

LIFT *papers*

REVISTA DO LABORATÓRIO
DE INOVAÇÕES FINANCEIRAS
E TECNOLÓGICAS

2ª EDIÇÃO

LIFT Papers

Revista do Laboratório de Inovações Financeiras e Tecnológicas

Volume 2 • Número 1 • Maio 2020

Editor-Chefe da Revista

André Henrique de Siqueira, PhD

Editor Adjunto da Revista

Aristides Andrade Cavalcante Neto, MSc
Rodrigo de Azevedo Henriques

Corpo Editorial da Revista

Marcus Vinicius Cursino Soares
Rafael Sarres de Almeida

Ficha catalográfica elaborada pela Biblioteca do Banco Central do Brasil

LIFT Papers / Banco Central do Brasil. Vol. 2, n. 1, (maio 2020). Brasília: Banco Central do Brasil, 2020.

Semestral

Disponível em:

https://www.liftlab.com.br/docs/lift_Red.pdf.

ISSN 2675-2859

1. Inovação Tecnológica – Brasil. 2. Sistema Financeiro – Brasil. 3. Crédito. I. Banco Central do Brasil.

CDU 336.7:004.738.5

Presidente do Banco Central do Brasil

Roberto Campos Neto

Presidente da Fenasbac

Paulo Renato Tavares Stein

Comitê-Executivo LIFT 2020

Aloisio Tupinambá Gomes Neto

André Henrique de Siqueira – Coordenação

Aristides Andrade Cavalcante Neto – Coordenação

Breno Santana Lobo

Hélio Fernando Siqueira Celidonio

Marcus Vinicius Cursino Soares

Rafael Sarres de Almeida

Reinaldo Lívio Wielewski

Rodrigo de Azevedo Henriques – Coordenação

Maria Aparecida Padilha Ribeiro – Coordenação

Representantes dos Parceiros de Tecnologia

AWS

Leandro Bennaton

Ana Motta

IBM

Fábio Luis Marras

Ludimila Salimena

Leonardo Guaraldi Couto

MICROSOFT

Ronan Damasco

João Paulo Fernandes

Cristiano Gomes

R3

Keiji Sakai

Luiz Jerônimo

MULTILEDGERS

Pedro Souza

Marcela Gonçalves

CIELO

Gustavo Burin

Whatson Silva

***BluPay* – Switch de Pagamento Instantâneo em DLT Corda**

Rubens Antonio Rocha Junior

O *switch* de pagamentos instantâneos *BluPay* integrará as principais oportunidades geradas pelas mudanças previstas pelo Banco Central do Brasil no ecossistema financeiro com os comunicados sobre pagamentos instantâneos (Comunicado 32.927, de 21 de dezembro de 2018) e *open banking* (Comunicado 33.455, de 24 de abril de 2019). O *switch* de pagamentos instantâneos *BluPay* é uma solução baseada em conceitos *blockchain*, que usa em sua arquitetura a plataforma DLT Corda. O uso de tais tecnologias viabiliza a liquidação, em tempo real, de pagamentos entre prestadores de serviço, permitindo que as transações possam ser processadas de forma segura 24 horas por dia, sete dias por semana e em todos os dias do ano. O principal diferencial inovador do projeto é prover uma camada de aplicação que implementa *Smart Contracts* por meio da tecnologia DLT Corda, resultando em transparência, segurança, privacidade e rastreabilidade, possibilitando executar uma conciliação entre as partes envolvidas nas transações e, com isso, diminuir a quantidade de requisições ao Sistema de Liquidação, gerando economia em chamadas e otimizando a performance do Sistema Financeiro Nacional.

..... Introdução

Sendo a internet um dos principais veículos de comunicação plenamente consolidados e em plena evolução, podemos elencar diversos setores e aspectos influenciados pela tecnologia, como as áreas sociais e político-econômicas de um país. Nessa linha, pode-se dizer que o Sistema Financeiro Nacional (SFN), por intermédio do Banco Central do Brasil (BCB), tem acompanhado essa evolução tecnológica para promover melhorias no sistema de pagamentos no Brasil, influenciando como os brasileiros transferem seus recursos financeiros entre pessoas físicas e/ou pessoas jurídicas.

Assim como a emissão de cheques em papel foi uma grande novidade no sistema financeiro, os cartões de crédito e débito inovaram na experiência dos usuários, tornando-se um meio de pagamento cada vez mais usado.

Com o pagamento instantâneo, pretende-se criar uma melhor experiência de utilização de serviços financeiros utilizados em nosso cotidiano, tais como:

- uso de dinheiro em espécie, o que pode trazer inconvenientes relacionados à segurança;
- memorização de várias senhas de cartões débito;
- restrições para saque de qualquer valor em qualquer horário do dia;
- escassez de recursos financeiros, causando um impacto econômico, i.e., “menos dinheiro circulando no comércio”;
- alto número de desbancarizados¹ no país, o que restringe o acesso dessas pessoas ao sistema financeiro.

Em linhas gerais, pretende-se alcançar com o projeto que usuários efetuem as suas movimentações financeiras de forma mais prática, segura, confiável e sem limitações.

Utilizando tecnologias modernas aliadas à grande demanda por rapidez e eficiência, a camada de aplicação *BluPay* para o *switch* de pagamentos instantâneos tem como objetivo oferecer uma plataforma de integração e conectividade que atenda aos requisitos elencados nos comunicados oficiais emitidos pelo BCB (Comunicado 32.927, de 21 de dezembro de 2018 e Comunicado 33.455, de 24 de abril de 2019) para implementação do Sistema de Pagamentos Instantâneos no Brasil.

.....
¹ Termo usado para pessoas físicas sem vínculo com qualquer instituição bancária.

.....1 Objetivos

O *switch* de pagamentos instantâneos *BluPay* tem como objetivo oferecer uma plataforma de conciliação e conectividade que atenda aos requisitos do BCB para implementação do Sistema de Pagamentos Instantâneos no Brasil.

Essa plataforma conta com uma camada de aplicação que implementa serviços tais como conciliação bruta em tempo real das diferentes transações permitidas no Sistema de Pagamentos Brasileiro entre os nós participantes da rede. Essa camada possui acesso por quaisquer instituições que desejam usar o Sistema de Pagamentos Instantâneos, desonerando o Sistema de Transferência de Reserva (STR) do alto processamento de transações.

.....2 Fundamentação teórica

Qualquer inovação tecnológica, quando bem aplicada, tem a capacidade de melhorar não somente a vida de um número restrito de pessoas, mas de milhões de cidadãos ao redor do mundo, de forma democrática, transparente e totalmente acessível. Não é raro o consumo de notícias sobre descobertas que passam a impressão de estarem muito distantes, seja por questões financeiras ou geográficas.

Para que uma nova tecnologia tenha impacto, é preciso que ela se faça presente na rotina das pessoas, resolvendo problemas recorrentes com inteligência e praticidade para substituir tecnologias existentes. Esse é um dos pilares para a disrupção tecnológica, a exemplo da tecnologia *blockchain*.

A popularização do *blockchain* foi associada ao *Bitcoin*² nos últimos anos, porém a sua empregabilidade é mais extensa do que o uso em criptomoedas. Essa tecnologia é extremamente versátil e compatível com incontáveis aplicações que necessitem de transparência, colaboração e descentralização. Dessa forma, permite a criação de um ecossistema altamente democrático e facilmente acessível, no qual todos os seus participantes tomam e validam decisões que impactam diretamente o seu funcionamento. O protagonismo é distribuído, sem a concentração das definições nas mãos de um seletivo grupo de tomadores de decisões.

Essa atuação de toda a rede garante sua segurança e credibilidade, em um cenário no qual tudo fica registrado, e a chance de alteração de dados ou fraudes é inexistente. A confiança é estabelecida por meio da colaboração, e os contratos inteligentes (nos termos do *blockchain*, os chamados *smart contracts*) ajudam a assegurar tudo que é decidido. Aliando o mais alto nível em criptografia a ideias inovadoras, surge um cenário propício ao desenvolvimento de projetos com muito pioneirismo.

É sabido que ainda há muito a ser descoberto nessa área, mas a procura por novas soluções e o aperfeiçoamento do que já vem sendo desenvolvido é contínuo. Um ponto, no entanto, é certo: qualquer atividade que demande transparência de registros de atividades, preze pela colaboração entre todos os seus participantes e que se proponha a ser segura, honesta e verdadeiramente inovadora, tem no *blockchain* a justificativa para sua implementação.

.....
² Criptomoeda descentralizada ou dinheiro eletrônico para transações ponto a ponto criada em 2008.

Seja na política (por meio do registro de votos em uma eleição ou dos gastos de políticos em um mandato), no mundo corporativo (validando todas as etapas dentro de uma *supply chain* ou criando um *token* para uso interno), na educação (onde estudantes podem desenvolver projetos socioambientais sobre uma plataforma *blockchain*) ou qualquer outro segmento, o *blockchain* tem inúmeras aplicabilidades.

Prado (2017) descreve esse conteúdo da seguinte forma:

(...) Como o *blockchain* elimina intermediários, as transações acontecem em tempo real, com menos custos e sem perder em segurança, já que elas podem ser verificáveis e auditáveis. O risco de fraudes é reduzido por meio de contratos inteligentes.

2.1 Conceitos básicos

2.1.1 Rede *peer-to-peer* (ponto a ponto)

A computação ponto a ponto (P2P) pode ser definida como um paradigma genérico de arquitetura de *software*, classificado no mesmo nível de abstração da computação cliente/servidor (ver figura 1). Os sistemas baseados no paradigma P2P consistem em componentes de *software*, chamados de pontos, nós ou *peers*, que compartilham e/ou utilizam os recursos de outro(s) ponto(s) para execução de tarefas de modo. Cada ponto atua como cliente e servidor simultaneamente, o que fez surgir o termo *servent* (*server* e *client*). Os recursos compartilhados podem ser os mais variados: poder computacional, espaço de armazenamento, largura de banda e conteúdo. Não existe restrição em relação à quantidade de pontos que podem participar do sistema. Os trabalhos de Aberer *et al.* (2002a) e Milojevic *et al.* (2002) apresentam uma visão geral sobre o paradigma P2P e uma descrição atualizada de seus principais sistemas.

A computação P2P pode oferecer inúmeras vantagens, entre elas:



- aumento do poder computacional, aproveitando o tempo ocioso das estações de trabalho conectadas à rede;
- capacidade de os pontos poderem assumir funções diferenciadas na rede, ora como clientes, ora como servidores;
- redução de custo para o compartilhamento de recursos, possibilitando a realização de tarefas utilizando a infraestrutura disponível no momento, por exemplo, armazenamento de *backup*;
- manutenção da autonomia dos pontos participantes, evitando que um ponto seja controlado por outro.

O modelo de rede com topologia P2P pura ou descentralizada é o que segue mais fielmente os princípios do paradigma P2P. Todos os pontos são capazes de se comunicar diretamente entre si e possuem o mesmo papel na rede. Sua principal característica está no funcionamento totalmente descentralizado, ou seja, não existe a ideia de um servidor ou repositório central (ver Figura 1). Os pontos podem se conectar automaticamente e começar a compartilhar recursos, serviços e/ou conteúdo com quaisquer outros pontos já conectados. Os mecanismos de busca e manutenção da infraestrutura, assim como o compartilhamento de recursos, estão distribuídos pela rede. Cada ponto é responsável por manter informações sobre seus próprios dados e, conseqüentemente, ao receber uma solicitação de consulta, pode responder a ela e/ou reescrevê-la, repassando-a aos pontos vizinhos.

