LIFT *papers*

Revista do Laboratório
de Inovações Financeiras
e Tecnológicas

#4 | ABRIL 2022

Fenasbac

BANCO CENTRAL
DO BRASIL

LIFT Papers

Revista do Laboratório de Inovações Financeiras e Tecnológicas

Número 4 | Abril 2022

Ficha catalográfica elaborada pela Biblioteca do Banco Central do Brasil

LIFT Papers / Banco Central do Brasil. N. 4, (abril 2022). Brasília: Banco Central do Brasil, 2020.

Semestral
Disponível em:
https://revista.liftlab.com.br
ISSN 2675-2859

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

CDU 336.7:004.738.5

Simplificando Pagamentos Digitais: prevenção à lavagem de dinheiro e antifraude

Luiz Guilherme Aragão Madeira Coimbra[1]
Fabio Hideki Ikeno[2]
Eric Alexandre Ikeda[3]
Gabriel Magalhães Rodrigues[4]

O projeto Simplificando Pagamentos Digitais é um *hub* que integra pagamentos digitais diretamente no sistema de caixa de lojas físicas e dos canais digitais do varejo. Diante do crescimento do volume de transações Pix e das necessidades de segurança desse ambiente, especialmente para a prevenção à lavagem de dinheiro por meio do pagamento da fatura de cartão de crédito, a Shipay propõe, no projeto, o emprego de diferentes técnicas de aprendizado de máquina, além de algoritmos estatísticos e de grafo, como métodos preventivos. A adoção pioneira dessas técnicas no Brasil, combinadas com os serviços do Microsoft Azure, parceiro tecnológico do projeto, tem o potencial de detectar transações suspeitas e agir, em tempo real, de maneira mais ágil e eficiente do que os métodos tradicionais. A contribuição deste projeto se apoia em três pilares: 1. Inclusão por meio do incremento de adesão ao Pix, derivado de uma maior percepção pública de valor quanto à segurança; 2. Competitividade em função da efetividade da prevenção à lavagem de dinheiro, menos custos e mais agilidade na análise de dados transacionais; e 3. Transparência em virtude da inteligência envolvida tanto na análise de dados quanto no nível de segurança do pagamento instantâneo.

Palavras-chave: meios digitais de pagamento; Pix; prevenção à lavagem de dinheiro; algoritmos; aprendizado de máquina; estatísticos; grafo.

1 Co-CEO & founder da Shipay, luiz.coimbra@shipay.com.br
2 CTO & founder da Shipay, fabio.ikeno@shipay.com.br
3 eric.ikeda@shipay.com.br
4 gabriel.rodrigues@shipay.com.br

Introdução

O presente relatório descreve a proposta do projeto em aplicar diferentes técnicas de aprendizado de máquina, bem como algoritmos estatísticos e de grafo, em conjunto com serviços gerenciados na nuvem do Microsoft Azure, a fim de oferecer uma camada adicional de inteligência, análise e segurança no ambiente Pix. A ênfase da proposta recai sobre a prevenção à lavagem de dinheiro (PLD) por meio de uma ferramenta que, além de detectar casos potenciais, evolua para a rápida interrupção da transação.

O documento está estruturado da seguinte forma. Após esta introdução, serão apresentados os objetivos a partir de breve contextualização, levantamento do problema e da solução que contribui para mitigá-lo. Em seguida, a fundamentação teórica apresenta os principais eixos sobre os quais o projeto é construído, são eles: o Pix como um dos meios de pagamento digital instantâneo; as transações de lavagem de dinheiro (LD) e os mecanismos de prevenção; o aprendizado de máquina (*Machine Learning* – ML) aplicada à PLD no ambiente Pix; os grafos e sua utilização; a Lei de Benford na detecção de fraude; e os serviços Microsoft destinados à prevenção de fraude diante das oportunidades e dos desafios do Sistema Financeiro Aberto.

A seção referente à visão geral oferece um panorama da proposta para aplicação da tecnologia disponibilizada pelo parceiro tecnológico como camada de segurança do ambiente Pix com o fim de prevenir transações de LD. Após a visão geral, são apresentadas as funcionalidades da proposta seguidas de uma seção referente ao escopo do protótipo.

Posteriormente, o relatório lista as características inovadoras da proposta, bem como as contribuições para o Sistema Financeiro Nacional que delas decorrem. A conclusão encerra o documento, conectando o percurso que se estende do problema identificado até aos potenciais ganhos que a solução pretende trazer para o ambiente Pix.

1 Objetivos

Em sua pesquisa sobre as mudanças nos hábitos de consumo de serviços financeiros em função das novas tecnologias, a *International Data Corporation* constatou que a utilização de meios digitais de pagamento é a preferência de seis em cada dez brasileiros das classes A, B e C (VALENTE, 2019). Embora a taxa de crescimento do volume de pagamentos com cartões tenha sofrido redução devido à pandemia, os pagamentos digitais cresceram aceleradamente (TAYAR; FONTES; CRADDOCK; MURATORE, 2021). Em 2020, no Brasil, houve aumento de 32% nas transações não presenciais (TAYAR; FONTES; CRADDOCK; MURATORE, 2021) e, segundo a Associação Brasileira das Empresas de Cartões de Crédito e Serviços, de 469,6% nos pagamentos por aproximação (ABECS, 2021).

