também inclua diversos doadores pode aumentar a confiança geral nos processos e, nesse sentido, esse compartilhamento multilateral e confiável de informações não parece ser alcançável através de outra tecnologia.

8. Tanto no processo antigo quanto no processo novo, a intermediação é realizada pelo próprio BNDES, que gerencia, repassa e comprova o uso dos recursos do Fundo Amazônia. O desenho da solução até o momento tem o objetivo de disponibilizar informações em tempo real para todos os envolvidos.

GOVERNANÇA

9. A governança da solução é descentralizada, uma vez que todos os *stakeholders*

possuem um poder de decisão igualitário. As decisões são tomadas em comum acordo entre o BNDES e KfW.

USO

10. A solução está em fase-piloto, envolvendo um pequeno grupo de organizações não governamentais (ONGs) beneficiárias do Fundo Amazônia.

11. O plano é, no futuro, envolver mais etapas do processo de doação de recursos, com o objetivo de abranger informações referentes ao acompanhamento dos gastos e à prestação de contas, bem como envolver outros doadores, principalmente, o governo da Noruega.

ARQUITETURA TÉCNICA

12. A solução é desenvolvida em conjunto pelo KfW e BNDES e utiliza a DLT *Multichain*, que é um fork permissionado do *bitcoin*, cujo algoritmo de consenso é baseado no pBFT.

13. Todas as informações são armazenadas na própria DLT. Todavia, a ferramenta foi integrada com o SAP do BNDES. Conforme são executadas liberações referentes ao Fundo Amazônia, são criados itens no *workflow* do TruBudget.

14. Na camada de apresentação, é utilizado o *React*, uma biblioteca *JavaScript* para criar interfaces de usuário.

CUSTOS E BENEFÍCIOS

15. Em decorrência do projeto TruBudget estar na fase-piloto, o BNDES não realizou análise de custos de sustentação da solução. Tem-se, apenas, como registro de custos os salários de cinco empregados em tempo parcial.

16. Os benefícios propiciados pelo projeto abrangem, principalmente, um maior acompanhamento pelos entes doadores de recursos e uma redução de custos de auditoria, sendo essencial a incorporação na plataforma de mais documentos comprobatórios.

10. DIÁRIO DE BORDO (AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL)

Quadro 10 – Diário de bordo

1. Características gerais do estudo de caso					
Nível governamental envolvido	Inclui aspesctos entre outras esferas públicas ou governos estrangeiros?	Inclui aspesctos entre diversas áreas de governo ou com a iniciativa privada?	Serviço público provido/ viabilizado	Aspecto transformador	Abertura do software
Federal	Não	Operadoras de transporte aéreo	Registro do Diário de Bordo dos voos de operadoras brasileiras	Eliminar o uso de papel, promovendo auditabilidade e economicidade	Código aberto

2. Funcionalidades			
Funcionalidades providas	Instituições ou funções desintermediadas	Desburocratização	Combate a fraude e corrupção
Infraestrutura de guarda de registro de diário de bordo. Distribuição dos dados, regras de governança em *smart contracts*	Infraestrutura centralizada de armazenamento	Permite auditorias e fiscalizações *online*, pela consulta dos registros da *ledger*, em contraponto à presença dos técnicos da Anac nas aeronaves e aeroportos	Registros em papel são sujeitos a fraudes. A imutabilidade e não repúdio dos dados do diário de bordo em blockchain tornam a solução mais segura e robusta quanto a fraudes

3. Governança			4. Uso			
Papéis e entidades envolvidas	Tipo de blockchain	Tipo de governança	Operação atual	Capacidade esperada	Vazão	Estágio
Anac – desenvolvimento dos contratos inteligentes. Definição dos processos de fiscalização dos operadores aéreos. Operadores Aéreos – usuários do sistema	Permissionada e privada	Centralizada - Anac	-	9000 operadores aéreos 12 milhões de transações por ano	5 a 20 tps	Em produção, operadores aéreos solicitaram que o processo fosse implantado gradualmente, por serviços menos críticos

5. Arquitetura técnica				
Camada de usuário	Sistemas não-DLT	Camada API	Plataforma DLT	Detalhamento da infraestrutura DLT
Um gerenciador web construído em React JS *Fabric-client* do *Hyperledger Fabric*	Servidor de autenticação *Keycloak*	APIs internas que expõem informações dos sistemas da Anac. Web API para acesso ao Hyperledger	*Hyperledger Fabric*	*Smart contracts* escritos em *JavaScript (NodeJS)* Mecanismo de consenso *Raft*

6. Custo total de propriedade		7. Benefícios	
Investimento inicial até entrada em produção	Despesas recorrentes	Benefícios quantitativos	Benefícios qualitativos
Orçado dentro do contrato da fábrica de software contratada pela Anac	Custo de sustentação do contrato com a fábrica de software	Expectativa de mais fiscalização e menos burocracia	Expectativa de melhor gestão dos processos de fiscalização dos registros realizados pelos operadores aéreos

1. A Agência Nacional de Aviação Civil (Anac) regulamenta, por meio das resoluções 457/2017 e 458/2017, o registro primário de informações relativas a cada voo efetuado no território brasileiro (etapa de voo e manutenções). Tal conjunto de informações é denominado diário de bordo. O uso de registros de diário de bordo digitais em *blockchain* é regulamentado pela agência por meio da resolução 511/2019.

2. O correto registro dos chamados diários de bordo pelo operador da companhia aérea ou aeronauta é de grande importância para a melhoria da aviação no país. Milhões de voos são realizados anualmente em território nacional, havendo a necessidade da correta avaliação dos procedimentos para os casos normais ou de exceção.

3. A Anac criou uma rede privada baseada em tecnologia *blockchain* para que todos os operadores aéreos, devidamente cadastrados, possam fazer uso dessa infraestrutura que provê aos registros de diário de bordo das aeronaves as características de imutabilidade, auditabilidade e segurança.