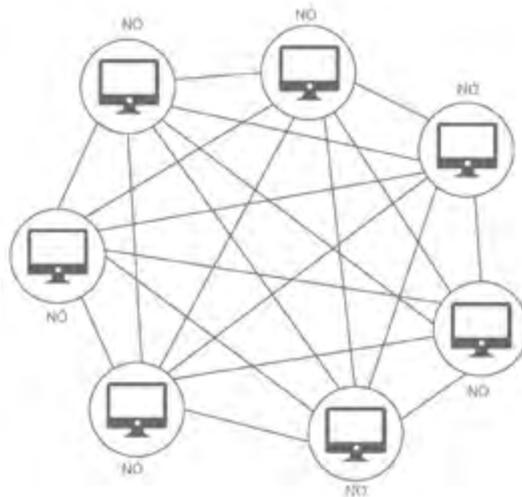
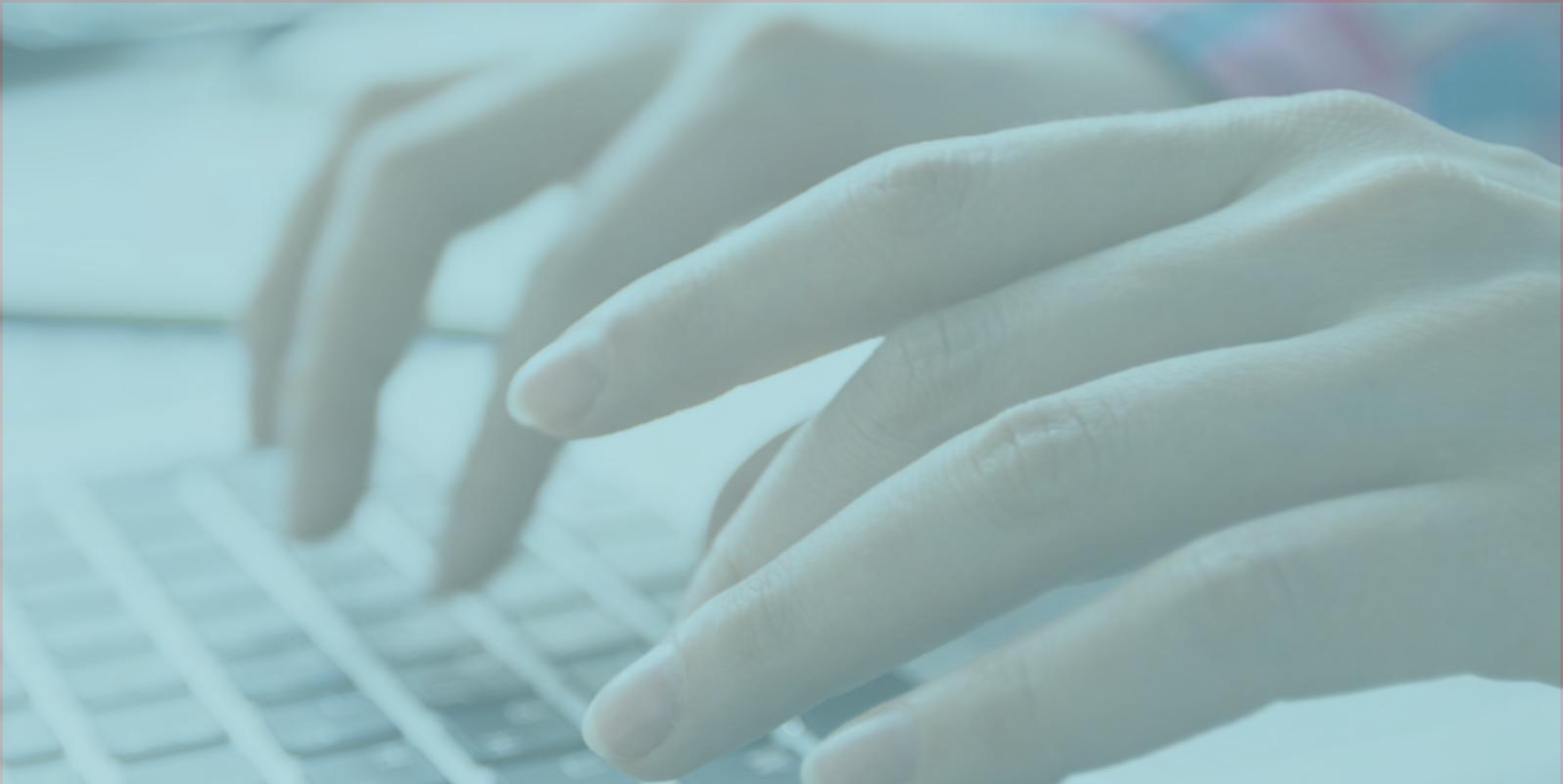


Figura 1 – Rede *peer-to-peer*



Justamente por apresentar estrutura descentralizada, a rede P2P possui uma maior escalabilidade, pois, à medida que o número de nós cresce, a performance da rede também é elevada. Já uma rede no modelo cliente/servidor tem seu desempenho reduzido de acordo com o crescimento de requisições vindas por parte dos clientes.

2.1.2 Criptografia

A criptografia é um termo atualmente muito relacionado com a segurança em rede, mas que é conhecido desde os tempos antigos. A criptografia é um processo de ocultação, por meio de códigos, do real significado de uma informação, garantindo que somente o remetente e o destinatário entendam o seu conteúdo. Amaro (2009) ainda é mais abrangente quanto à sua conceituação:

Um processo pelo qual um texto puro (normal) é convertido em uma mensagem codificada (texto cifrado), através da aplicação de um algoritmo (...), de forma a ser possível retornar a mensagem à sua forma original.

Ainda analisando a criptografia, Amaro (2009) aponta os seus quatro princípios básicos:

- Confidencialidade da mensagem: somente o destinatário deve ser capaz de acessar a mensagem em sua forma original;
- Integridade da mensagem: capacidade de detectar qualquer alteração durante a transmissão da mensagem;
- Autenticação do remetente: a possibilidade de o destinatário identificar o remetente e ter a garantia de que a mensagem é realmente enviada por ele;
- Não repúdio ao remetente: impossibilidade de o remetente negar o envio da mensagem.

Vale ressaltar que esses princípios não são entregues de uma só vez ao se utilizar uma criptografia. Para isso, é necessário o uso de serviços – por exemplo, função *hash* e assinatura digital – para a entrega total desses elementos. Não é preciso necessariamente haver todos os princípios, como no caso do *blockchain*, que preza mais pela integridade e autenticação, visto que tem um caráter de manter as informações abertas.

Na Ciência da Computação, a criptografia é categorizada em dois tipos: simétrica (de chave privada) ou assimétrica (de chave pública).

2.1.3 Criptografia simétrica

Também chamada de criptografia de chave secreta ou única, utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados. Em casos nos quais a informação é codificada e decodificada por uma mesma pessoa, não há necessidade de compartilhamento da chave secreta. Entretanto, quando essas operações envolvem pessoas ou equipamentos diferentes, é necessário que a chave secreta seja previamente combinada por meio de um canal de comunicação seguro (para não comprometer a confidencialidade da chave). Exemplos de métodos criptográficos que usam chave simétrica são: AES, Blowfish, RC4, 3DES e IDEA.



Figura 2 – Criptografia simétrica

2.1.4 Criptografia assimétrica

Também conhecida como criptografia de chave pública, utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada; e uma privada, que deve ser mantida em segredo por seu dono. Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Qual chave usar para codificar depende da proteção que se deseja, se confidencialidade ou autenticação, integridade e não repúdio. A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um *smartcard* ou um *token*. Exemplos de métodos criptográficos que usam chaves assimétricas são: RSA, DSA, ECC e Diffie-Hellman.



Figura 3 – Criptografia assimétrica

2.1.5 Função hash

Uma função *hash* é um método criptográfico que, quando aplicado sobre uma informação, independentemente do tamanho que ela tenha, gera um resultado único e de tamanho fixo, chamado *hash*.³

Pode-se utilizar *hash* para:

- verificar a integridade de um arquivo armazenado no computador ou em *backups*;
- verificar a integridade de um arquivo obtido da internet (alguns sites, além do arquivo em si, também disponibilizam o *hash* correspondente, para que se possa verificar se o arquivo foi corretamente transmitido e gravado);
- gerar assinaturas digitais.

Para verificar a integridade de um arquivo, por exemplo, pode-se calcular o *hash* dele e, quando julgar necessário, gerar novamente esse valor. Se os dois *hashes* forem iguais, então pode-se concluir que o arquivo não foi alterado. Caso contrário, esse pode ser um forte indício de que o arquivo esteja corrompido ou de que foi modificado. Exemplos de métodos de *hash* são: SHA-1, SHA-256 e MD5.



Figura 4 – Exemplo da função hash

³ O *hash* é gerado de tal forma que não é possível realizar o processamento inverso para se obter a informação original e qualquer alteração na informação original produzirá um *hash* distinto. Apesar de ser teoricamente possível que informações diferentes gerem *hashes* iguais, a probabilidade de isso ocorrer é bastante baixa.

2.1.6 Assinatura digital

A assinatura digital permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isso e que ela não foi alterada.

A assinatura digital baseia-se no fato de que apenas o dono conhece a chave privada e que, se ela foi usada para codificar uma informação, então apenas seu dono poderia ter feito isso. A verificação da assinatura é feita com o uso da chave pública, pois, se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo.

Para contornar a baixa eficiência característica da criptografia de chaves assimétricas, a codificação é feita sobre o *hash* e não sobre o conteúdo em si, pois é mais rápido codificar o *hash* (que possui tamanho fixo e reduzido) do que a informação toda.

2.1.7 Árvore Merkle

Uma Árvore Merkle é uma estrutura de dados utilizada por sua eficiência em resumir e averiguar a integridade de grandes volumes de dados. No *blockchain*, ela funciona sumarizando todos os registros presentes em um bloco, criando uma espécie de impressão digital dos registros (ANTONOPOULOS, 2014).

Na Ciência da Computação, o termo “árvore” é utilizado para representar estruturas de ramificação. Porém, diferentemente dessas outras árvores, a representação nessa estrutura ocorre de modo contrário, em que a raiz (normalmente ligada à parte inferior) está disposta no topo; e as folhas, posicionadas na base.

Essa estrutura é construída por meio de repetidas submissões de pares de nós de *hash*, até que reste somente uma única *hash*, chamada Raiz da Árvore de Merkle, alocada nos metadados contidos no bloco (ANTONOPOULOS, 2014).