Como meio de pagamento digital instantâneo, o Pix obteve, desde o seu lançamento oficial, em outubro de 2020, uma taxa média de crescimento mensal de 18% no número de usuários (FEBRABAN, 2021). Dados do Banco Central do Brasil (2021a) apontam 313 milhões de chaves cadastradas no Diretório de Identificadores de Contas Transacionais (DICT) em agosto de 2021. Esse crescimento, tanto em adesão quanto em número de transações, pode ser explicado pela facilidade, praticidade e agilidade do uso do Pix nos pagamentos e operações bancárias.

Entretanto, não obstante tais benefícios, o pagamento instantâneo traz consigo riscos relacionados à fraude e a crimes financeiros. Os resultados da pesquisa realizada pela

TransUnion mostram que as fraudes envolvendo os serviços financeiros no Brasil cresceram 457% durante a pandemia (INFRA NEWS TELECOM, 2021).

Ao fazer a transação com Pix, todas as informações referentes às chaves utilizadas de quem paga e recebe ficam armazenadas no Diretório de Identificadores de Contas Transacionais (DICT). No caso de suspeita de fraude ou lavagem de dinheiro, essas informações podem ser acessadas. Porém, a transação instantânea não é impedida. Embora existam mecanismos de segurança estabelecidos pelo Banco Central (BC) – que serão explorados mais adiante – não há um método preventivo para interromper a transação. As medidas tomadas *a posteriori* servem para reparar o evento fraudulento, mas não para preveni-lo. Contudo, é importante destacar que o BC está atento a essas limitações e procura, por meio de ajustes evolutivos na regulamentação, atuar na melhoria dos mecanismos de segurança.

Diante desse cenário, o foco do presente projeto recai sobre o pagamento de fatura de cartão de crédito. Os provedores de cartão de crédito não são, necessariamente, bancos e, além disso, tanto o processo quanto a infraestrutura de analistas de prevenção de lavagem de dinheiro não estão adaptados ao Pix. Na verdade, pelo fato de o Pix ser algo novo, visto que passou a vigorar no dia 16 de novembro de 2020, são necessários avanços e ajustes nas áreas de PLD.

O uso de algoritmos estatísticos e de grafo e, posteriormente, do ML pretende mitigar esse problema por meio da detecção de anomalias nas transações Pix para pagamentos de faturas de cartão de crédito. O emprego das diferentes técnicas propostas permite que os analistas de PLD mapeiem e, consequentemente, mitiguem os casos de lavagem de dinheiro. A realização desse mapeamento tem como objetivos específicos:

1. O estabelecimento de um método preventivo que identifique rapidamente transações suspeitas no ecossistema Pix.
2. A garantia de uma camada de segurança de PLD, diferente das camadas já existentes no Sistema de Pagamentos Instantâneos (SPI), que favoreça a percepção pública de valor e adesão à ferramenta Pix.

2 Fundamentação Teórica

2.1 Pix: características e medidas de segurança

De acordo com a análise feita pelo Deutsche Bank (2020) sobre o futuro dos pagamentos, a adoção de meios digitais, especialmente após a crise financeira global de 2008, constitui uma jornada ascendente em direção à desmaterialização dos pagamentos. A crise mostrou que era preciso encontrar um caminho diante do cenário de baixa liquidez no sistema financeiro, dificuldades de obtenção de crédito e redução da confiança no sistema bancário centralizado.

Essa crescente tendência de digitalização do pagamento fez parte das motivações do BC em busca de inovação com a criação do Pix, nas palavras de Silva e Cruz (2020):

> Com relação aos planejamentos incessantes acerca da virtualização do mercado financeiro, o Banco Central do Brasil objetiva implantar novos instrumentos revolucionários de pagamentos eletrônicos e, com base nesta iniciativa, desenvolveu o Pix, instrumento de pagamento eletrônico que consiste basicamente na transferência de valores monetários em tempo real e de forma virtual. (SILVA; CRUZ, 2020, p. 197)

O pagamento instantâneo implica, portanto, "a transferência eletrônica de fundos, na qual a transmissão da ordem de pagamento e a disponibilidade de fundos para o usuário recebedor ocorrem em tempo real" com um serviço ininterrupto (BCB, 2021a).

O Pix contém chaves de transação que podem ser: CPF, CNPJ, e-mail, número do celular ou, utilizadas na mensageria DICT, para não haver associação com dados pessoais, a chave pode ser criada com letras e números aleatórios. A chave Pix permite que o SPI identifique os dados da conta transacional que o usuário mantém na instituição de sua escolha e realize, imediatamente, a transação. A conta transacional pode ser constituída pela conta de depósito, de poupança ou de pagamento pré-paga.

O SPI é a infraestrutura centralizada na qual são liquidadas as transferências de fundos comandadas pelos usuários do Pix e pelas próprias instituições perante o Banco Central. A conta mantida no Banco Central por um participante direto do SPI é denominada conta de pagamentos instantâneos (PI). As transferências dos valores monetários ocorrem somente entre as contas daqueles que participam do sistema.