4. Contratos inteligentes da plataforma de *blockchain Hyperledger* são utilizados para assegurar que as regras de negócio envolvidas nos registros de diário de bordo sejam cumpridas, ao contrário do registro em papel, em que o operador aéreo tem liberdade para escrever o que deseja, resultando, muitas vezes, em registros imprecisos, incompletos ou fora do formato exigido.

FUNCIONALIDADES

5. Os contratos inteligentes são utilizados para registrar dados de aeronaves, aeronautas, operadores aéreos, prepostos de operadores aéreos, diários de bordo de aeronaves, volumes dos diários de bordo, etapas de voo e discrepâncias técnicas (manutenções das aeronaves).

6. Os registros das etapas de voo e discrepâncias técnicas podem ser assinados pelos aeronautas.

7. A Anac disponibiliza APIs abertas para que os *softwares* utilizados pelos operadores aéreos possam se integrar à solução de diário de bordo em *blockchain* provida. Além disso, uma aplicação web foi desenvolvida pela Anac para uso por operadores aéreos, possibilitando o uso direto da solução de diário de bordo em *blockchain*.

GOVERNANÇA

8. Foi escolhida a arquitetura permissionada, em que apenas a Anac e os operadores aéreos têm permissão para participar da *blockchain*, possuindo seus próprios nós.

9. A governança da rede, criação e definição do consenso da blockchain, adição de novos operadores, adição de novos nós, (*Hyperledger Fabric Peer*), criação e atualização

de contratos inteligentes (*chaincodes*) e criação de novos livros-razão (*Hyperledger Fabric Channels*) é de responsabilidade exclusiva da Anac.

USO

10. A Anac espera que a aplicação seja utilizada por um total de 9 mil operadores, realizando 12 milhões de transações por ano.

ARQUITETURA TÉCNICA

11. Como já mencionado, uma aplicação web foi desenvolvida para comunicação direta dos operadores aéreos, possibilitando o uso direto da solução de diário de bordo em *blockchain.* Essa aplicação foi desenvolvida com a tecnologia de *Frontend ReactJS*, que faz uso de APIs da Anac desenvolvidas em *NodeJS*. Tais APIs expõem dados de aeronautas, aeronaves, aeródromos, operadores aéreos e prepostos de operadores aéreos, além de acessarem a *blockchain* pelo módulo *fabric-client*, do *Hyperledger Fabric*. A autenticação é provida por um servidor *Keycloak.*

CUSTOS E BENEFÍCIOS

12. Com a utilização da aplicação, espera-se uma melhor gestão dos processos de fiscalização dos registros realizados pelos operadores aéreos, bem como redução da burocracia.

11. RNDS (MINISTÉRIO DA SAÚDE)

Quadro 11 – RNDS

1. Características gerais do estudo de caso					
Nível governamental envolvido	Inclui aspesctos entre outras esferas públicas ou governos estrangeiros?	Inclui aspesctos entre diversas áreas de governo ou com a iniciativa privada?	Serviço público provido/ viabilizado	Aspecto transformador	Abertura do software
Federal	Estadual e Municipal	Planos de saúde e grandes redes hospitalares podem fazer parte da rede	Prontuário eletrônico dos pacientes	Interoperabilidade digitalização Visão integrada do paciente	Código Aberto

2. Funcionalidades			
Funcionalidades providas	Instituições ou funções desintermediadas	Desburocratização	Combate a fraude e corrupção
Timeline dos pacientes, distribuição dos dados clínicos, regras de consentimento em *smart contracts*	Potencial de desintermediar funções executadas por estabelecimentos de saúde públicos e privados	Permite consulta de timeline e documentos clínicos dos pacientes de qualquer estabelecimento de saúde. Gestão de consentimento alinhada com regras do MS	Registro eletrônico de saúde sem a possibilidade de alteração

3. Governança			4. Uso			
Papéis e entidades envolvidas	Tipo de blockchain	Tipo de governança	Demanda atual	Capacidade	Vazão	Estágio
MS – desenvolvimento dos contratos inteligentes, definição dos processos de gestão da informação e padrão de mensagens Secretarias estaduais e municipais – participantes da rede. Armazenamento local dos documentos clínicos. UBS, Hospitais, Clínicas – Usuários do sistema	Privada e permissionada	Híbrida – MS e Estados	1,2M de registros de saúde por ano e 10 transações por segundo – Alagoas 2000 UBS	40 até 600 TPS 5Bi de registros de saúde por ano 200 mil estabelecimentos de saúde	1.800 tps (resultado obtido em prova de conceito arquitetural)	Preparação de ambiente de produção Piloto

5. Arquitetura técnica				
Camada de usuário	Sistemas não-DLT	Camada API	Plataforma DLT	Detalhamento da infraestrutura DLT
App/PWA ConecteSUS Cidadão App/PWA ConecteSUS Profissional	EHR Service – Microserviços BFF – Cache de sistema	APIs externas para os PEPs. API interna para acesso ao *Hyperledger*	*Hyperledger Fabric*	*Smart contracts* escritos em *Go (GoLang)* Mecanismo de consenso *Raft*

6. Custo total de propriedade		7. Benefícios	
Investimento inicial até entrada em produção	Despesas recorrentes	Benefícios quantitativos	Benefícios qualitativos
Orçado dentro do contrato das fábricas contratada pelo MS	Orçado como manutenção contrato das fábricas contratada pelo MS	Aumento da quantidade de pacientes atendidos	Melhoria no atendimento ao paciente

1. A utilização de Registros Eletrônicos de Saúde (RES) ainda tem um problema a ser resolvido: como os dados clínicos são armazenados em silos, a informação é desorganizada e armazenada em vários formatos, tornando praticamente impossível traçar histórico de pacientes e trocar informações com outros profissionais de saúde. A chave para esse obstáculo é a interoperabilidade dos registros médicos.