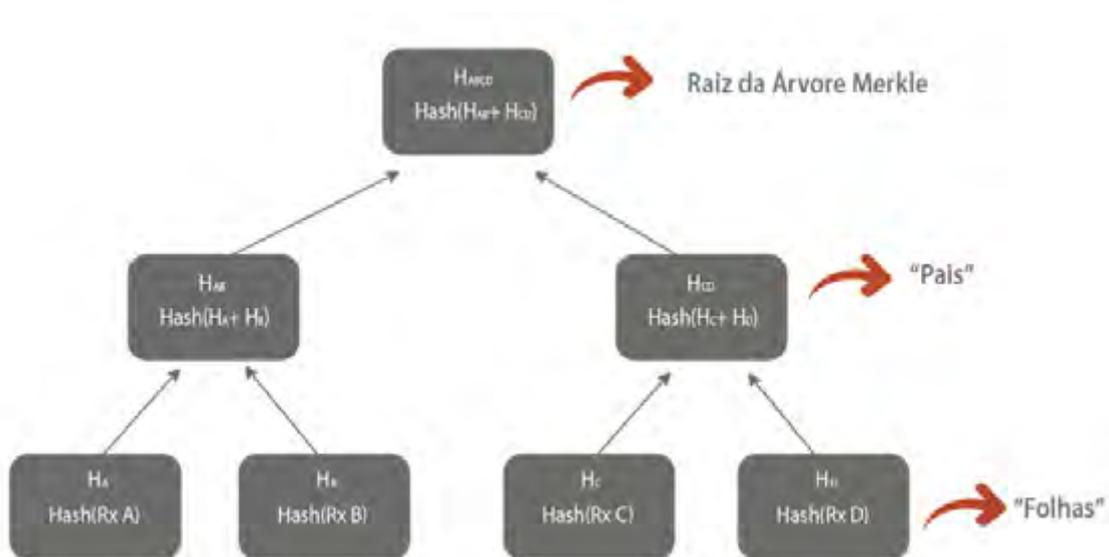


Figura 5 – Estrutura da Árvore de Merkle

Na Figura 5, tem-se um exemplo dessa estrutura. Nesse caso, contendo quatro registros: A, B, C e D. Dispostos na parte inferior da árvore, eles são denominados “folhas”. Cada folha é submetida a uma função *hash* que, concatenada com o seu respectivo par, resulta no nó “pai”. Seguindo a mesma lógica, os pais desses registros também são submetidos a uma função *hash*, criando assim a Raiz da Árvore Merkle. Por ser uma árvore binária, ou seja, é necessário um par de registros, em caso de o número total de folhas ser um número ímpar, há a duplicação da folha que não possui seu respectivo par (ANTONOPOULOS, 2014).

No exemplo apresentado, a *hash* de cada folha representa a *hash* de um respectivo registro; já a raiz da Árvore Merkle representa a *hash* do bloco. Pode-se perceber que, em qualquer tentativa de alteração da *hash* da raiz, todos os ramos são conjuntamente alterados, resultando em um erro no próprio bloco e no bloco posterior, que também possui em seus metadados a *hash* do bloco antecessor. Essa funcionalidade, em conjunto com a rede descentralizada, garante a imutabilidade de qualquer informação disposta no *blockchain*.

2.2 Blockchain

Blockchain é o nome pelo qual ficou conhecida a tecnologia que viabilizou o *Bitcoin*, um sistema de pagamentos totalmente digital que independe de uma autoridade para validar e verificar as transações. Com ele, é possível enviar dinheiro para outra pessoa que esteja em qualquer lugar do mundo, com a segurança e a confiança de que a transação será realizada, mesmo que não se conheça tal pessoa (NAKAMOTO, 2008). Mais recentemente, eles foram propostos como meio de implementar outros tipos de aplicativos descentralizados (FERRER, 2016; LAZAROVICH, 2015; LEWENBERG et al., 2015).

Simplificadamente, a tecnologia agrupa dados em blocos (*block* em inglês) que vão se juntando de forma a criar uma cadeia (*chain* em inglês) ordenada e linear conforme mostrado na Figura 6.



Figura 6 – Blockchain

A tecnologia *blockchain* baseia-se na noção de um livro-razão distribuído, que atua como um banco de dados contendo informações sobre o histórico de transações de uma empresa. É constantemente auditado por grupos de agentes (selecionados de acordo com diferentes políticas, dependendo do domínio do aplicativo). O resultado de cada auditoria é armazenado em um bloco e transmitido para a rede. Os blocos são anexados sequencialmente ao livro, formando uma cadeia criptograficamente vinculada. Tentativas de adulterar os blocos ou alterar a sua ordem podem ser facilmente detectadas.

Toda a comunidade pode aceitar ou rejeitar a confiabilidade de qualquer bloco, de acordo com um conjunto predefinido de regras. Se um agente receber várias adições válidas em suas cópias locais do livro-razão, eles sempre escolhem a maior cadeia de blocos válidos (ou a mais antiga, se tiverem o mesmo comprimento), ignorando outras cadeias conflitantes e menos relevantes. Esse procedimento conceitualmente simples garante que, eventualmente, seja alcançado consenso, mesmo em cenários em que a propagação é lenta devido à alta latência da rede.

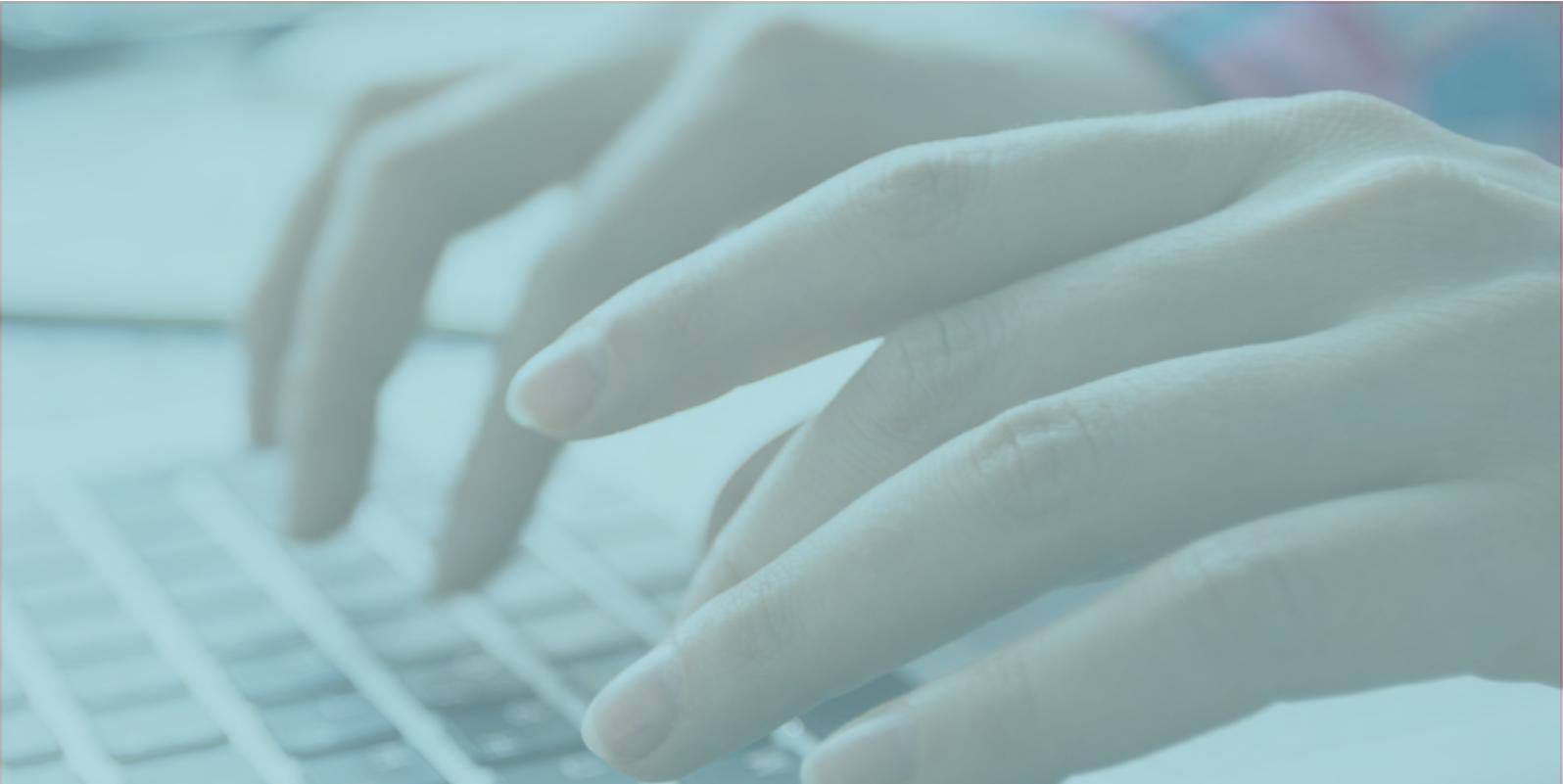
Da mesma forma, nós mal-intencionados podem tentar inserir entradas maliciosas no livro-razão, mas a comunidade simplesmente rejeitará seus bloqueios e ignorará sua cadeia, forçando efetivamente que cumpram as regras. A capacidade de criar um consenso distribuído é muito importante, pois impede que as informações registradas sejam falsas ou duplicadas.

Com essa característica, o *blockchain* permite que partes que não necessariamente tenham confiança uma na outra transacionem qualquer ativo digital sem a intermediação de alguma autoridade ou parte central responsável por atestar a veracidade das informações. É um registro seguro, auditável e imutável. Esse tipo de infraestrutura – ou seja, tanto a ideia original quanto suas derivações – pode potencialmente ser aplicada a diversas áreas, de diferentes formas.

2.3 *Smart contracts* (contratos inteligentes)

Com bancos de dados tradicionais, é fácil criar *software* que monitore um banco de dados, determine se uma determinada condição foi ou não cumprida e atualize o banco de dados de acordo. É exatamente isso que os contratos inteligentes fazem também, mas no ambiente confiável de *blockchains*. Um contrato inteligente não é inteligente nem legal; em vez disso, é um acordo entre duas ou mais partes, formulado e aplicado com código





criptográfico imutável. Esse código é executado em todos os nós da rede *blockchain* e determina como os dados no livro-razão distribuído são modificados.

Os contratos inteligentes eliminam a dependência de intermediários confiáveis ao fazer acordos comerciais. Normalmente, um contrato inteligente inclui termos e condições, métricas de desempenho e possivelmente multas. Durante a execução, o contrato inteligente monitorará, verificará e aplicará automaticamente as condições acordadas, o que pode potencialmente economizar tempo e dinheiro para as partes envolvidas.

2.4 Distributed Ledger Technology

Os livros-razão são os fundamentos da contabilidade – um sistema pelo qual as pessoas estabelecem quem possui o quê, quem tem o quê e quem deve o que a quem. Embora o conceito permaneça o mesmo, o meio usado para registrar transações variou ao longo do tempo graças aos avanços tecnológicos. De búzios a papiros, de livros a computadores – o objetivo sempre foi manter registros da maneira mais eficiente e eficaz possível.

Os seres humanos mantêm livros contábeis há milhares de anos e, embora o meio e os métodos tenham mudado ao longo do tempo, um elemento da manutenção de livros contábeis não mudou. Na nossa história, um terceiro sempre teve que registrar e supervisionar transações e manter contas. Isso faz sentido, pois fornece uma base para validação e permite que as pessoas que conduzem uma troca de valor confiem umas nas outras.

O crescimento do comércio e do comércio global levou à criação de uma vasta rede de sistemas de contabilidade, que são vulneráveis a tempo de inatividade, má interpretação e fraude, cujas repercussões podem ser catastróficas e de longo alcance – basta pensar na crise financeira de 2008.

A tecnologia de contabilidade distribuída é a primeira forma de contabilidade para eliminar a necessidade de terceiros. Isso permite que um livro-razão seja distribuído entre

todos os que o usam, colocando a responsabilidade de mantê-lo e validá-lo nas mãos de quem o usa. O resultado é um sistema descentralizado de registro de dados, em que as transações são instantâneas, transparentes, confiáveis e incorruptíveis.

A *Distributed Ledger Technology* (DLT) é o primeiro sistema a ignorar a necessidade de confiar um no outro ao realizar transações de valor, cujas implicações serão profundas e de longo alcance.

DLT é um termo genérico usado para descrever tecnologias que armazenam, distribuem e facilitam a troca de valor entre usuários, privada ou publicamente, e a tecnologia *blockchain* é apenas uma delas. Por ter sido a primeira DLT totalmente funcional, a tecnologia *blockchain* é mais conhecida do que os gráficos acíclicos direcionados por bloco (blockDAG) e do que os gráficos acíclicos direcionados baseados em transações (TDAG). Portanto, da mesma forma, que a categoria “veículo” abrange o carro de passageiro, o navio de carga e o ônibus espacial, o termo DLT abrange um amplo conjunto de tecnologias.