O DICT configura outro conceito relevante para compreensão do Pix. Ele permite a busca de detalhes das contas transacionais com chaves de endereçamento mais convenientes para quem efetua um pagamento. Ao armazenar as informações das chaves Pix, o DICT se caracteriza como um banco de dados. Segundo o Banco Central (2021b), "as informações retornadas pelo DICT permitem que o pagador confirme a identidade do recebedor, proporcionando uma experiência mais fácil e segura".

Embora os mecanismos de segurança do Pix representem uma garantia importante para a sua utilização, cumpre destacar que o DICT fornece apenas o nome, a chave e a instituição financeira do pagador e recebedor para fins de confirmação. Dessa forma, ele não possui um caráter preventivo em termos de detecção de possíveis fraudes (FLETES, 2020).

Em agosto de 2021, o Banco Central estabeleceu novas práticas para avançar nas medidas de segurança no ecossistema Pix. Entre elas, destacam-se as que se destinam a evitar a lavagem de dinheiro (BCB, 2020c):

- **estabelecer limite de R$ 1.000,00** para operações **entre pessoas físicas** (incluindo MEIs) utilizando meios de pagamento em arranjos de **transferência no período noturno** (das 20 horas às 6 horas), incluindo transferências intrabancárias, Pix, cartões de débito e liquidação de TEDs;
- permitir que os **participantes recebedores do Pix retenham uma transação por 30 minutos durante o dia ou por 60 minutos durante a noite para a análise** de risco da operação, informando ao usuário quanto à retenção;
- **tornar obrigatório** o mecanismo, já existente e hoje facultativo, **de marcação no Diretório de Identificadores de Contas Transacionais** (DICT) de contas em relação às quais existam indícios de utilização em fraudes no Pix, inclusive no caso de transações realizadas entre contas mantidas no mesmo participante;
- **permitir consultas ao DICT para alimentar os sistemas de prevenção à fraude das instituições**, de forma a coibir crimes envolvendo a mesma conta em outros meios de pagamento e com outros serviços bancários;
- exigir que os participantes do Pix adotem controles adicionais em relação a transações envolvendo contas marcadas no DICT, inclusive para fins de eventual recusa a seu processamento, combatendo assim a utilização de contas de aluguel ou "laranjas";
- **determinar que os participantes** de arranjos de pagamentos eletrônicos **compartilhem, tempestivamente, com autoridades de segurança pública**, as informações sobre **transações suspeitas** de envolvimento com **atividades criminosas**;
- **exigir das instituições reguladas controles adicionais sobre fraudes**, com reporte para o Comitê de Auditoria e para o Conselho de Administração ou, na sua ausência, à Diretoria Executiva, bem como manter à disposição do Banco Central tais informações; e
- **exigir histórico comportamental e de crédito para que empresas possam antecipar recebíveis de cartões** com pagamento no mesmo dia (D+0), mitigando a ocorrência de fraudes. (BCB, 2020 [*S./p.*], grifo nosso])

Para conferir ainda mais robustez aos mecanismos de segurança, no final de setembro de 2021, o Banco Central alterou o regulamento do Pix por meio da Resolução BCB nº 147. Dentre as inovações disponíveis exclusivamente para o Pix, destacam-se:

- A inclusão do bloqueio cautelar pelo Provedor de Serviços de Pagamento (PSP) do usuário recebedor em caso de suspeita de fraude;
- A obrigatoriedade da solicitação da notificação de infração pelos participantes provedores de conta transacional em caso de fundada suspeita de fraude e da utilização das notificações de infração nos mecanismos de detecção de fraude pelos participantes do Pix
- A ampliação do uso de informações para fins de prevenção à fraude através de nova funcionalidade do DICT
- A ampliação da responsabilização das instituições
- A criação de mecanismos adicionais para proteção dos dados. (BCB, 2021d, [*S./d.*])

Cumpre destacar que, na mesma resolução, o Banco Central também estabeleceu a possibilidade de suspensão da transação Pix suspeita de fraude por 72 horas, a fim de que a legitimidade da transação possa ser averiguada. Em nota, o BC explica que tais medidas reafirmam a necessidade de os participantes do ecossistema Pix aprimorarem seus mecanismos de segurança e análise de fraude.

Porém, de acordo com Lima (2020, [*S./p.*]), o estabelecimento de medidas de segurança para o Pix "deve ser abrangente e, como qualquer outro sistema, não simplesmente alertar para possíveis ações criminosas, mas também fornecer proteção e segurança ao cidadão". O autor alerta, ainda, que a criação do Pix envolve uma repressão posterior ao ato fraudulento, e não uma prevenção. E isso é particularmente importante em se tratando de crimes relacionados à lavagem de dinheiro, conforme será visto no item a seguir. Maior segurança no ambiente Pix influencia a percepção de credibilidade e favorece a adesão. Segundo o relatório de pesquisa da Febraban (2021), a aderência ao Pix ainda é maior entre as pessoas físicas do que entre pessoas jurídicas, e a segurança do ambiente pode ser uma das razões para a não adesão do comércio à ferramenta.

2.2 Lavagem de dinheiro: transações e prevenção

O Conselho de Controle de Atividades Financeiras (COAF, 2021, [*S./p.*]) define a lavagem de dinheiro (LD) como "um conjunto de operações comerciais ou financeiras que buscam a incorporação na economia de cada país, de modo transitório ou permanente, de recursos, bens e valores de origem ilícita".