2. A Rede Nacional de Dados em Saúde (RNDS) pretende facilitar a interoperabilidade dos prontuários do cidadão por meio da disponibilização dos itens de histórico do paciente em uma estrutura de *blockchain* compartilhada entre os estados. Hoje, no Brasil, existem 2 mil tipos de prontuários em operação. Cada prontuário tem seu modelo de dados específico e cada um segue em padrão. O caminho que se está trilhando é a troca de informações do resumo de atendimento clínico do paciente e o respectivo envio à RNDS. Os documentos clínicos completos serão ainda armazenados em estruturas privadas de cada estado.

3. Assim, a RNDS pode ser definida como um repositório de informações retrospectivas, simultâneas e prospectivas do paciente em formato digital, cujo principal objetivo é promover o cuidado da saúde de forma integrada, contínua, eficiente e de qualidade. Além disso, a RNDS deve ser acessível e estar disponível em diferentes instituições de saúde.

4. A *blockchain* armazena a história de interações entre pacientes e agentes de saúde, juntamente com *links* para os registros de saúde eletrônicos (em inglês, *Electronic Health Record* – EHR), que contêm descrições detalhadas de cada uma das interações. Um *hash* do registro médico também é armazenado no bloco. Assim, a fidelidade do conteúdo pode ser facilmente verificada.

5. Sempre que um paciente X encontra um agente de saúde Z, o agente deve ter a ferramenta de *software* apropriada e as credenciais corretas para recuperar os dados de saúde do paciente via *blockchain*. O profissional Z pode solicitar os dados de X e solicitar o direito de ler os dados. O usuário X deve autorizar explicitamente, mas o acesso sem autorização pode ocorrer nos casos de emergência médica ou quando configurado para estratégia "*opt out*" no contexto de atendimento (no hospital ou na unidade de saúde). Neste caso, novas transações são criadas na *blockchain*. Para cada arquivo é criada uma transação, autorizando Z a ter acesso a esse arquivo. Nota-se que Z pode escolher, com base no conteúdo de metadados armazenado em cada transação, acessar apenas arquivos específicos. Por exemplo, Z pode solicitar acesso somente aos arquivos relevantes para a atual consulta médica.

FUNCIONALIDADES

6. Os contratos inteligentes são utilizados para gerir as seguintes informações digitais: paciente, profissional de saúde, histórico do paciente, registros de atendimento clínico (consultas), internações, vacinas e dispensação de medicamentos, nesta primeira fase.

7. Além disso, eles servem, também, para assegurar que as regras de negócio envolvidas nos registros do prontuário eletrônico sejam cumpridas, ao contrário do registro em papel, em que o profissional de saúde tem liberdade para escrever o que deseja, implicando muitas vezes registros imprecisos e incompletos. Garante, ainda, a devolução das informações apenas aos profissionais autorizados, respeitando as leis de consentimento e a Lei Geral de Proteção de Dados (LGPD).

8. Estruturas em *blockchain* facilitam a interoperabilidade dos dados dos pacientes, garantindo imutabilidade, cumprimento de estratégias de consentimento e descentralização da gestão de dados de saúde. Também permitem que os entes federados consigam simultaneamente armazenar as informações e garantir o compartilhamento do histórico dos cidadãos. Ainda nesse contexto, a estruturação das informações facilita a escalabilidade dos nós participantes da rede, reduzindo a necessidade de armazenamento centralizado e, ainda assim, garantindo a interoperabilidade. Com o uso do padrão *Fast Healthcare Interoperability Resources* (FHIR) para transporte e armazenamento dos dados clínicos, o Ministério da Saúde (MS) define a infraestrutura necessária para evoluir o cuidado de saúde, com previsão de utilizar estratégias de *data analytics* e inteligência artificial.

9. O MS disponibiliza APIs abertas para que os *softwares* utilizados por estabelecimentos de saúde (Prontuário Eletrônico do Paciente – PEP) possam se integrar à solução da RNDS em *blockchain.* Além disso, dois aplicativos foram desenvolvimentos pelo MS, possibilitando o uso direto por parte dos cidadãos – ConecteSUS Cidadão (antigo MeuDigisus) – e profissionais de saúde – ConecteSUS Profissional.

GOVERNANÇA

10. Foi escolhida a arquitetura permissionada, na qual apenas o MS, as secretarias de saúde que escolheram fazer parte da rede e, no futuro, os participantes privados, como planos de saúde ou grandes redes de hospitais, têm permissão para participar da *blockchain*, possuindo seus próprios nós.

11. A governança da rede, criação e definição do consenso da *blockchain*, adição de novos operadores, adição de novos nós, criação e atualização de contratos inteligentes (*chaincodes*) e criação de novos livros-razão (*Hyperledger Fabric Channels*) são de responsabilidade exclusiva do MS.

USO

12. Atualmente, a rede é composta por nós do MS hospedados em nuvem contratada pelo ministério para utilização no piloto, em Alagoas. Após o piloto, existe plano de expansão em mais estados, ainda a definir.

13. De acordo com testes obtidos em prova de conceito arquitetural, a solução será

capaz de suportar até 1.800 transações por segundo (tps), suficiente para o número de atendimentos por ano de toda a população usuária do Serviço Único de Saúde (SUS).

ARQUITETURA TÉCNICA

14. Na arquitetura, os metadados serão utilizados no livro-razão e distribuídos entre os diversos participantes da rede. Já os documentos clínicos serão utilizados em *private data collection*, a fim de garantir a privacidade e economicidade de armazenamento do documento. Uma vez que os documentos serão armazenados apenas na organização custodiante e em uma estrutura limitada de organizações de *backup*, não haverá eventual armazenamento excessivo dos documentos clínicos. Como é compartilhado no livro-razão, o histórico do paciente estará acessível para qualquer organização, o que facilitará as consultas dos pacientes nos estabelecimentos de saúde. Os dados serão trafegados e armazenados em padrão FHIR, em que os mais de 2 mil tipos de prontuários existentes no país estruturarão as informações seguindo a estratégia de transformação digital da saúde brasileira. No primeiro momento, serão utilizados microsserviços de transição, capazes de realizar a conversão dos dados enviados em Clinical Document Architecture (CDA), OpenEHR e FHIR.