Blockchain é um tipo de DLT e abrange todos os dados governados por consenso e que não são centralizados.

Em resumo, a DLT é uma arquitetura de banco de dados que permite que os proprietários de bens digitais os transfiram de ponto a ponto. Cada transferência em uma DLT é mantida como um registro em um livro-razão distribuído.

Um livro-razão distribuído é um banco de dados armazenado em todos os nós em uma rede.

A DLT pode ter dois tipos de razão:

- livro-razão sem permissão (*permissionless ledger*): um livro-razão distribuído entre nós, que pode ser executado por qualquer pessoa sem permissão. O objetivo de um livro-razão sem permissão é possibilitar que qualquer pessoa contribua com dados para o livro-razão, e que todos os que possuam o livro-razão tenham cópias idênticas. Os nós mantêm a integridade do livro-razão, alcançando um consenso sobre seu estado. Um livro-razão sem permissão pode ser usado como um registro global imutável de transferências. Qualificamos esse tipo de livro como público;
- livro-razão permitido (*permissioned ledger*): um livro-razão distribuído apenas entre os nós pré-selecionados por uma autoridade central, como um banco ou um governo. Qualificamos esse tipo de livro como privado.

Quando os dados são armazenados em bancos de dados proprietários, é difícil compartilhar esses dados com outras pessoas, sem que sejam alterados e perdidos em outros bancos de dados.

A DLT cria uma única fonte de verdade em que todos os participantes podem confiar. Quando os dados são adicionados a um livro distribuído, qualquer pessoa com conexão à internet pode acessá-los, conectando-se a qualquer nó da rede.

2.4 ISO 20022

Uma abordagem única de padronização (metodologia, processo, repositório) a ser usada por todas as iniciativas de padrões financeiros, a ISO 20022 é uma norma internacional de várias partes, preparada pelo Comitê Técnico ISSO/TC68, responsável pelo desenvolvimento de padrões internacionais para a indústria de produtos e serviços financeiros. Descreve uma plataforma comum para o desenvolvimento de mensagens usando:

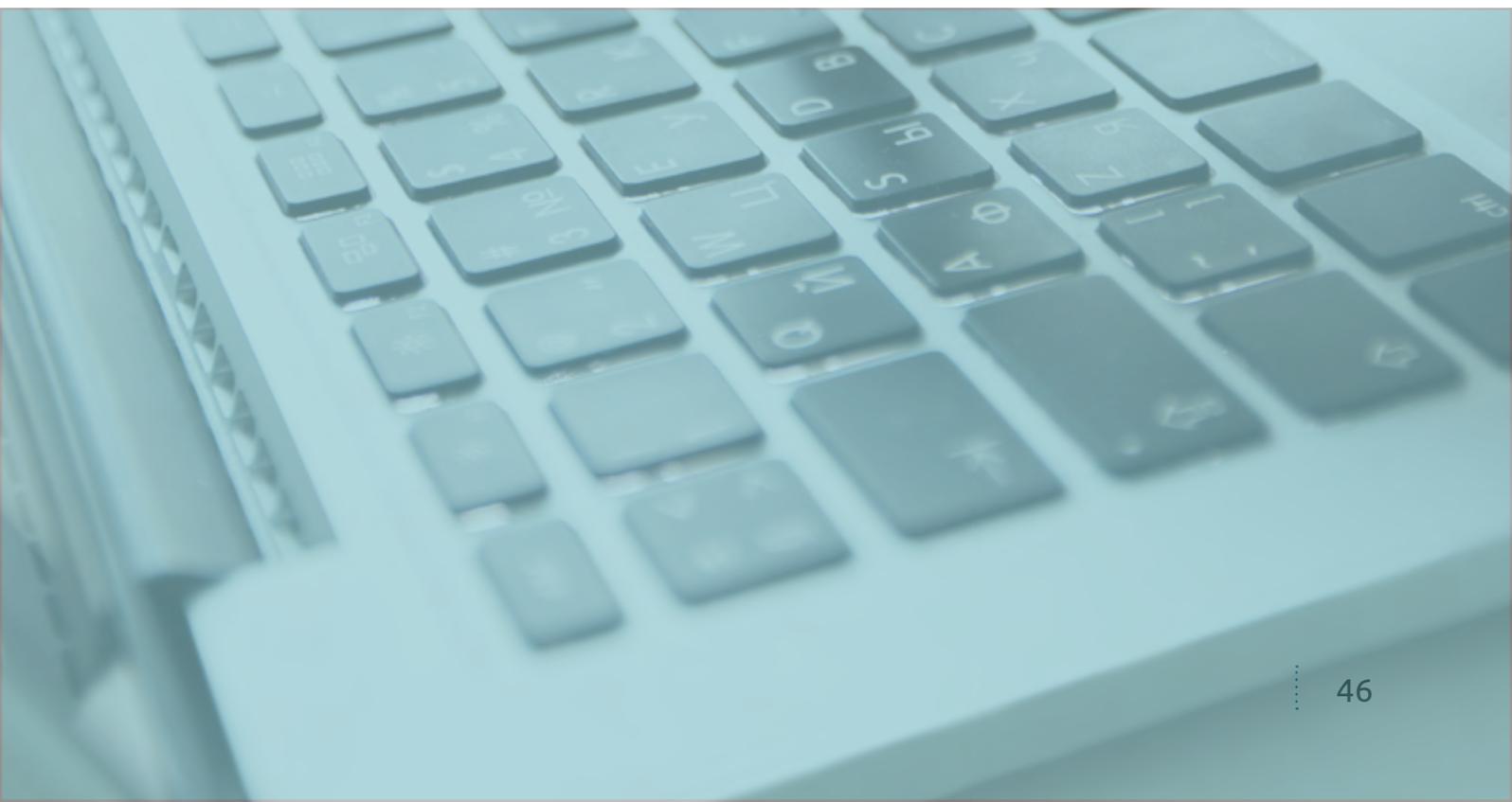
- uma metodologia de modelagem para capturar, de maneira independente da sintaxe, áreas de negócios financeiros, transações comerciais e fluxos de mensagens associados;
- um dicionário central de itens de negócios usados em comunicações financeiras;
- um conjunto de regras de design XML e ASN.1 para converter os modelos de mensagens em esquemas XML ou ASN.1, sempre que o uso da sintaxe ISO 20022 XML ou ASN.1 for preferido.

2.4.1 Mensagens ISSO 20022

O padrão de mensagens ISO 20022 é estruturado em cinco diferentes domínios de negócios:

- Pagamentos (*Payments*);
- Mercado de Capitais (*Securities*);
- Serviços para Comércio Internacional (*Trade Services*);
- Cartões (*Cards*);
- Câmbio (*Foreign Exchange*).

Cada domínio apresenta diferentes áreas de negócio, formadas por um conjunto de mensagens, estruturado de acordo com as operações a serem realizadas por meio da troca



de mensagens padrão ISO 20022. O domínio de Pagamentos, por exemplo, é composto pelas áreas Gerenciamento de Contas (*Account Management*), Iniciação de Pagamento (*Payments Initiation*), Compensação e Liquidação de Pagamentos (*Payments Clearing & Settlement*), Gerenciamento de Caixa (*Cash Management*) e Comunicação a Autoridades (*Authorities Communications*).

Cada área de negócio do padrão ISO 20022 representa o fluxo de comunicação para a realização de um processo específico. Assim, toda realização de inclusão ou alteração de modelos de negócios ou mensagens padrão ISO 20022 exige a observação dos processos, etapas, práticas, atores e papéis já registrados para aquela determinada área de negócio. Dessa forma, a metodologia evita que sejam desenvolvidas mensagens distintas para propósitos equivalentes ou semelhantes e que existam informações duplicadas e/ou de entendimento ambíguo.

Outra característica do padrão ISO 20022 é o conceito de três camadas distintas na construção das mensagens:

- a primeira camada fornece os conceitos e os processos de negócios-chaves para a criação das mensagens, como definição dos processos e atividades, regras de negócios, atores envolvidos etc.;
- a camada intermediária fornece modelos de mensagens ou mensagens lógicas. Essa camada descreve toda a informação que é necessária para desempenhar as atividades do negócio. Seus componentes são organizados em uma estrutura hierárquica;
- a última camada é a da sintaxe, que é o conjunto de regras que define a linguagem, por exemplo, a sintaxe XML.

Os componentes de mensagens, que formam a camada intermediária, funcionam como blocos de construção na montagem das mensagens e podem ser reutilizados sempre que exista a necessidade de apresentar informações equivalentes em diferentes mensagens padrão ISO 20022. Por exemplo, a identificação de instituições financeiras é necessária em quase todas as mensagens padrão ISO 20022 sob o escopo do domínio de Pagamentos. Nesse caso, foi desenvolvido um componente de mensagens padronizado para a identificação de instituição financeira que pode ser reutilizado em todas as mensagens que necessitam dessa informação.

A documentação detalhada é um dos preceitos do padrão ISO 20022. Uma das principais ferramentas é o repositório financeiro, composto pelo Dicionário de Dados e pelo Catálogo de Processos de Negócios. O Catálogo de Processos de Negócios trata da definição das mensagens, das áreas e das transações de negócio e também da estrutura de cada mensagem, e o Dicionário de Dados armazena os termos usados nas mensagens. Essa ferramenta auxilia as organizações solicitantes no desenvolvimento de mensagens, habilitando a consulta de qualquer termo e definição usada no âmbito do padrão internacional.



2.5 R3 CORDA

A plataforma Corda, desenvolvida pelo consórcio bancário R3, é uma plataforma de *blockchain* e *smart contract*, conhecida como Cordapps.

O Corda é um projeto de *blockchain* de código aberto, projetado para os negócios desde o início. Somente o Corda permite criar redes *blockchain* interoperáveis que transacionam em estrita privacidade. A tecnologia de contrato inteligente da Corda permite que as empresas realizem transações diretamente.

Como plataforma *blockchain*, permite que as partes transacionem diretamente um valor, gerenciem transações reais entre partes identificáveis com privacidade e segurança jurídica.

Como *smart contract*, permite que o Corda faça as transações usando contratos complexos e qualquer tipo de ativo.

Corda foi projetado a partir do zero com base nas necessidades dos membros do R3. Apesar de ainda usar a palavra “*blockchain*” extensivamente para ajudar a comercializar seu produto, o Corda não possui nenhuma cadeia de blocos. Mais do que qualquer outra plataforma de DLT, Corda afasta-se radicalmente da arquitetura de *blockchains* convencionais. Seu modelo de governança é explicitamente projetado para refletir os interesses comuns da diversificada base de usuários da plataforma.

O Corda é um DLT no qual várias entidades mantêm uma cópia do banco de dados subjacente e, naturalmente, têm permissão para contribuir. Todas as entidades que participam do armazenamento distribuído de dados formam uma rede chamada de “nós” ou “pares”. Devido ao armazenamento distribuído de dados, surge a dificuldade de garantir que todos os nós concordem com uma verdade comum, por exemplo, a correção de uma razão, já que as alterações feitas por um nó devem ser propagadas para todos os outros nós na rede. O resultado de chegar a uma verdade comum é chamado de consenso entre os nós, sem permissão e de permissão. Se a participação é sem permissão, qualquer pessoa pode participar da rede. Por outro lado, se a participação for permitida, os participantes são selecionados

- Integração com infraestrutura legada: a adoção corporativa será uma abordagem em fases, e o Corda foi criada para integrar e interoperar facilmente com os sistemas que administram seus negócios.
- Aplicativos para todos os setores: o Corda é a porta de entrada para uma rede vibrante de aplicativos *blockchain* para finanças e comércio, conhecidos como CorDapps, que resolvem problemas complexos do mundo real.