Essa incorporação acontece por meio de um processo dinâmico em três fases que ocorrem de maneira independente e, muitas vezes, simultânea: 1. distanciamento dos fundos de sua origem; 2. disfarce das diversas movimentações; 3. disponibilização do dinheiro para criminosos. De acordo com o Coaf (2021), o objetivo da primeira fase, denominada "colocação", é evitar a associação direta dos envolvidos com o crime. Na segunda, chamada "ocultação", busca-se colocar obstáculos ao rastreamento dos recursos. E, finalmente, as diversas movimentações no ciclo de lavagem têm o objetivo de fazer com que o dinheiro disponibilizado seja considerado lícito ou limpo. Essa fase é conhecida como "integração".

Existe uma modalidade de LD, por exemplo, que acontece por meio da geração de saldo credor em cartão de crédito. É apenas um mecanismo que movimenta recursos ilícitos no âmbito da lavagem de dinheiro no sistema financeiro. Segundo Gouveia (2021), seus estágios podem ser compreendidos dentro das fases da LD da seguinte forma: 1. a atividade ilícita envolve o dinheiro proveniente de atos criminosos; 2. na fase da colocação, ocorre a conversão desse dinheiro em outros recursos monetários; 3. na fase da ocultação, os recursos são movimentados para disfarçar a origem (realização de pagamento acima do valor da fatura); 4. na fase da integração, são feitos investimentos em negócios em negócios lícitos ou compra de ativos (restituição do saldo credor usado na compra de bens e investimentos).

A destinação da LD pode ser usada para favorecer esquemas de corrupção, tráfico de drogas e até o terrorismo. Na verdade, o financiamento do terrorismo tem ligação estreita com a LD, por isso ambos os conceitos, geralmente, são citados em conjunto (COAF, 2021).

Com a introdução do Pix, houve redução nas transações em moeda, visto que o uso de papel-moeda pode se reduzir pela metade até 2030 (UOL, 2020). Além disso, as técnicas destinadas à LD procuraram caminhos para contornar as restrições. Como reforça Lima (2020), a presença de mecanismos de proteção não elimina a criminalidade, pois, diante das barreiras, ela busca formas de migrar ou se aperfeiçoar.

Esse panorama torna ainda mais importante o aprimoramento dos sistemas de segurança e prevenção de fraude das instituições financeiras. Os atos fraudulentos realizados com papel-moeda, depósitos em espécie e propriedades adquiridas em dinheiro servem

de alerta para o que é possível ocorrer no cenário digital, pequenas quantias podem desaparecer instantaneamente de diversas contas. Lima (2020, [*S./p.*]) afirma que "se de um lado o sistema facilita a investigação quanto à lavagem de capitais e movimentação de proveitos criminosos, na outra ponta agiliza a vantagem defeituosa de outros crimes patrimoniais".

Os mecanismos de segurança do Pix citados no item anterior desempenham o papel de restringir a ocorrência de fraudes e LD. Contudo, as medidas tomadas *a posteriori* servem para reparar o evento fraudulento, mas não para preveni-lo. Nesse sentido, a tecnologia proporcionada pelo ML tem se mostrado como caminho para solucionar tal dificuldade, conforme será apresentado no próximo item.

2.3 O aprendizado de máquina aplicado à prevenção de lavagem de dinheiro

O aprendizado de máquina ou *machine learning* é, na verdade, um subconjunto da inteligência artificial que permite que o computador aprenda com os dados em vez de utilizar uma programação explícita. Essa tecnologia compõe um sistema capaz de automatizar a tomada de decisões complexas, baseadas na própria experiência da máquina obtida por meio da utilização do sistema (SAS, 2020).

Em 2019, uma das palestras proferidas no 13º Seminário "Controles Internos e *Compliance*, Auditoria e Gestão de Riscos" foi realizada por Clesito Fechine, coordenador de gestão da informação da Unidade de Inteligência Financeira (UIF). Nela, Fechine afirmou que o aperfeiçoamento dos processos de prevenção à lavagem de dinheiro (PLD) se encontra justamente no uso do ML, especialmente diante do aumento que ele observara até então de 140% na comunicação de suspeitas de LD (CNSEG, 2019). O ML traz consigo a capacidade de identificar padrões suspeitos e analisar dados de maneira mais eficiente e ágil em face dos desafios trazidos pelo pagamento instantâneo.

Os analistas de PLD podem se beneficiar do uso do ML por meio do reconhecimento de atividades suspeitas. As técnicas de detecção possibilitadas por essa tecnologia identificam anomalias ou "observações que aparentam ser matematicamente distantes do esperado", e isso se diferencia dos métodos tradicionais porque "com pouco direcionamento e sem dados classificados, é possível encontrar atividades potencialmente suspeitas não definidas por uma regra" (SAS, 2020).

Dessa forma, as instituições financeiras podem promover mudanças na arquitetura da PLD por meio da troca dos mecanismos baseados em regras para modelos de ML. Elas também podem utilizar o ML para suportar a construção de modelos que alimentem os mecanismos tradicionais. Isso agrega inteligência às atividades, favorecendo a "classificação de risco, ajuste de regras e priorização de alertas" (SAS, 2020, [*S./p.*]).