CUSTOS E BENEFÍCIOS

15. Com a adoção massiva da solução, o segmento de saúde tem o potencial de melhorar o atendimento ao paciente, uma vez que todos os estabelecimentos poderão compartilhar informações transversais de atendimento do cidadão.

16. Ainda, além de diminuir o custo das operações de registro e guarda de documentos clínicos físicos, a RNDS em *blockchain* traz grandes vantagens na interoperabilidade dos dados clínicos e visão distribuída da linha do tempo de saúde, bem como da garantia de acesso aos dados apenas por meio de consentimento, em conformidade com a LGPD.

17. Por fim, a RNDS em *blockchain* também impossibilita a alteração de registros passados e garante que diversas validações sejam realizadas antes da gravação do registro, evitando, assim, diversas fraudes e falhas na fiscalização.

12. OUTRAS INICIATIVAS NAS ESFERAS FEDERAL E ESTADUAL

BLOCKCHAIN COMO SERVIÇO

1. *Blockchain* como Serviço, tradução para o termo "*Blockchain-as-a-Service*" ou "BaaS", é um acrônimo informal que designa um modelo de simplificação da tarefa de criar redes *blockchain*, normalmente desenvolvido por companhias que adquiriram experiência no desenvolvimento de soluções na tecnologia e que, portanto, atuam como fornecedores de conhecimento, serviços especializados e *frameworks*, quase sempre voltados para implantação em nuvem.

2. Assim, o termo "BaaS" pode ser definido como um modelo único que permite que consumidores utilizem serviços baseados em nuvem para desenvolver, utilizar e hospedar aplicações e contratos inteligentes baseados em *blockchain*, fornecendo plataformas completas que facilitam o processo de desenvolvimento. Companhias responsáveis por esse tipo de plataforma atuam como uma ponte entre empresas (clientes) e plataformas de *blockchain* corporativo. Embora as últimas forneçam uma versão generalizada da tecnologia, nem todas as organizações possuem conhecimento e experiência necessários para integrar as plataformas disponíveis no mercado às suas soluções de negócio. Os serviços comumente fornecidos são: implementação da rede, manutenção dos nós, responsabilidade por monitorar artefatos tecnológicos cruciais, garantia de disponibilidade, fornecimento de protocolos de segurança, gerenciamento de banda etc. O cliente final foca tão somente nas funcionalidades e estratégias de negócio, delegando ao provedor do modelo de serviço o gerenciamento da infraestrutura.

3. Dentre os estudos de caso considerados, as empresas Serpro e Dataprev atualmente estão com iniciativas de fornecimento do modelo *blockchain* como Serviço para a Administração Pública federal.

SERPRO

4. A empresa Serpro recentemente deu início à construção da plataforma *Multiledgers*, definida como uma "solução para oferecer BaaS na modalidade de autosserviço e em ambiente multinuvem". A solução, segundo a empresa, oferecerá "a possiblidade de criar redes DLT nas tecnologias *Corda*, *Quorum* e *Hyperledger Fabric*, em nuvem privada ou em nuvens públicas".

5. Inicialmente foi construída para uso interno, tendo como principal motivação o fato de o *Hyperledger* ser um ambiente complexo, gerando a necessidade de simplificar o processo de construção de uma rede *blockchain*. Foram realizados testes com as plataformas *Ethereum* e *Corda*. Porém, o *Hyperledger Fabric* é, atualmente, a ferramenta mais bem conhecida pela equipe de desenvolvimento.

6. O serviço, oferecido em nuvem, permite que se executem máquinas virtuais em múltiplas nuvens que podem interagir em uma única rede *blockchain*. Um dos objetivos

é aumentar a facilidade para que os órgãos contratem os serviços do Serpro, uma vez que terão a possibilidade de utilizar vários ambientes de nuvem, sem precisar fazer a contratação individual de cada um dos ambientes ou mesmo ter que implementar em *datacenters* locais (*on-premise*).

7. Além do *Hyperledger Fabric*, também é provida a solução *Hyperledger Indy*, voltada para prover carteiras (*wallets*) de identidade descentralizada, para casos de uso como compartilhamento de documentos e diplomas.

DATAPREV

8. A solução de *blockchain* como Serviço da empresa Dataprev foi construída a partir do ganho de experiência com o projeto bCPF, em parceria com a RFB. Segundo a equipe responsável, o mesmo framework empregado naquele projeto tem potencial de reutilização em outras iniciativas e órgãos, com exceção apenas da camada de dados.

9. O serviço oferecido inclui desde a criação da rede até a implementação de contratos inteligentes, dispensando o conhecimento da tecnologia por parte do cliente e concentrando os esforços de instalação, suporte e sustentação na Dataprev.

ASSINADOR.BR – PETROBRAS

10. Assinador.BR é um projeto de P&D desenvolvido pelo Centro de Pesquisas da Petrobrás com o objetivo de conhecer e experimentar a tecnologia blockchain. Esclarece-se que o projeto ainda não iniciou a fase-piloto.

11. A solução proposta é de utilização apenas interna na Petrobrás, pelos empregados participantes da comissão que avalia os convênios a serem firmados com instituições de ensino e pesquisa externas. Nesse sentido, o relatório de avaliação produzido pela comissão é assinado pelos participantes com a utilização da solução desenvolvida.

12. Para isso, foi criada uma infraestrutura na qual foi desenvolvida uma aplicação em smartphone que permite aos participantes da comissão receber, visualizar e assinar os relatórios. Os hashes das assinaturas são gravados na blockchain por meio de um contrato inteligente na plataforma *Ethereum.*

SOLUÇÃO ONLINE DE LICITAÇÃO (SOL)

13. Solução Online de Licitação (SOL) é um aplicativo de compras, desenvolvido e disponibilizado pelos estados da Bahia e do Rio Grande do Norte, que permite às organizações beneficiárias dos Projetos Bahia Produtiva (BA) e Governo Cidadão (RN) realizar licitações para a compra e/ou contratação de bens, serviços e obras.