Os principais recursos de Corda são (BROWN *et al.*, 2016):

- registrar e gerenciar a evolução dos acordos financeiros e outros dados compartilhados entre duas ou mais partes identificáveis, de maneira que se baseie em construções legais existentes e seja compatível com a regulamentação existente e emergente;
- coreografar o fluxo de trabalho entre empresas sem um controlador central;
- apoiar o consenso entre empresas, no nível de acordos individuais, não um sistema global;
- apoiar a inclusão de nós de observadores, reguladores e supervisores;
- validar transações somente entre as partes;
- apoiar uma variedade de mecanismos de consenso;
- gravação de *links* explícitos entre documentos em linguagem humana e código de contrato inteligente;
- uso de ferramentas padrão do setor;
- restringir o acesso aos dados dentro de um contrato, liberando apenas aqueles explicitamente autorizados ou logicamente privilegiados;
- permissão que dá o controle de governança para R3 e para as organizações que participam da transação;
- o contrato inteligente vincula a lógica de negócios e os dados de negócios a uma prosa legal associada, a fim de garantir que os acordos financeiros na plataforma estejam firmemente firmados na lei e possam ser aplicados em caso de ambiguidade, incerteza ou disputa.

2.5.3 Corda Ledger

O Corda *Ledger* permite o gerenciamento e a sincronização de acordos comerciais entre várias partes.

2.5.4 Corda Network

Podemos pensar na rede Corda como um gráfico totalmente conectado, onde os nós no gráfico são nós Corda com potencial para se comunicar com outros nós.

Como não há rede de difusão ou fofoca global, devem-se especificar os destinatários das suas mensagens no Corda. Dessa forma, controla-se quem vê o quê e quando o vê.

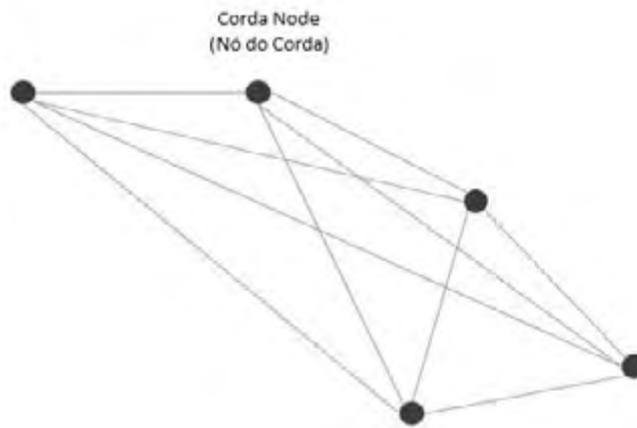


Figura 7 – A rede Corda é como um grafo

Os nós Corda se descobrem por meio de um serviço de Mapa de Rede. Pode-se pensar no serviço como uma lista telefônica, que publica uma lista de nós de mesmo nível, contendo metadados sobre quem eles são e quais serviços podem oferecer.

Outras plataformas de DLT usam redes globais de difusão e fococas para propagar dados. Corda usa mensagens ponto a ponto.

De uma perspectiva de dados, podemos pensar no Corda *Ledger* como um Diagrama de Venn.

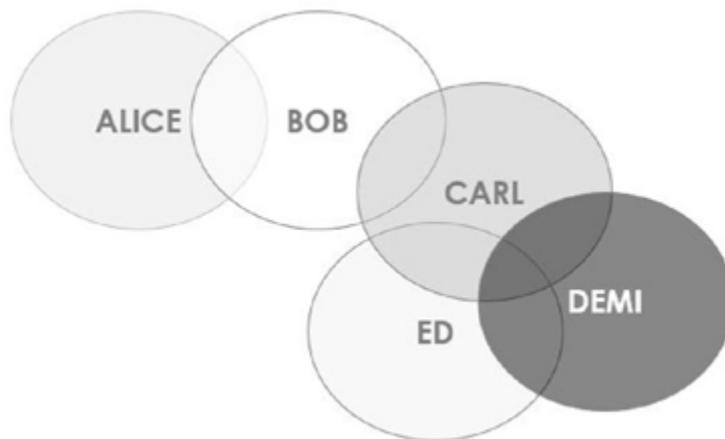


Figura 8 – Diagrama de Venn

No exemplo, o Diagrama de Venn consiste em cinco conjuntos.

- Alice;
- Prumo;
- Carl;
- Demi;
- Ed.

Cada conjunto contém fatos conhecidos. Onde os conjuntos se sobrepõem, fatos compartilhados são armazenados no livro-razão Corda.



Figura 9 – Fatos compartilhados

Notavelmente, nesse exemplo do Diagrama de Venn, Alice apenas compartilha fatos (e, portanto, é apenas consensual) com Bob – não com Carl, Demi ou Ed.

O Corda Ledger é uma construção subjetiva do ponto de vista de cada colega. Não há colegas que possam ver tudo. No exemplo do Diagrama de Venn, Alice e Demi verão um conjunto completamente diferente de fatos compartilhados.

Os círculos numerados no Diagrama de Venn abaixo representam fatos compartilhados no Corda Ledger.

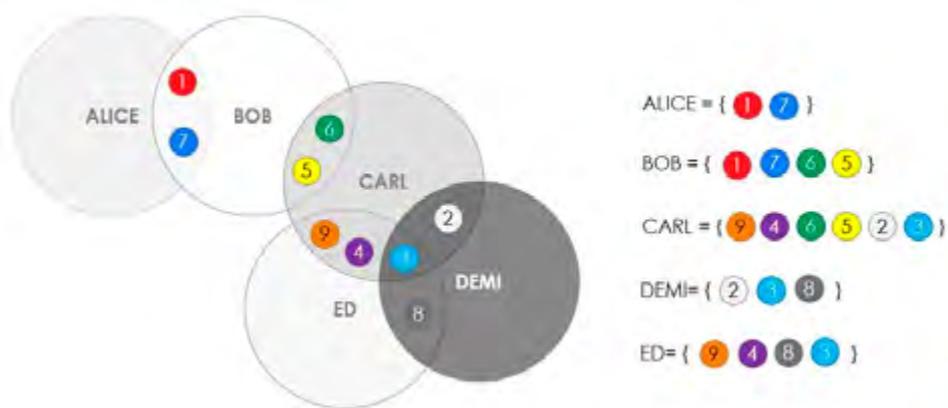


Figura 10 – Fatos compartilhados entre mais participantes

Como se pode ver, Bob e Alice estão em consenso sobre os fatos 1 e 7, enquanto Bob e Carl estão em consenso sobre os fatos 5 e 6, e assim por diante.

Em Corda, não existe uma razão central (também conhecido como geral) operando com a agência em nome de todos os nós da rede. Em vez disso, cada nó da rede mantém um cofre contendo todos os fatos conhecidos.



Pode-se pensar nesse cofre como um banco de dados ou uma tabela simples, conforme ilustrado a seguir.

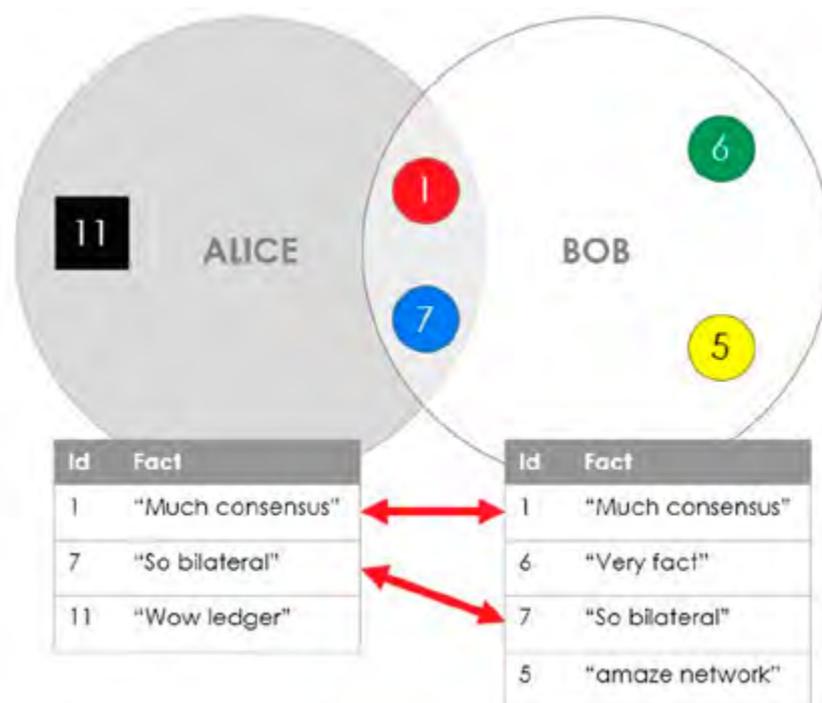


Figura 11 – Cofre Corda (Vault)

Onde há linhas compartilhadas entre nós – no exemplo, fatos/linhas 1 e 7 –, esses são fatos compartilhados.

Novamente, em Corda, nem todos os fatos contábeis precisam ser compartilhados entre pares. Por exemplo, o fato de Alice 11 em seu cofre (*Wow ledger*) não é compartilhado com Bob. O fato 11 é um fato unilateral.

Principais conclusões:

- a rede Corda é mais bem representada como um gráfico totalmente conectado contendo nós;
- não há rede de transmissão ou fofoca global em Corda;
- os nós Corda se descobrem por meio de um serviço de mapa de rede;
- cada nó do Corda inclui um cofre e todo cofre contém fatos;
- esses fatos podem ser compartilhados com outros nós na rede;
- o Corda *Ledger* é subjetivo da perspectiva de cada colega.

2.5.5 Estados (*states*)

Em Corda, os estados são objetos imutáveis, que representam fatos compartilhados, como um acordo ou contrato em um momento específico.

Como exemplo, Alice e Bob poderiam ter um fato compartilhado entre eles, que é uma IOU⁴.

Neste IOU, Alice é o devedor e Bob é o credor. No livro-razão de Alice e de Bob, aparece a mesma IOU.



Figura 12 – Estado do Corda

O modelo de estado pode ser usado para representar literalmente qualquer coisa. Pode ser usado para representar instrumentos financeiros ou acordos multilaterais, como troca de taxa de juros, empréstimos sindicalizados etc.