O artigo intitulado *Como IA e* Machine Learning *estão redefinindo práticas antilavagem* – produzido pela *Statistical Analysis System*, empresa de *Business Intelligence* – apresenta alguns usos do ML já colocados em funcionamento para PLD. Além da detecção de anomalias, é possível: complementar o acompanhamento de transações; segmentar clientes; classificar o risco de clientes; analisar redes sociais, definir e ajustar limites.

Dentro da estratégia modular para o Pix, a Microsoft, parceira de tecnologia do projeto, criou o módulo antifraude e antilavagem de dinheiro, que é "responsável pela prevenção

de fraudes e análise de LD" (MICROSOFT, 2021). A arquitetura, proposta no projeto Simplificando Pagamentos Digitais, utiliza serviços do Azure fundamentados em ML, com modelos supervisionados, banco de dados baseado em grafos, serviços sem servidor (*serveless) para a* definição do perfil do usuário e detecção de anomalias por meio de modelos probabilísticos. Esse módulo supre o requerimento de transações em tempo real, mantendo o desempenho e a eficiência na detecção de falso-positivos.

O objetivo do projeto Simplificando Pagamentos Digitais, ao utilizar diferentes técnicas de aprendizado além de algoritmos estatísticos e de grafos para PLD, é fortalecer a segurança do ambiente Pix a fim de que mais consumidores e empresas, de todos os portes, possam aderir à tecnologia de pagamento digital instantâneo. É importante ressaltar que os serviços Azure, ágeis e escaláveis, favorecem o aprendizado contínuo e dinâmico do comportamento fraudulento, e podem ser utilizados para sistemas antifraude, além do PLD (MICROSOFT, 2021). Dessa maneira, o projeto decidiu focar inicialmente no PLD, boleto e Pix, sendo inédito no Brasil e expansível para o antifraude em tempo real.

2.4 Utilização de grafos

Um dos meios utilizados para identificar transações financeiras suspeitas remete ao século XVIII, quando o alemão Leonhard Euler, considerado um dos mais proeminentes matemáticos de sua época, propôs a resolução do problema das sete pontes de Königsberg e, daí, fundou as bases para a Teoria dos Grafos (WIKIPEDIA, 2021a).

Contudo, sua descoberta permaneceu restrita aos muros da academia, até que, 200 anos depois, o húngaro judeu Dénes Kőnig reviveu a teoria, trazendo para a sociedade um livro didático intitulado *Theorie der endlichen und unendlichen Graphen* (Teoria dos grafos finitos e infinitos). Segundo Bondy e Murty (2008), diversas situações cotidianas podem ser descritas por meio de diagramas (grafos) formados por conjuntos de pontos (atores, entidades, vértices), ligados por linhas (relacionamentos, vínculos, arestas).

Entretanto, antes de abordar a aplicabilidade dos grafos à PLD, entende-se como necessário traçar um paralelo entre a Teoria dos Grafos e o conceito de sociedade em rede de Manuel Castells (2013). De maneira simplificada, esse conceito afirma que a modernidade e os avanços tecnológicos que dela decorrem ampliam as redes de conexões entre os indivíduos. Os indivíduos dessa teia social são os vértices, e seus relacionamentos são as arestas. Essa relação se aproxima da Teoria dos Grafos. Nos grafos, os vínculos aparecem agrupados tanto em soma de valores quanto em contagem de lançamentos, mas segregados por natureza do lançamento.

Entende-se que os grafos podem ser aplicados à PLD dada a compreensão que essa teoria permite acerca da complexidade das relações humanas e, por consequência, das relações financeiras. Ao aplicar a técnica da análise de grafos na análise de transações bancárias suspeitas de envolvimento com LD, Lima, Serrano e Cupertino (2020) concluem que

> Os grafos são uma ferramenta aplicável na repressão ao crime de lavagem de dinheiro, uma vez que promovem ganhos informacionais diversos, favorecem a descoberta de transações financeiras típicas de lavagem de dinheiro, como *polling accounting* e *straw men*, além de auxiliarem no rastreamento de recursos no sistema bancário, inclusive em redes financeiras complexas. (LIMA; SERRANO; CUPERTINO, 2020, p. 1)

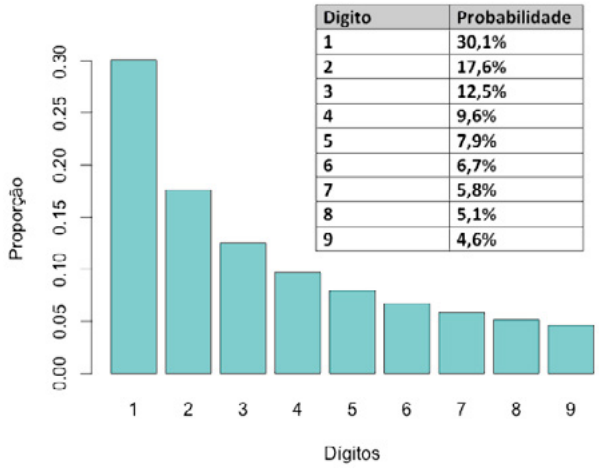
Como sugestão de pesquisas e aplicações futuras, os referidos autores recomendam

> O estudo das medidas de centralidade dos grafos nas análises de redes de transações bancárias. Redes altamente centralizadas são dominadas por pessoas que controlam o fluxo de recursos, ao passo que redes pouco centralizadas não possuem um único ponto de movimentação de recursos, dificultando o rastreamento de recursos. (LIMA; SERRANO; CUPERTINO, 2020, p. 1)

Diante dessas observações, os criadores do projeto entendem a importância da utilização dos grafos para a detecção de LD. Por meio dos grafos, é possível identificar a origem do dinheiro que pretende ser ocultado na LD, o que facilita identificar a correlação entre os nós (pessoas físicas e jurídicas, instituições financeiras e não financeiras) e o fluxo financeiro entre eles.