14. O aplicativo também permite que fornecedores de todo o país enviem suas propostas e acompanhem o resultado das licitações. A plataforma utiliza *software* livre, modelo de código aberto e tecnologia *blockchain*, para garantir plena integridade, transparência e auditabilidade ao processo licitatório.

APLICAÇÕES E INICIATIVAS DA TECNOLOGIA BLOCKCHAIN EM OUTROS PAÍSES

1. AUSTRÁLIA

Website - Digital Transformation Agency

1. A Agência de Transformação Digital do governo australiano criou um sítio eletrônico (*https://www.dta.gov.au/help-and-advice/technology/blockchain*) em que elaborou um guia geral sobre a tecnologia blockchain, para ajudar outras agências de governo na compreensão e no desenvolvimento de soluções distribuídas.

The National Blockchain Roadmap

2. Com o estabelecimento de um *roadmap*, o governo australiano pretende fornecer apoio ao governo, ao setor privado e aos pesquisadores, para promover a inovação e colaboração em torno da *blockchain*. O documento elaborado destaca algumas das enormes oportunidades que a tecnologia *blockchain* pode oferecer em toda a economia. O *roadmap* não apenas identifica as oportunidades atuais e futuras da *blockchain*, mas também fornece indicações sobre o desenvolvimento futuro e as oportunidades dessa tecnologia.

3. O governo australiano destacou oportunidades na economia que podem ser aproveitadas e possibilitadas pelo uso da tecnologia *blockchain*: criar empregos, aumentar o crescimento econômico, economizar dinheiro das empresas e melhorar a produtividade geral. Além disso, a combinação da tecnologia *blockchain* com outras tecnologias e dados digitais que sustentam as *blockchains* é vista como um fator que pode adicionar um enorme valor econômico.

Making Money Smart

4. Trata-se de um experimento que emprega o uso de *blockchain* na criação de "dinheiro inteligente" – programado para "saber" quem, em que e quando pode ser gasto –, por meio do uso de contratos inteligentes, que representam regras de orçamento. O estudo de caso foi patrocinado pelo *National Disability Insurance Scheme* (NDIS). Os objetivos incluíam: eliminação de papel e cálculos manuais; checagens automáticas de elegibilidade e pagamentos em tempo real; e controle de fraudes por meio de análise de dados.

2. ÁFRICA

Bitland

5. O projeto é parte de uma iniciativa, concebida por um grupo de técnicos de vários países, voltada para combater a corrupção e empoderar as pessoas por meio da propriedade legalizada. Atualmente, um piloto está sendo executado na cidade de Kumasi, Gana. *Bitland* é uma plataforma experimental que utiliza *blockchain* para preencher a lacuna entre governos e áreas sem registro. O objetivo é permitir que indivíduos pesquisem propriedades de terra e registrem os respectivos títulos de propriedade na *blockchain*, de forma permanente e auditável. Vislumbra-se que as pessoas possam usar seus dispositivos móveis para registrar uma propriedade com a acurácia de um GPS, assentar uma disputa ou mesmo vender e comprar terra.

3. RÚSSIA

Active Citizen

6. Por meio de um programa já existente, denominado *Active Citize*n, a cidade de Moscou tem permitido que residentes votem a respeito de vários assuntos da administração local. Em um esforço para aliviar as preocupações acerca da confiabilidade na contagem dos votos, foi adicionada uma versão privada da blockchain *Ethereum* à arquitetura do projeto. Um dos desafios atuais é a escalabilidade. De acordo com os desenvolvedores, foi contratada uma consultoria para auditar o sistema e avaliar a possibilidade de manipulação dos resultados das votações. Nenhuma vulnerabilidade foi encontrada nesse sentido.

4. UNIÃO EUROPEIA

European Union Blockchain Observatory and Forum

7. Em fevereiro de 2018, a Comissão Europeia, em colaboração com o Parlamento Europeu, lançou o *European Union Blockchain Observatory and Forum*. A organização atua como uma plataforma de engajamento de partes interessadas. É uma iniciativa para acelerar a inovação e aceitação da *blockchain*, aproveitando a comunidade existente, com o intuito de mapear projetos, gerenciar grupos de trabalho sobre casos de uso e marco regulatório, produzir relatórios temáticos e realizar treinamentos. A organização recebe debates afetos ao tema, organiza *workshops* e produz relatórios, com a ajuda de diversos atores europeus e internacionais.

Value Added Tax (VAT)

8. Na Europa, o imposto sobre valor agregado *(value added tax* – VAT) é uma importante fonte de receita para os estados-membro e a União Europeia. A cada ano, bilhões de euros são perdidos, devido a fraudes, sobretudo por ser o imposto autodeclarado. As autoridades somente podem auditar *a posteriori*. O processo é caro e lento, o que significa que só uma pequena porção dos impostos é de fato examinada.

9. Desta forma, está sendo construída uma plataforma, baseada em *blockchain*, que objetiva combater as fraudes. A solução utiliza o serviço de carimbo de tempo para registrar o momento exato em que cada nota fiscal é gerada e quando é fornecida para as autoridades fiscais. Como resultado, ao fim de cada mês, a autoridade fiscal pode facilmente identificar os casos em que não foram recolhidos impostos.

10. O projeto prevê que as autoridades fiscais atuem como nós da rede e os bancos, como oráculos externos, confirmando se o imposto foi realmente pago e processado.

5. ESTÔNIA
e-Estonia KSI

11. A Estônia, em 2012, tornou-se a primeira nação a adotar as tecnologias distribuídas, com o intuito de que seus cidadãos confiem 100% nos dados governamentais. O país utiliza uma implementação permissionada da tecnologia para assegurar integridade. Assim, se uma organização pública tem um ativo digital, ela pode utilizar o serviço em *blockchain* para comprovar que uma informação não foi modificada após o momento de seu registro.

12. A tecnologia que suporta os sistemas da Estonia é a *blockchain Keyless Signature Infrastructure* (KSI), também utilizada pela Organização do Tratado do Atlântico Norte (OTAN) e pelo Departamento de Defesa dos EUA (DoD, USDOD, DOD ou Department of Defense).