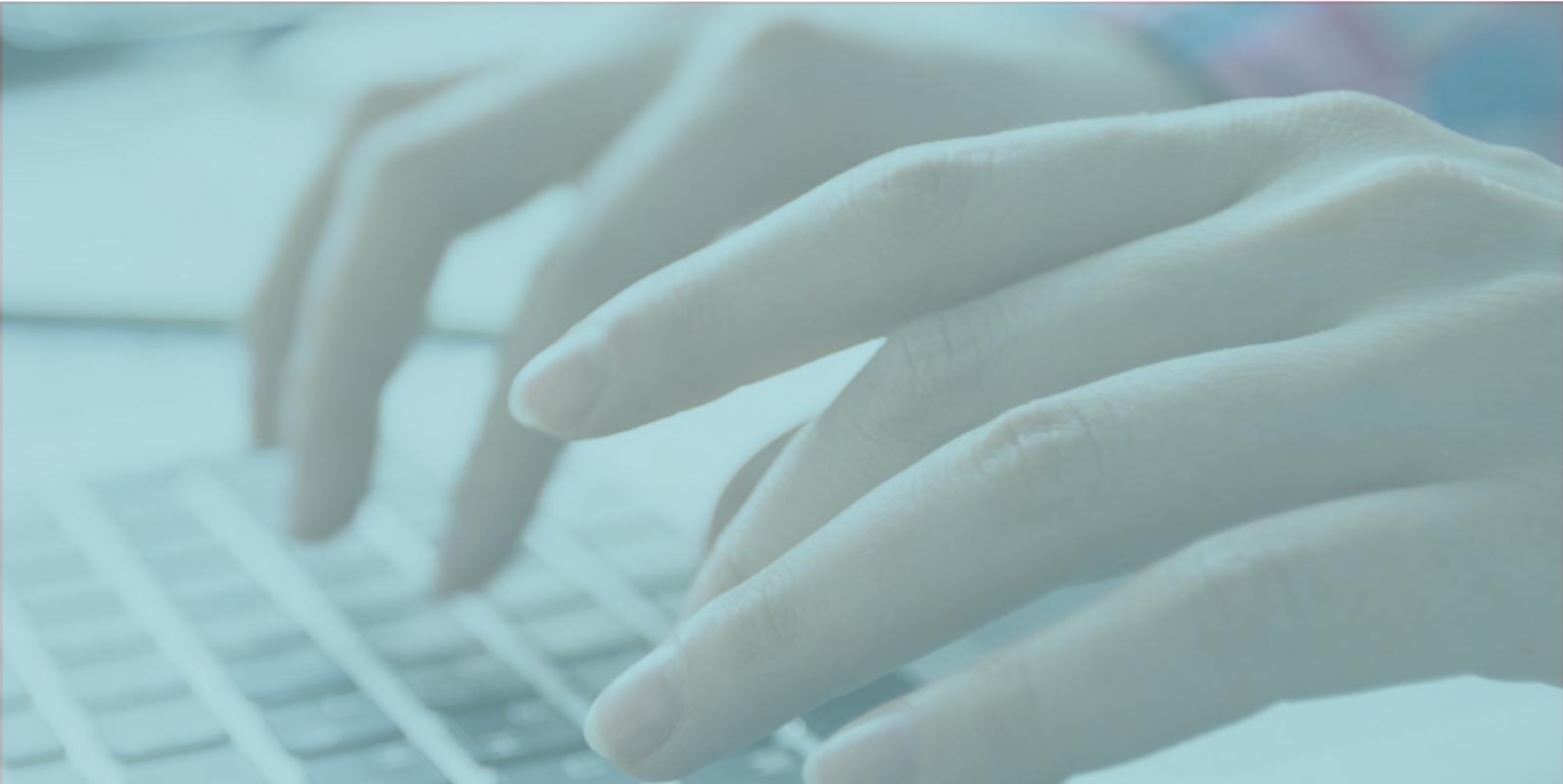
Diferentes tipos de estados podem conter atributos diferentes. Por exemplo, um título pode ter uma data de cupom, data de resgate, valor nominal etc.

Depois que um estado é criado como um tipo específico, ele não pode ser alterado para outro tipo. Por exemplo, se um estado for criado como um estado de vínculo, sempre será um estado de vínculo.

Os estados contêm dados sobre fatos compartilhados em um momento específico. Eles não podem ser alterados uma vez criados, pois são imutáveis.

No entanto, isso entra em conflito com a natureza de acordos ou fatos compartilhados, pois se espera que “evolam” ao longo do tempo em resposta a eventos do mundo real. No

.....
⁴ Abreviação de “I O (we) (yo) U” (Eu devo você). Cada IOU registrará o fato de que um nó deve a outro nó uma certa quantidade.



exemplo anterior, Alice pode pagar uma certa quantia de IOU, portanto esperamos que o fato compartilhado mude.

Estados antigos podem ser substituídos por novos. Um novo estado é criado copiando o antigo e atualizando suas propriedades, conforme necessário. Existe apenas uma versão mais recente a qualquer momento. Depois que um novo estado é criado, o antigo deve ser marcado como histórico.

Os estados históricos permanecem acessíveis e fornecem uma trilha de auditoria útil. Estados nunca são excluídos.

Uma sequência de estados representa o ciclo de vida de um acordo. É criado após uma ou mais transições de estado. As transições de estado ocorrem em ordem cronológica. Um exemplo de uma sequência de estados IOU é o seguinte: começamos por não ter acordo sobre o livro-razão. Alice empresta R\$10,00 a Bob em 1º de fevereiro de 2017, para que um fato compartilhado seja criado no razão que representa esse acordo bilateral. Em 24 de fevereiro de 2017, Alice paga a Bob R\$5,00 para que um novo objeto de estado seja criado com o fato atualizado do valor pago por Alice. Em 2 de março de 2017, Alice incorre em juros de R\$1,00, pois ainda precisa liquidar o IOU na data de vencimento, em 1º de março de 2017. Finalmente, ela paga a Bob R\$6,00 (incluindo principal e juros) para liquidar o IOU no mesmo dia. Como Alice pagou o IOU integralmente, o contrato expirou e não há mais motivo para que o IOU exista no livro-razão.

O cabeçalho (*header*) da sequência reflete o estado atual do fato compartilhado. O cabeçalho está sempre atualizado, enquanto todos os estados anteriores são históricos.

O estado atual do livro-razão é composto por todos os cabeçalhos de todas as sequências de estados. Pode-se consultar o cofre para todas os cabeçalhos de cada sequência de estados ou por tipo (por exemplo, todos os estados de vínculo).



Principais conclusões:

- os estados são objetos imutáveis que representam fatos compartilhados, como um acordo ou contrato em um momento específico;
- o ciclo de vida de um fato ou acordo compartilhado ao longo do tempo é representado por uma sequência de estados;
- o livro-razão, do ponto de vista de cada ponto, consiste em todas as cabeças de sequência de estados rastreadas no cofre.

2.6 Open banking

O *open banking*, na ótica do Banco Central do Brasil:⁵

[...] compartilhamento de dados, produtos e serviços pelas instituições financeiras e demais instituições autorizadas, a critério de seus clientes, em se tratando de dados a eles relacionados, por meio de abertura e integração de plataformas e infraestruturas

A Figura 13 mostra em detalhes o que é *open banking*.

⁵ Comunicado 33.455, de 24 de abril de 2019.

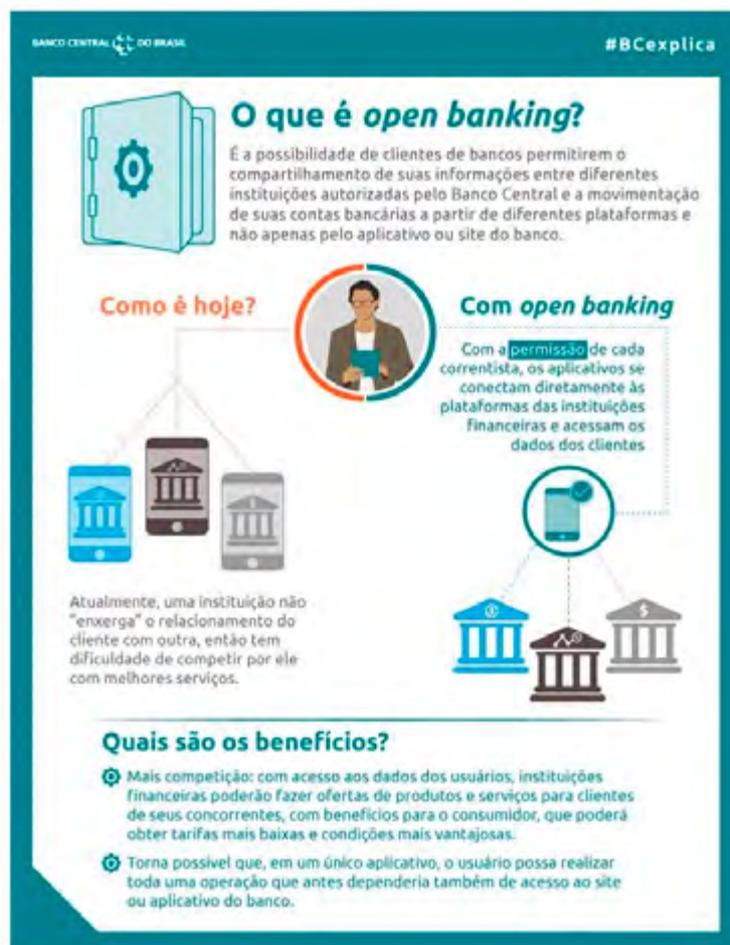


Figura 13 – O que é open banking. Fonte: Banco Central do Brasil

2.7 Identidade digital (FinId)

Hoje, em instituições financeiras, uma transação que exige identificação – seja para um pagamento, um empréstimo ou outra operação – significa coletar comprovante físico por meio de um canal digital (como a fotografia de uma carteira de motorista ou carteira de identidade) ou depender de processos de reconhecimento do cliente através de cópias autenticadas de documentos de identificação, endereço, local de trabalho pelo cliente. O mesmo acontece para o comércio, entretenimento, educação, serviços do governo e todas as áreas nas quais é necessário se identificar para ter a permissão de acesso ou de uso de algum serviço.

De maneira resumida, identidade digital é a possibilidade de um usuário/cliente, ter um cadastro em uma entidade, onde ele prova sua identidade através da verificação de documentos somente uma vez. Em todas as outras entidades nas quais esse usuário queira se cadastrar, basta informar sua identidade (*alias*) e, de forma automática, sua identidade é validada na entidade que possa fazer a sua autenticação.

2.8 Lei Geral de Proteção de Dados Pessoais

LGPD é a sigla adotada para designar a Lei Geral de Proteção de Dados Pessoais (Lei 13.709, de 14 de agosto de 2018). Seu principal objetivo é garantir transparência no uso dos dados das pessoas físicas em quaisquer meios.

A LGPD usa os direitos fundamentais de liberdade e de privacidade como norte para estabelecer regras a respeito da coleta e armazenamento, de dados pessoais e seu compartilhamento. A intenção é proporcionar proteção dos dados das pessoas físicas.

3 Escopo do protótipo

A implementação de uma camada de aplicação *blockchain* em DLT Corda que viabiliza um sistema de liquidação bruto em tempo real de todos os participantes para pagamentos instantâneos.

Alguns casos de uso para o *switch* de pagamentos *BluPay* a serem considerados para a fase de incubação do LIFT estão descritos na seção 4, Visão Geral, e foram descritos a partir da implementação de uma aplicação móvel como prova de conceito que realiza pagamentos e recebimentos. Outros cenários e ações são contemplados dentro do escopo de segurança, comunicação e conectividade para o *switch BluPay* ao longo de seu desenvolvimento conforme o documento de Especificações Técnicas e de Negócio⁶ do Banco Central.

3.1 Segurança

Atendendo aos requisitos de segurança, o *switch* de pagamentos *BluPay* tem por objetivo prover disponibilidade, integridade, confidencialidade e autenticidade implementados através da tecnologia DLT Corda.

3.2 Comunicação

Uso do catálogo de mensagens no padrão ISO 20022 entre o SPI e o participante cuja discussão do escopo das mensagens trocadas está em progresso para validação dos campos de mensageria e suporte de requisitos não funcionais tais como:

- volume de mensagens;
- tempo de resposta;
- disponibilidade.