2.5 Lei de Benford e a detecção de fraudes fiscais

Figura 1. Distribuição da probabilidade do primeiro algarismo



Fonte: Disponível em: https://www.monolitonimbus.com.br/lei-de-benford/.

A Lei do Primeiro Algoritmo, também conhecida como Lei de Benford, foi proposta pelo matemático e engenheiro elétrico Frank Benford, e consiste na análise probabilística de certos números de serem utilizados. O matemático notou que, tanto na natureza quanto nas produções humanas, se observados para análise apenas os primeiros dígitos de cada número, a distribuição de ocorrência do aparecimento de determinado algoritmo se dava de acordo com a proporção apresentada na figura 1, em que os números de menor valor unitário apareciam com maior recorrência que os de maiores valores unitários. Tais proporções foram obtidas pela seguinte fórmula:

$$B(d)= \log(d+1) - \log(d)$$

Em que "B" representa a probabilidade e "d" representa o dígito que está em análise. Dessa forma, a Lei de Benford é capaz de identificar anomalias numéricas, podendo indicar que tais números analisados tenham sido adulterados, visto que fogem da proporcionalidade de distribuição dos dígitos.

A Lei de Benford tem sido utilizada para identificar inúmeras fraudes ao longo da história, e hoje compõe a infraestrutura da arquitetura que utilizaremos. Um dos mais marcantes exemplos de aplicação da Lei do Primeiro Algoritmo na detecção de fraude ocorreu no Brasil durante a reforma do Estádio do Maracanã, em que o Tribunal de Contas da União identificou que havia ocorrido um superfaturamento de R$ 107 milhões por parte da empreiteira responsável. Tal fraude se deu por meio de algo conhecido como "Jogo de Planilha", no qual o fraudador infla os valores dos insumos para a realização da obra e, assim, pratica-se desvio de dinheiro após o processo de licitação.

2.6 O Open Finance e a prevenção à fraude e à lavagem de dinheiro

O Open Banking é um sistema no qual os clientes do sistema bancário (bancos, *fintechs, IPs*) podem consentir o compartilhamento de suas informações com instituições autorizadas pelo Banco Central. Além disso, suas contas bancárias podem ser movimentadas "a partir de diferentes plataformas e não apenas pelo aplicativo ou site do banco" (BCB, 2021e). Ademais, cumpre destacar que, na Fase III do Open Banking, poderá ser iniciado o Pix via estrutura do Open Banking.

Entre outros benefícios como transparência, inclusão, portabilidade e estímulo à inovação, esse tipo de abertura visa conferir mais competitividade ao mercado. As instituições participantes do ecossistema do Open Banking poderão ofertar produtos e serviços para clientes da concorrência e, com isso, permitir opções com menores custos e melhores condições.

Na esteira da abertura do acesso aos dados e em uma perspectiva mais ampla, encontra-se o conceito de Open Finance, que vai além dos produtos bancários. Como o Banco Central estabeleceu um cronograma de fases graduais e evolutivas para o Open Banking no Brasil, os primeiros passos se aplicam aos bancos e às instituições financeiras. Contudo, o horizonte do projeto envolve a ampliação do escopo de empresas, como plataformas de investimento, corretoras de seguro e fundos de previdência (BRENOL, 2021).

Segundo o Banco Central do Brasil (2021e, [*S./p.*]), as medidas de proteção dos dados dos clientes envolvem o "consentimento (autorização de compartilhamento), autenticação (verificação de identidade) e confirmação". Porém, não obstante a segurança do sistema e o estabelecimento de regras publicadas pelo Conselho Monetário Nacional (CMN) e pelo Banco Central, é importante a atenção para a possibilidade de aumento das tentativas de fraudes financeiras.

Considerando a curva ascendente do volume de transações por meio do Pix, e os desafios que acompanham esse crescimento, a Microsoft desenvolveu uma arquitetura inteligente antifraude para o Pix e Open Finance (MICROSOFT, 2021). A proposta envolve um fluxo analítico que captura percepções a partir de dados transacionais e de comportamento dos consumidores.

Em seu documento sobre Open Finance, a Microsoft enfatiza a importância de mitigar o risco de fraude no ecossistema e explica que "todos os participantes devem garantir que os controles de combate à fraude tenham acesso suficiente aos sistemas em sua organização" (MICROSOFT, 2021, [*S./p.*]).