13. KSI é um sistema distribuído para fornecer *timestamp* e serviços de assinatura digital com suporte a servidor. A expressão *keyless* não significa que chaves criptográficas não são utilizadas durante a criação de assinaturas. As chaves ainda são necessárias para autenticação, mas as assinaturas podem ser verificadas com segurança, sem assumir sigilo continuado das chaves.

14. Isso permite que, posteriormente, um usuário consulte o sistema KSI, por meio de um valor hash, que retorna uma espécie de assinatura que fornece *proof-of-time* criptográfica, integridade do dado assinado e atribuição de origem, ou seja, qual entidade gerou a assinatura. Assim, qualquer cidadão pode logar no sistema e ver quem manipulou seus dados (por exemplo, se a polícia de trânsito utilizou sua placa ou um médico tratou seus dados médicos). A solução *blockchain* foi projetada para garantir que tudo tenha sido registrado com segurança e a informação não tenha sido adulterada por agentes maliciosos.

6. LUXEMBURGO
Infrachain Governance Framework5.

15. O projeto Infrachain objetiva criar um arcabouço de governança e uma camada de rede compostos por nós independentes. Os nós precisam estar em conformidade com

regulações sobre armazenamento de dados, segurança e privacidade e operam com base em acordos de nível de serviço. O *framework* Infrachain é uma camada no topo de *blockchains* privadas. Adicionalmente, remove a necessidade por operações de mineração computacionalmente intensivas, pois apenas nós certificados são aceitos. Serviços públicos podem se beneficiar de um projeto desse tipo, com ganho em produtividade e menor tempo de implantação, adotando o arcabouço proposto, ao invés de criarem soluções próprias complexas. Também se beneficiam por usarem um conjunto comum de nós certificados.

7. GEÓRGIA
Exonum land title registy

16. A Geórgia utiliza *blockchain* permissionada para fornecer aos cidadãos um certificado digital de seus títulos de propriedade. A *blockchain* é usada por cidadãos, para validar certificados, e por notários, para fazer novos registros. Dentre os benefícios, tem-se uma significativa redução dos tempos de registro e verificação das propriedades (de dias para minutos ou segundos). A solução também proporciona transparência no processo de registro, redução dos custos operacionais, bem como maior segurança e confiabilidade, oferecidas por certificados digitais. Embora todo o processo ocorra dentro de uma *blockchain* permissionada, com acesso apenas dos donos de propriedades e cartórios, um *hash* criptográfico é publicado na rede pública do *bitcoin*, para que a verificação dos certificados possa ser feita por qualquer um.

8. MALTA
Blockcerts academic credentials

17. Em 2017, o governo maltês lançou um projeto para verificação de credenciais acadêmicas utilizando *blockchain*. Optou-se por usar o padrão aberto *Blockcerts*, para gerenciamento de registros acadêmicos, que, por sua vez, usa tecnologia *blockchain* como infraestrutura. As funcionalidades incluem a emissão de credenciais acadêmicas, a verificação de certificados e o armazenamento de credenciais pessoais no computador ou *smartphone* do usuário. O aplicativo *Blockcerts* fornece uma carteira em que o cidadão tem controle sobre quem pode enxergar e verificar seus registros acadêmicos, bem como um verificador universal, que é uma página web acessível a todos. Ao fornecer o localizador uniforme de recursos (*Uniform Resource Locator* – URL) do certificado, é possível verificar a validade, o proprietário das credenciais, a data de emissão, a instituição emissora e o identificador da transação.

9. HOLANDA
Dutch Blockchain Coalition

18. A *Dutch Blockchain Coalition* (DBC) é uma *joint venture* entre parceiros do governo, academia e indústria, sediada na Holanda. A missão da DBC é desenvolver aplicações

de *blockchain* confiáveis, robustas, criar as melhores condições possíveis para permitir o surgimento de aplicações de *blockchain* e utilizar *blockchain* como uma fonte de confiança, bem-estar, prosperidade e segurança para cidadãos, empresas, instituições e órgãos do governo. Para essa missão, a DBC representa um catalisador e facilitador, que ativa e se conecta com uma extensa rede público-privada. A coalisão trabalha com agenda de ação, que prospecta as possibilidades da tecnologia *blockchain*, avalia se essa tecnologia satisfaz a legislação e cria programas de pesquisa e treinamento relacionados ao tema. A iniciativa concentra-se em três linhas de ação: desenvolver infraestrutura de suporte a redes *blockchain* - identidades digitais, avaliar condições para utilização de *blockchain* e desenvolver e avaliar socialmente a solução. No âmbito internacional, a DBC celebra acordos sobre padronização, normas e governança, em parceria com a Organização Internacional para Padronização (*International Organization for Standardization* – ISO) e com a Comissão Europeia.

Pension infrastructure

19. Este projeto da Holanda é uma *blockchain* com o objetivo de criar um sistema de administração de pensões mais transparente. O projeto tem várias partes interessadas: empregadores, autoridades tributárias, fundos de pensão e cidadãos, com diferentes funcionalidades para cada um desses papeis. Contratos inteligentes são usados para determinar, não apenas as regras de acesso, como também as regras de contribuição para os fundos de pensão de um cidadão. O ambiente de execução é a *Ethereum*.

20. Os benefícios da *blockchain* incluem: economia na administração de pensões, devido à automação de verificações e ao compartilhamento de dados; mais segurança, devido às garantias de distribuição e integridade das informações; e mais transparência. Além disso, o cidadão pode visualizar, em tempo real, informações sobre a evolução de seu plano de pensão e respectivo saldo. Já a autoridade tributária pode acessar todas as informações das contribuições de vários fundos associados a uma pessoa, aumentando a supervisão regulatória sobre o sistema de pensões.