⁶ https://www.bcb.gov.br/content/estabilidadefinanceira/forumpireunioes/Especificaca%C3%A7%C3%B5esPI_vers%C3%A3o3.o.pdf (versão 3.0 acessada disponível em 20/set/2019)

3.3 Conectividade

Padrões tecnológicos de conectividade ainda em definição pelo Banco Central sobre a interface de comunicação a ser usada, i.e., via REST API⁷ ou implementação de filas no estilo MQ.⁸ O *BluPay* se conectará ao SPI⁹ por meio da já existente RSN.¹⁰ O serviço de tradução de mensagens ISO 20022 a ser implementado no *switch BluPay* se faz necessário para conectividade do SPI e seus participantes diretos e indiretos ainda é alvo de estudo para evolução e progresso.

4 Visão geral

O *switch* de pagamentos instantâneos *BluPay* integrará as principais oportunidades geradas pelas mudanças previstas no ecossistema financeiro com os comunicados sobre pagamento instantâneo.

Com o objetivo de validação de hipóteses, uma prova de conceito de um aplicativo bancário genérico foi implementada para simulação de um sistema de pagamentos instantâneos. As principais funcionalidades são pagamentos via QR Code,¹¹ pagamentos de boleto, requisição de cobranças por CPFs e envio de cobranças por WhatsApp.

O protótipo foi desenvolvido como uma ferramenta que exemplifica a partes interessadas as possibilidades do sistema de pagamentos instantâneos, bem como a aplicação das novas regras do BCB para aplicações em ambiente real.

Cabe aqui ressaltar a existente RSN,¹² com a capacidade de integrar essa plataforma como um novo ponto dentro do ecossistema, disponibilizando para os agentes do sistema financeiro a capacidade de realizar as suas transações, utilizando o barramento oferecido pela solução.

4.1 Casos de uso usando o *switch* de pagamentos instantâneos *BluPay*

Independentemente do meio como uma cobrança para pagamento é gerada, seja por boletos ou QR Code por exemplo, os casos de uso nesta seção têm o *switch* de pagamentos instantâneos *BluPay* como intermediário para todas as transações bancárias.

⁷ REST, acrônimo do inglês para *Representational State Transfer*, e API, do inglês *Application Programming Interface*, trata-se de uma comunicação eficiente entre aplicações de maneira a utilizar as características do protocolo HTTP.

⁸ MQ, acrônimo para Message Queue, padrão para implementação de um sistema de mensageria e enfileiramento de mensagens.

⁹ Sistema de Pagamentos Instantâneos é a infraestrutura centralizada e única de liquidação bruta e em tempo real do ecossistema de pagamentos instantâneos brasileiro

¹⁰ O Banco Central elegeu a Rede do Sistema Financeiro Nacional (RSFN) para suportar o tráfego de comunicação dentro do ecossistema de pagamentos instantâneos brasileiro.

¹¹ Do inglês *Quick Response Code*, é um código de barras bidimensional que pode ser convertido em outras informações por exemplo um texto, um número de telefone, um e-mail etc., sendo facilmente escaneado através da câmera de qualquer smartphone.

¹² RSN – Rede Blockchain do Sistema Financeiro Nacional

4.1.1 Identidade Digital (FinId)

O usuário cadastra seus dados no *BluPay* usando o aplicativo FinId (Figura 14) e informa para quais instituições financeiras ele permite o compartilhamento de suas informações e qual instituição financeira é a primária.

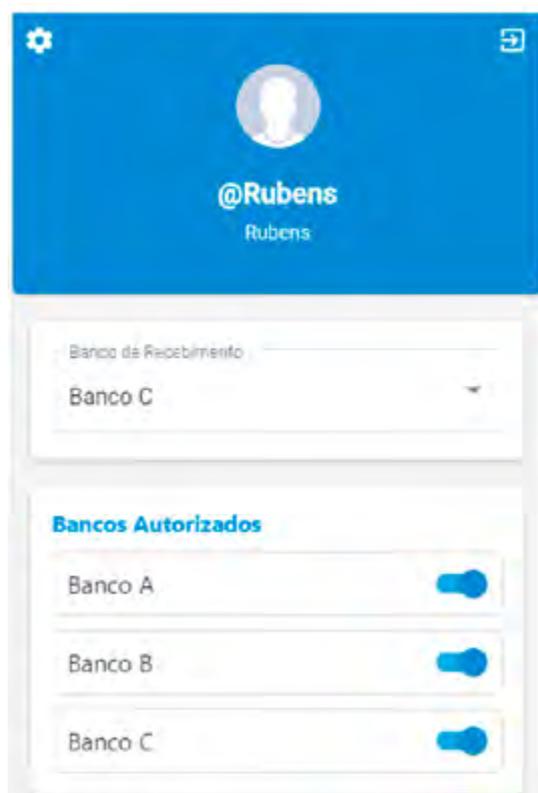
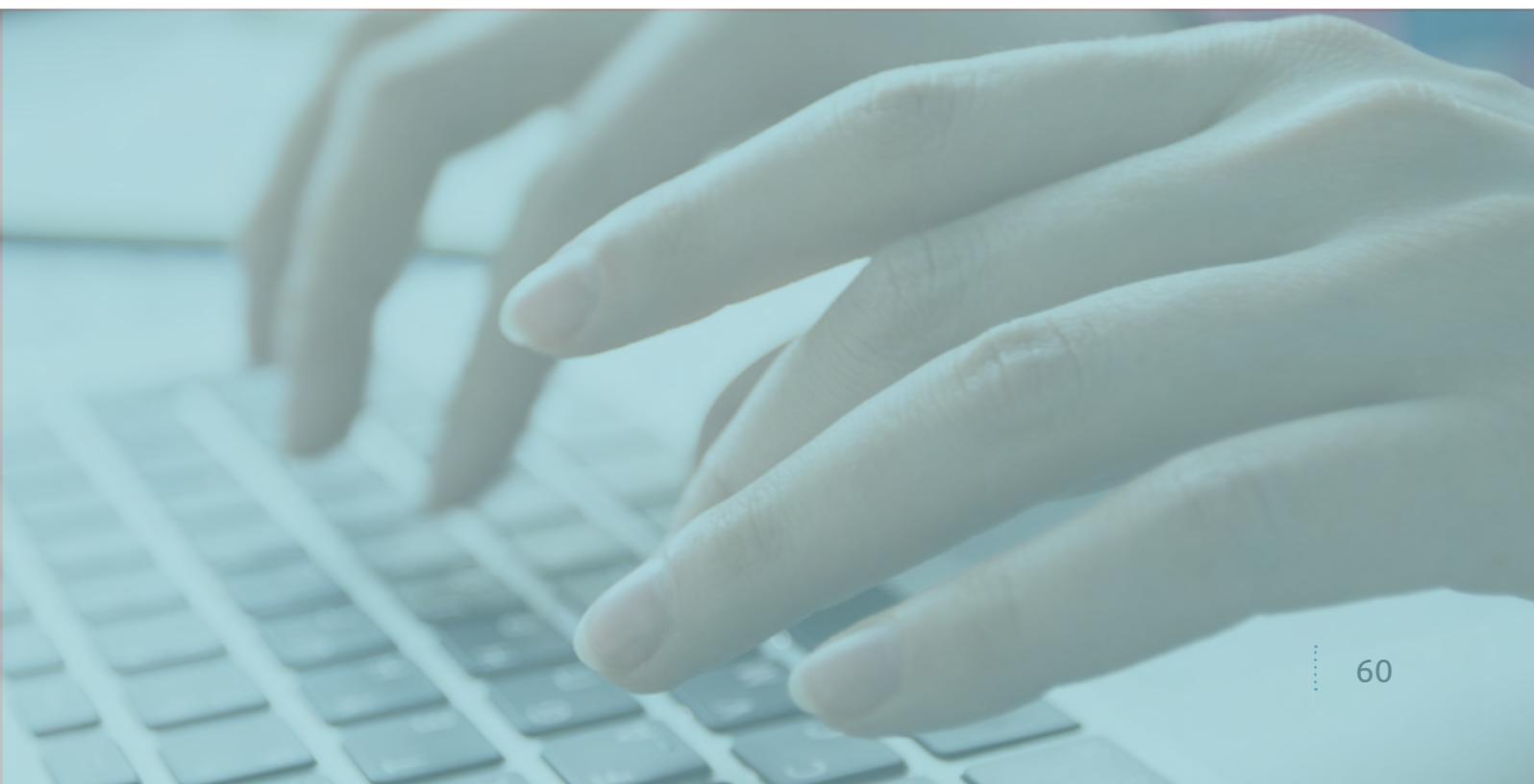


Figura 14 – Tela do aplicativo FinId



4.1.2 Pagamento instantâneo

Foi desenvolvido um aplicativo (Figura 15) que emula um aplicativo de uma instituição financeira já utilizando os conceitos de *open banking*, ou seja, é um aplicativo único que se conecta a qualquer instituição financeira. Nesse aplicativo, o usuário visualiza seu saldo e realiza operações de pagamentos e recebimentos por meio de QRCode ou apenas informando o *alias* do usuário. Nesse momento, estamos usando os conceitos de Identidade Digital, identificando o usuário da instituição financeira apenas pelo *alias*. A instituição financeira na qual o usuário receberá valores pagos por outro usuário está configurada como instituição financeira primária (Banco de Recebimento) no aplicativo FinId (Figura 14).

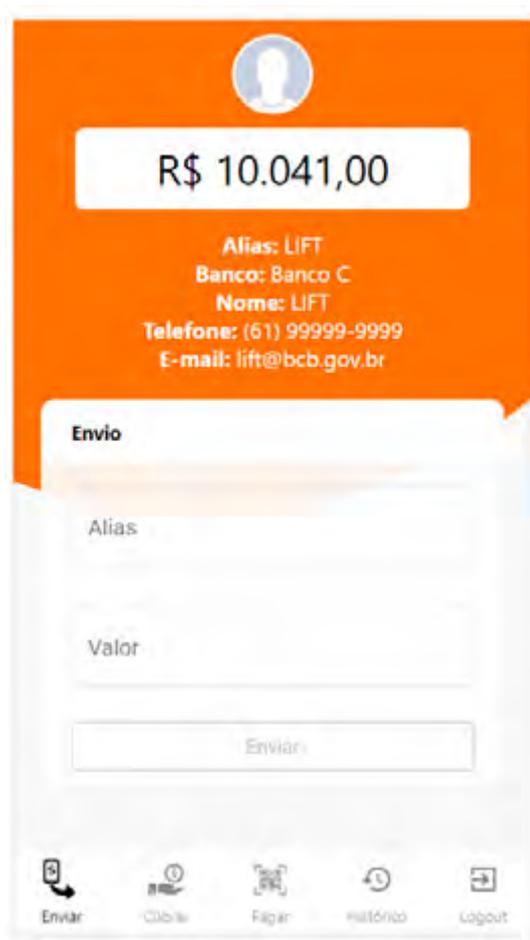


Figura 15 – Aplicativo – Instituição financeira

4.1.3 Pagamento instantâneo utilizando QR Code

O usuário receptor define o valor a ser recebido em seu dispositivo, seleciona o botão para gerar o QR Code e disponibiliza para o Pagador efetuar a leitura do código (Figura 15 e Figura 16).

O usuário pagador aciona em seu aplicativo bancário a funcionalidade de pagamento instantâneo. Ao acionar a função, a câmera é acionada, e o dispositivo tenta identificar o QR Code gerado pelo receptor.

Uma vez realizada a leitura, o Pagador confirma as informações fornecidas pelo Recebedor e autoriza o pagamento.

Ao ser confirmado o pagamento, as regras de validação apontadas no Comunicado 32.927, de 2018, aplicam-se e, em até 20 segundos, o recurso deverá estar disponível na conta do Recebedor.