O sistema possui recursos que podem ser utilizados para facilitar a prevenção à fraude. Além da atenção aos requerimentos de segurança e às especificações técnicas obrigatórias, destaca-se o emprego da Identidade Digital Descentralizada, na qual a identidade e as interações digitais próprias de cada usuário não se encontram sob "controle de outras partes no ecossistema de compartilhamento de dados". A prevenção ainda conta com a autenticação multifator (Azure AD B2C) que mantém a "homogeneização do nível de segurança no login dos usuários". O modelo Zero Trust do parceiro tecnológico consiste em uma evolução dessa infraestrutura que aplica a "integridade do dispositivo e acesso com privilégios mínimos". A validação do usuário ainda dispõe de solução de prova de vida por meio de reconhecimento de voz, facial ou de movimento da cabeça.

O alvo dos recursos disponibilizados não se restringe à prevenção de fraude, a atenção também recai sobre aspectos como detecção e resposta à fraude, conforme destacado a seguir:

> No quesito resposta à fraude, cada instituição participante pode criar um mecanismo de maneira customizada, com revogação, modelo de responsabilidade e gerenciamento de disputas entre o TPP, PSU e ASPSP.
>
> Já no que diz respeito à detecção de fraude, foi criada a arquitetura de referência [...] que suporta antifraude e antilavagem de dinheiro. A arquitetura Antifraude proposta é híbrida, pois suporta tanto as cargas de trabalho relacionadas ao Open Banking, como a parte transacional – por exemplo para o Pix – que demanda um tempo de resposta para *score* em milissegundos. (MICROSOFT, 2021, [*S./d.*])

3 Visão Geral

A Shipay é um *hub* que integra carteiras digitais (PicPay, Mercado Pago, Ame, PagBank etc.) em sistemas como frente de loja, ERP, PDV, e-commerce e aplicativos. Dessa forma, a Shipay tem como *core* de sua atuação o objetivo de simplificar os pagamentos digitais, integrando diversas carteiras no sistema de caixa (PDV) por meio de um QR Code exclusivo do estabelecimento. Isso facilita o relacionamento dos consumidores e dos comerciantes com os meios de pagamento digitais (QR Code, Pagamento instantâneo, Criptomoedas, P2P, P2M e qualquer outro meio que surja no mercado). Portanto, a missão da Shipay é facilitar a vida do usuário, permitindo que o estabelecimento cadastre todas as novas carteiras disponíveis, tenha uma única interface e realize todas as transações, conciliando-as de forma automática e instantânea no sistema de caixa.

A empresa em questão oferece serviços relacionados ao Pix e, diante dos problemas ligados à LD, propõe-se a implementar em seu sistema diferentes técnicas de aprendizado de máquina, além de algoritmos estatísticos e de grafo na nuvem do Azure, com a meta de prevenir e barrar transações dessa natureza.

Contudo, para estabelecer uma prova de conceito, a princípio, a arquitetura é desenvolvida pelo projeto Simplificando Pagamentos Digitais nos casos de LD que envolvam o pagamento de fatura de cartão de crédito.

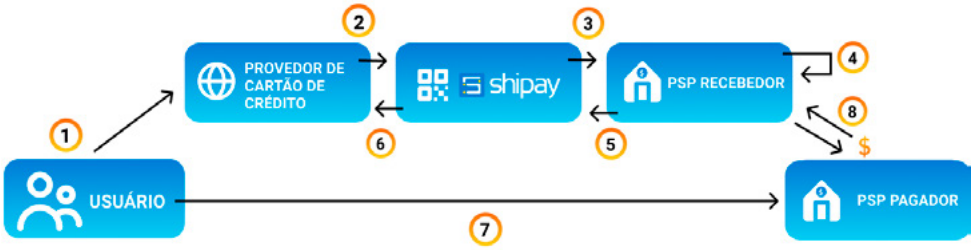
Essa escolha foi motivada por uma lacuna encontrada a partir da experiência dos membros do projeto, integrantes da empresa com clientes no mercado. Verificou-se o risco de ocorrência de LD por meio dos pagamentos de fatura de cartão de crédito. É possível que uma fatura de cartão seja paga por múltiplos CPFs (pessoas físicas), o que dificulta a

identificação da origem do dinheiro. Além disso, a fatura pode ser paga acima do limite disponível no cartão de crédito, liberando, instantaneamente, quando realizada pelo Pix, o limite proporcional ao valor pago. Isso, por sua vez, abre espaço para a transformação de ativos de origem ilícita em crédito.

Para compreender como a introdução da arquitetura funciona para fins de PLD, é necessário descrever o modelo atual de negócio da Shipay.

Cada número presente na Figura 2 ilustra o fluxo do modelo atual da seguinte forma:

Figura 2. Fluxograma de um pagamento de fatura de cartão de crédito via Pix



Fonte: Elaborada pelo autor.

1. O usuário emite o boleto da fatura do provedor do cartão de crédito.
2. Esse provedor aciona a Shipay para comunicar os dados da fatura do usuário.
3. A Shipay comunica as informações da transação ao PSP recebedor.
4. O PSP recebedor emite a cobrança.
5. A Shipay recebe a cobrança e emite um QR Code que contém os dados da ordem de pagamento.
6. A Shipay devolve a cobrança ao provedor de cartão de crédito.
7. O provedor de cartão de crédito envia o QR Code para o usuário, que opta por pagar a fatura via Pix por meio do PSP pagador de sua escolha.
8. A transação ocorre entre ambos os PSPs mencionados e, finalmente, a informação acerca da quitação da onerosidade passa pela Shipay e é enviada de volta ao usuário final.