Stadjerspas smart vouchers

21. *Stadjerspas* é um serviço que utiliza *blockchain* para fornecer *vouchers* de desconto para cidadãos de baixa renda no município de Groningen, Holanda. Em 2016, o sistema de *vouchers*, originalmente baseado em papel, foi movido para uma *blockchain*. Os "*smart vouchers*" têm regras que especificam beneficiários elegíveis, limites e condições de uso e podem ser usados em clubes, cinemas e para subsídios em outros programas. É assegurado que o dinheiro destinado para um propósito específico seja de fato gasto naquele propósito – auditabilidade. Usuários podem visualizar os *vouchers* para os quais são elegíveis em um aplicativo móvel. Com a utilização de uma rede *blockchain*, espera-se obter ganhos em eficiência – pagamentos automáticos aos provedores de serviço e eliminação de processos baseados em papel.

10. SUÉCIA

Chromaway property transactions

22. Embora o processo de transferência imobiliária funcione bem na Suécia, as autoridades estavam interessadas em descobrir se ele poderia ser melhorado com o uso de *blockchain*, tornando-se ainda mais rápido, transparente e barato. Bancos, autoridades tributárias e desenvolvedores colaboraram para mapear o processo de transferência imobiliária na *blockchain*, o qual foi utilizado para realizar uma prova de conceito.

23. O projeto utiliza a tecnologia *blockchain* para automatizar a execução das transações imobiliárias. Ao fornecer um fluxo de trabalho comum para vários atores, são obtidos ganhos de eficiência e economia. Para os cidadãos, não há necessidade de presença física no banco ou cartório, o que reduz parcialmente a necessidade dos tradicionais cartórios. Além disso, a nova solução reduz o trabalho em papel, o risco de fraude e, significativamente, os custos de transação.

11. SUÍÇA

Crypto Valley Association

24. Sediada na cidade de Zug, Suíça, a *Crypto Valley* é uma associação independente, apoiada pelo governo, concebida para construir o maior ecossistema de tecnologias *blockchain* e criptográficas do mundo. A iniciativa apoia *startups* e empresas por meio de recomendação de políticas, apoio em projetos em setores verticais, suporte em pesquisas e organização de conferências, *hackathons* e outros eventos do setor. O projeto também mantém conexões ativas com iniciativas semelhantes em todo o mundo, promovendo a inovação em *blockchain* e tecnologia criptográfica em uma escala global.

uPort11

25. A cidade de Zug lançou uma identidade emitida pelo governo na *blockchain Ethereum.* O objetivo é fornecer uma identidade para autenticação em serviços de *e-gov* e compartilhamento de dados pessoais. Da perspectiva do cidadão, o serviço permite a divulgação seletiva de informações para determinadas empresas e instituições. Riscos de ataques cibernéticos são reduzidos e há um menor custo de infraestrutura, uma vez que a propriedade e atestação de identidades é redirecionada aos próprios cidadãos. Não há, portanto, necessidade de armazenar dados pessoais, o que reduz o risco de vazamento de dados. São obtidos, também, ganhos em eficiência, pois muitas empresas e instituições públicas podem compartilhar uma única solução para autenticação dos serviços e acesso a eles, não sendo necessária a autenticação do cidadão por inúmeras senhas.

12. DUBAI
Dubai Blockchain Strategy 2021

26. Como parte de seus esforços para adotar as mais recentes tecnologias e práticas de inovação em nível global, a *Dubai Future Foundation* anunciou o estabelecimento do *Global Blockchain Council*, para explorar e discutir aplicações atuais e futuras, bem como organizar transações por meio da plataforma blockchain. Em abril de 2018, o governo lançou a *Dubai Blockchain Strategy* 2021, visando a capitalizar a tecnologia blockchain para transformar 50% das transações governamentais na plataforma *blockchain* até 2021. A estratégia se apoia em três pilares: eficiência do governo, indução da indústria e liderança internacional da tecnologia. O país usará *blockchain* para realizar transações digitais, dando a cada usuário um número de identificação exclusivo que aponta para suas informações na rede. Ao adotar essa tecnologia, o governo dos Emirados Árabes Unidos espera economizar tempo e dinheiro com transações e documentos processados em papel atualmente.

13. ILHA DE MAN
Isle of Man Blockchain Office and Sandbox

27. A *Blockchain Sandbox* é uma proposta de área de testes. Liderada pela *Digital Isle of Man*, consiste em uma iniciativa para posicionar a Ilha de Man como país pioneiro para sediar negócios baseados em *blockchain*. A *Blockchain Sandbox* foi criada para empresas, proporcionando um espaço colaborativo para empresas realizarem pilotos e testarem produtos e serviços inovadores, em que os riscos regulatórios são reduzidos.

28. Já a criação do *Blockchain Office* tem os seguintes benefícios: capacidade de trabalhar com um regulador, para entender como a legislação está evoluindo e como ela afetará os negócios; assistência na preparação do *sandbox* regulatório; orientação sobre demonstração futura do produto; operação em ambiente totalmente favorável através do sandbox; e engajamento da comunidade *blockchain*.

14. SINGAPURA
Ubin

29. O Projeto Ubin é um projeto colaborativo com a indústria para explorar o uso da tecnologia *blockchain* e de DLTs para compensação e liquidação de pagamentos e valores mobiliários, além de servir para pagamentos transacionais interbancários e de títulos governamentais mais rápidos, eficientes e de baixo custo. O projeto é liderado pela *Monetary Authority of Singapura* (MAS) e tem como meta desenvolver alternativas mais simples e eficientes para os mecanismos de pagamentos atuais do sistema financeiro.

30. O Projeto Ubin é um projeto multifásico plurianua, e está, neste momento, em sua quinta fase, com cinco relatórios de projeto publicados. Além da experimentação técnica, a fase atual do Projeto Ubin (fase 5) procurou determinar a viabilidade comercial

e o valor da rede de pagamentos baseada em *blockchain* e, atualmente, está passando por testes da indústria, para determinar sua capacidade de integração com aplicações comerciais de blockchain.