Figura 16 – Tela para gerar QR Code para cobrança



Figura 17 – Tela com QR Code para cobrança gerado

4.1.4 Pagamento instantâneo utilizando *alias*

O usuário pagador define o *alias* e o valor a ser enviado em seu dispositivo, e pressiona o botão Enviar.

Ao ser confirmado o pagamento, as regras de validação apontadas no Comunicado 32.927, de 2018, aplicam-se e, em até 20 segundos, o recurso deverá estar disponível na conta do Recebedor.

5 Características inovadoras

O projeto se propõe a inovar o sistema de pagamentos instantâneos brasileiro por meio da oferta direta de serviços às instituições financeiras usando tecnologia *blockchain* e a promover o acesso a STR aos participantes indiretos e Provedores de Serviços de Iniciação de Pagamentos.

Na Figura 14, temos um exemplo das transações e comunicação com o *BluPay* quando uma transferência de valores é realizada entre duas IFs.

As seguintes operações são realizadas:

1. a IF Banco A envia uma solicitação de transferência em seu nó Corda (TX3);
2. o próprio nó cria o bloqueio do saldo e cria um estado de transferência compartilhado com o banco de destino (TX4);
3. o estado de transferência é consumido, e são criados os estados de requisição de saque para o nó corda de origem e requisição de depósito para o nó corda de destino (TX5);
4. o nó Corda de destino consome a requisição de depósito e seu próprio saldo, criando um novo estado de saldo atualizado (TX6);
5. o nó Corda de origem consome o estado de requisição de saque e o estado de bloqueio dessa transação, não criando nenhum estado (TX7).

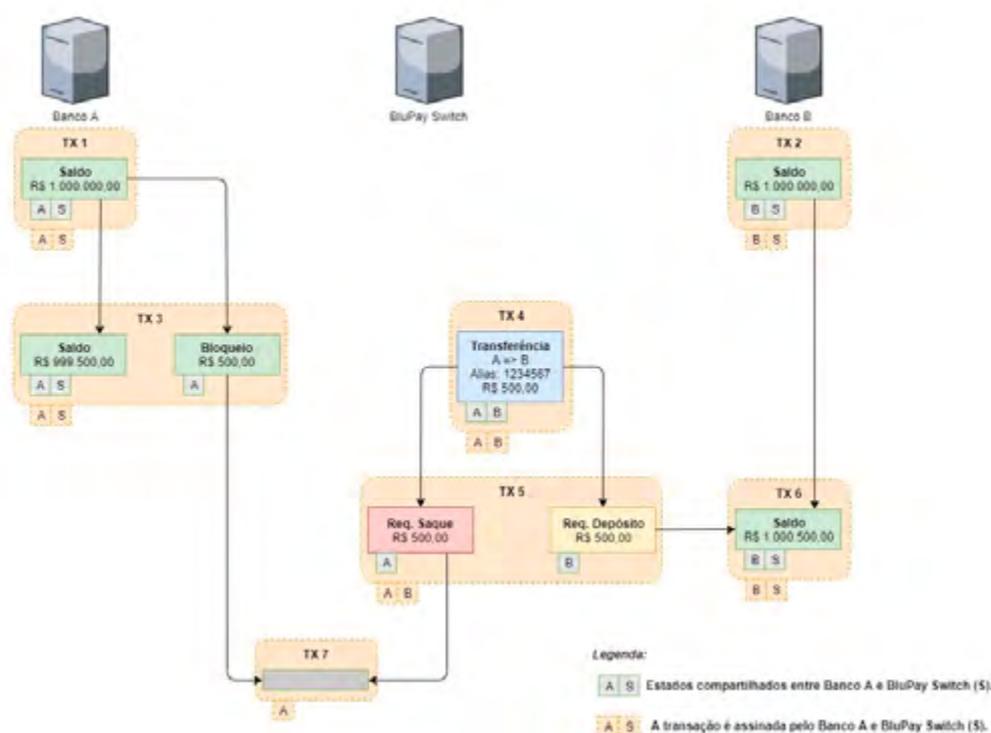


Figura 19 – Transferência de valores entre duas instituições financeiras

Por meio dos conceitos de *open banking* e FinId implementados em Corda pelo *BluPay*, clientes bancários podem visualizar em um único aplicativo o extrato consolidado de todas as suas contas bancárias e investimentos. Também será possível, por esse mesmo aplicativo, transferir recursos ou realizar pagamentos sem a necessidade de acessar diretamente o site ou aplicativo do banco. De maneira análoga, quaisquer prestadores de serviços podem utilizar essa aplicação para pagamentos de contas diversas (contas de consumo, impostos, boletos). Como exemplo temos: o serviço de televisão a cabo.

Identidade digital ou FinId, no contexto deste estudo para o LIFT, consiste no uso de um ciclo para criação de uma identidade digital em três fases: registro do usuário (simulando o cadastro e

a validação das informações do usuário); emissão de uma credencial (representada aqui por um *alias*); e a autenticação do usuário no uso dos sistemas bancários. Ainda, quando da transferência de valores para o correntista de uma instituição financeira, usa-se como entrada somente o *alias* do correntista recebedor. O sistema se encarregará para descobrir quem é esse usuário e qual instituição financeira foi configurada como primária para recebimento de valores.

O registro do usuário e sua posterior autenticação, ou seja, todos os dados dos usuários, estão implementadas em R3 Corda (Figura 16). É importante ressaltar que essa aplicação foi desenvolvida aderente aos conceitos de *open banking* e LGPD.

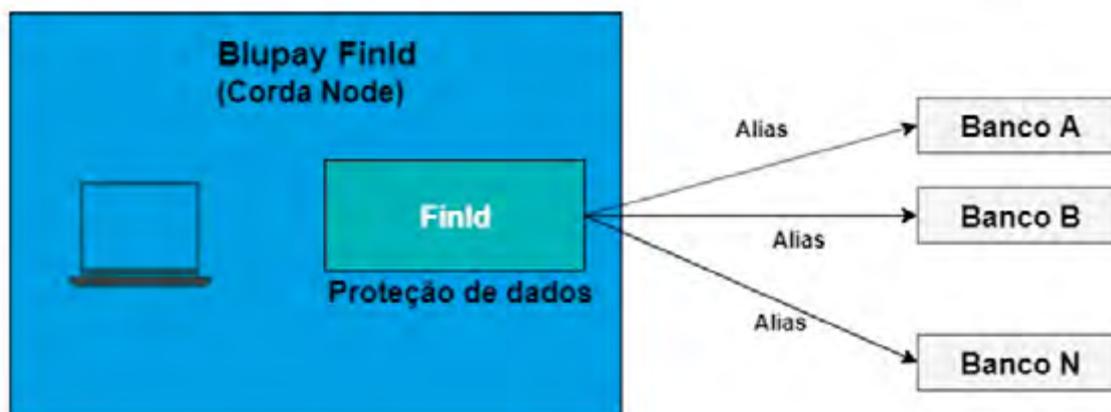


Figura 20 – FinId (identidade digital)

.....6 Contribuição para o SFN

A implementação do *switch* de pagamentos instantâneos *BluPay* faz parte de toda uma nova arquitetura para pagamentos e uma oportunidade para que os brasileiros melhorem sua experiência ao realizar movimentações financeiras entre instituições bancárias diferentes. Pode-se exemplificar que, tornando os pagamentos instantâneos desacoplados do atual horário comercial bancário para transações, isso impulsiona uma movimentação financeira diária maior de recursos que, por consequência, tem impactos diretos na economia do país, tornando o dinheiro mais barato e fomentando a economia.

O uso de uma tecnologia moderna e segura como o *blockchain*, que integra a arquitetura do *switch* de pagamentos instantâneos *BluPay*, torna o sistema financeiro de um país mais confiável e livre de antigas falhas como a ausência de rastreabilidade dos recursos financeiros transacionados entre bancos o que norteia crimes como a lavagem de dinheiro.

De modo geral, os benefícios para implementação de um novo paradigma para pagamentos instantâneos se estendem de modo ativo por todo SFN, atingindo todas as instituições bancárias, empresas públicas e privadas e a própria população.

Some-se aos itens anteriores a capacidade de otimização das requisições em ambientes críticos como a Camada de Liquidação e a STR. A *BluPay* contribui para que o ecossistema seja mais otimizado e com isso possuir mais capacidade de atender ao SFN.

.....7 Restrições

Por se tratar de um tema em constante progresso, por meio de adendos e atualizações ao Comunicado 32.927, de 2018, do Banco Central, não se identificam no momento, restrições que impeçam o desenvolvimento do *switch* de pagamentos instantâneos *BluPay*.

.....8 Conclusão

Os pagamentos instantâneos já são uma realidade na Ásia, mais especificamente na China e Índia, países estes com as maiores populações mundiais. O Brasil será um dos pioneiros nesse novo segmento, tornando-o postulante a modelo de referência em pagamentos instantâneos na América.

Como já explanado ao longo deste documento, o *switch* de pagamentos instantâneos *BluPay* viabiliza as oportunidades de modernização do ecossistema financeiro brasileiro segundo os Comunicados 32.927, de 2018, e 33.455, de 2019.

Como qualquer solução implementada computacionalmente, o *BluPay* resolve problemas existentes da vida real para pessoas físicas e jurídicas, e todo sistema bancário, tornando a liquidez imediata de recursos financeiros como um ativo que traz impactos diretos em todos os pilares da economia nacional.

O protótipo apresentado neste documento está em progresso e demonstra as funcionalidades para pagamentos por meio de uma aplicação *frontend*¹³ com interface visual ao usuário. É importante ressaltar que o *core*¹⁴ do *BluPay* a ser integrado dentro do ecossistema financeiro é executado em modo não visual, i.e., por meio de programas computacionais executados dentro de servidores em modo *backend*.¹⁵

.....
¹³ Representa a parte de um programa computacional implementada que é visual e apresentada ao usuário final na forma de uma aplicação *Web* ou móvel.

¹⁴ Parte principal de um sistema computacional que implementa as regras de negócio de uma aplicação.

¹⁵ Representa a parte de um programa computacional implementada que não é visual ao usuário final e que são executadas “por trás” das aplicações ditas *frontend*.

Referências

AMARO, George. **Criptografia Simétrica e criptografia de chaves públicas: vantagens e desvantagens. Revista Negócios e Tecnologia da Informação.** On Line. Disponível em: <http://publica.fesppr.br/index.php/rnti/issue/download/4/33>. Acessado em: out/2019.

ANTONOPOULOS, Andreas M. **Mastering bitcoin: unlocking digital cryptocurrencies.** Sebastopol: O'Reilly, 2014. 282 p.

BROWN, Richard Gendal et al. **Corda: an introduction.** R3 CEV, August, v. 1, p. 15, 2016.

FERRER, Eduardo Castelló. The blockchain: a new framework for robotic swarm systems. In: **Proceedings of the future technologies conference.** Springer, Cham, 2018. p. 1037-1058.

LAZAROVICH, A. (2015). **Invisible ink: blockchain for data privacy. PhD thesis, Massachusetts Institute of Technology.** On Line. Disponível em: <https://dspace.mit.edu/handle/1721.1/98626>.

LEWENBERG, Yoad; SOMPOLINSKY, Yonatan; ZOHAR, Aviv. Inclusive block chain protocols. In: **International Conference on Financial Cryptography and Data Security.** Springer, Berlin, Heidelberg, 2015. p. 528-547.

NAKAMOTO, S. (2008). **Bitcoin: a peer-to-peer electronic cash system.** On Line. Disponível em <https://bitcoin.org/bitcoin.pdf>.

PRADO, J. **O que é blockchain? Tecnoblog, 2017.** Disponível em: <https://tecnoblog.net/227293/como-funciona-blockchain-bitcoin/>. Acessado em: out/2019.