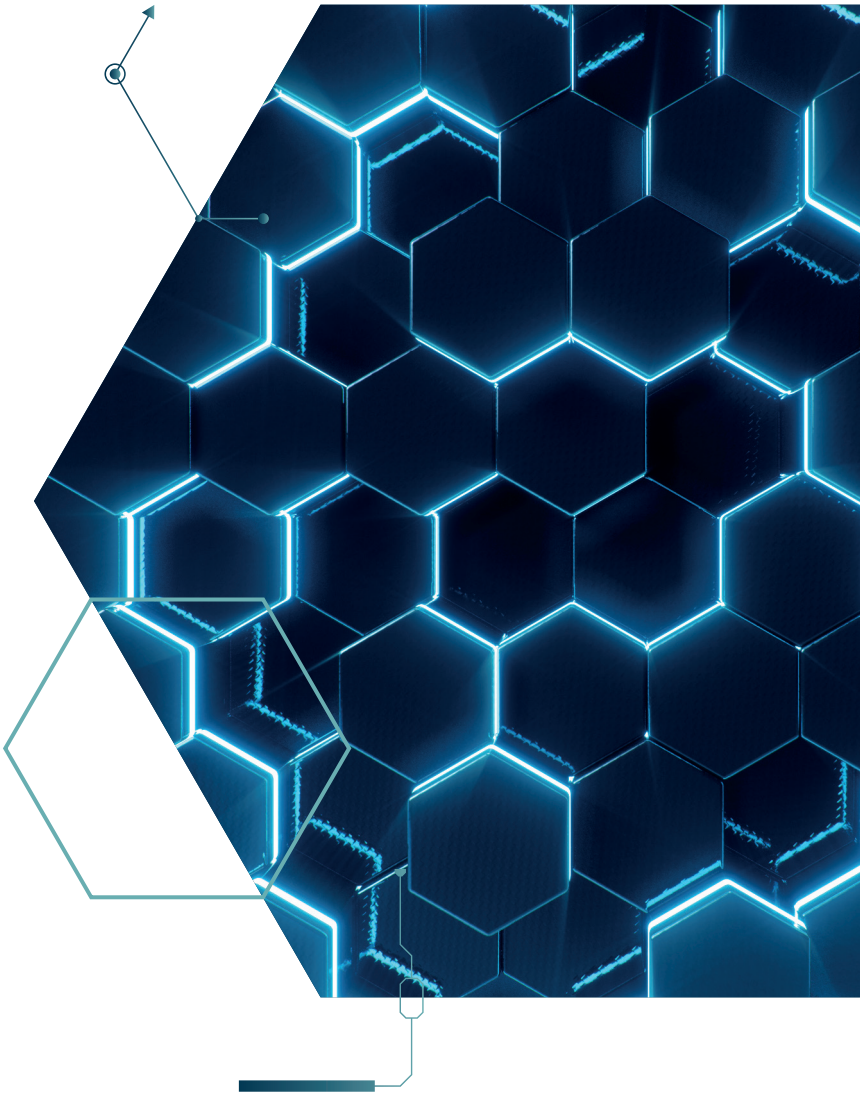
31. Uma funcionalidade desse projeto que merece ser destacada é o uso de *Hashed Time-Locked Contracts* (HTLC) para garantir que uma transação seja atômica de um pagamento em dólar canadense (CAD) para dólar de Cingapura (SGD), ou seja, entre duas plataformas DLTs diferentes.

15. STATE OF WEST VIRGINIA
WV's Secure Mobile Voting Application

32. O projeto permite que os eleitores de *West Virginia*, USA, que estejam servindo as forças armadas ou residam fora do estado recebam, votem e devolvam suas cédulas de votação de forma remota e com segurança. De acordo com o estado de *West Virginia*, o projeto é inédito na história dos Estados Unidos, sendo o primeiro aplicativo de votação móvel e o primeiro a utilizar a tecnologia *blockchai*n em uma eleição federal. Os líderes do projeto consideram que o piloto obteve sucesso, após superar requisitos de segurança, que incluíam utilização de padrões federais para desenvolvimento de software, testes de penetração, auditoria de código fonte e auditoria da infraestrutura de nuvem do sistema. O aplicativo também utiliza *software* de reconhecimento facial e biometria para autenticar a identidade do eleitor, aumentando a confiança do processo.

16. ALEMANHA
Blockchain Strategy of the Federal Government

33. O objetivo da estratégia de *blockchain* do governo alemão é criar uma estrutura regulatória direcionada ao investimento e crescimento, na qual as empresas de mercado funcionem sem intervenções estatais, garantindo o princípio da sustentabilidade. A ideia é explorar as oportunidades oferecidas pela tecnologia *blockchain* e seu potencial de mobilização para a transformação digital. A estratégia descreve uma visão holística da tecnologia, mostra os objetivos e princípios do governo federal em relação à tecnologia *blockchain* e propõe medidas específicas em cinco áreas de ação a serem adotadas até o final de 2021, relacionadas à: *blockchain* no setor financeiro; criação de regulação inovadora; previsibilidade e transparência para favorecer os investimentos; aplicação da tecnologia na Administração Pública; e conscientização e colaboração em favor da tecnologia.



Responsabilidade pelo conteúdo
Secretaria-Geral da Presidência (Segepres)
Secretaria das Sessões (Seses)

Projeto gráfico, diagramação e capa
Secretaria de Comunicação (Secom)
Núcleo de Criação e Editoração (NCE)

Tribunal de Contas da União
Secretaria-Geral da Presidência (Segepres)
SAFS Quadra 4 Lote 1
Edifício Sede Sala 146
70.042-900, Brasília – DF
(61) 3316-5338
segepres@tcu.gov.br

Ouvidoria do TCU
0800 644 1500
ouvidoria@tcu.gov.br

Impresso pela Senge/Segedam

TRIBUNAL DE CONTAS DA UNIÃO

_MISSÃO

Aprimorar a Administração Pública em benefício da sociedade por meio do controle externo.

_VISÃO

Ser referência na promoção de uma Administração Pública efetiva, ética, ágil e responsável.

www.tcu.gov.br