É possível, portanto, inserir a arquitetura de detecção de fraudes utilizando o mesmo fluxo do modelo de negócio atual. Dessa forma, todos os dados que naturalmente passam pelos servidores da empresa serão redirecionados para o módulo de detecção de anomalias fraudulentas. Nele são realizados inúmeros testes, gerando de dois a quatro tipos diferentes de *scores* (dependendo da fase de desenvolvimento da arquitetura) para avaliar a probabilidade da transação configurar LD. De posse desses dados, o módulo de prevenção à fraude e à lavagem de dinheiro consegue comunicar os participantes e bloquear a transação suspeita.

Com essa arquitetura, o projeto propõe um método rápido e eficaz de identificar transações suspeitas de LD. Sendo, assim, endereçado às dores do analista de PLD, que encontra dificuldades ao realizar suas análises, devido ao fato de o Pix ser um método de pagamento instantâneo.

Esse analista sabe que o Pix tem ganhado cada vez mais espaço no âmbito das transações financeiras. Sabe também que existem camadas de segurança, mas que elas não têm se mostrado eficazes em prevenir que as transações de LD ocorram. As análises desse profissional são feitas de maneira lógica e tendem a ser práticas e racionais.

Portanto, a tecnologia proposta simplificará o trabalho do analista de PLD, permitindo que ele obtenha: uma listagem dos Pix suspeitos de LD referente ao pagamento de fatura de cartão de crédito de determinado período; maiores detalhes acerca do Pix suspeito de LD; e condições de impedir a criação de uma cobrança Pix para pagamento de fatura de cartão de crédito em caso de suspeita de LD.

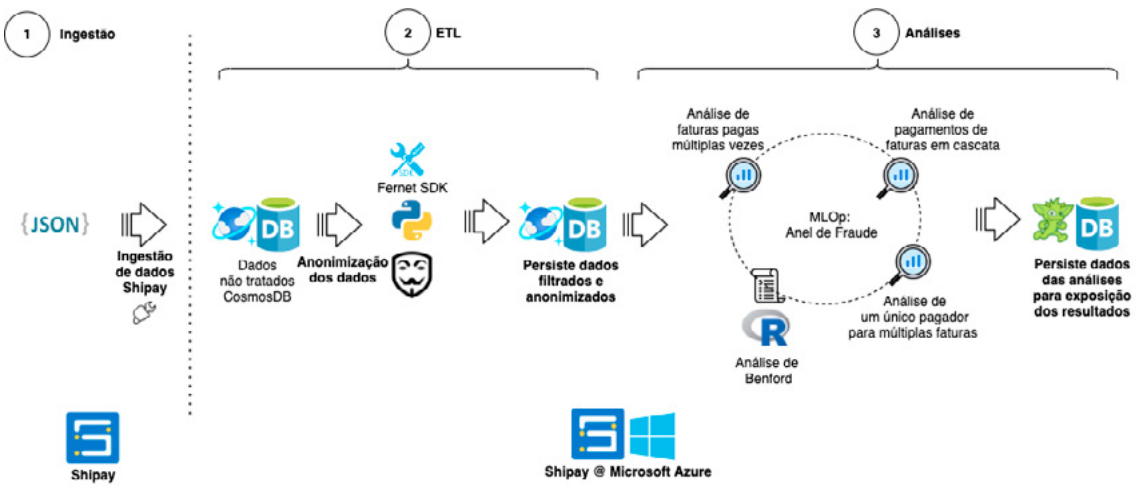
Em termos gerais, a proposta do projeto consiste em uma arquitetura que se utiliza de diferentes técnicas de aprendizado, bem como de algoritmos estatísticos e de grafos para identificar transações de LD. Por meio do ML, é possível detectar anomalias e traçar perfis transacionais dos usuários no Pix para pagamentos de faturas de cartão de crédito. Com a evolução do projeto, o Simplificando Pagamentos Digitais propõe que a arquitetura antilavagem de dinheiro poderá ser utilizada em todo o ecossistema Pix. Porém, ressalta-se que a proposta não representa um método para prevenção a qualquer tipo de fraude no ambiente Pix.

3.1 Funcionalidades

A arquitetura de referência criada se aplica à prevenção de fraude e de LD. A proposta suporta a parte transacional para o Pix, que demanda um tempo de resposta em milissegundos. Os serviços da nuvem do Azure facilitam a construção e a testagem de modelos customizados, baseando-se em dados anonimizados dos usuários da transação.

A Figura 3 mostra a estrutura que o projeto utilizou para fins de protótipo. É possível notar que se trata de uma arquitetura enxuta e ágil, visto que o tempo médio de resposta, para a parte antifraude, é inferior a 100 milissegundos, quando aliada aos algoritmos supervisionados. Se comparado ao tempo máximo de uma transação Pix, que é de 10 segundos, torna-se evidente a viabilidade e velocidade da infraestrutura para a PLD (AZURE MICROSOFT, 2021).

Figura 3. Esquema da arquitetura de referência utilizada para fins deste protótipo



Fonte: Elaborada pelo autor.

Os passos envolvidos são:

1. Ingestão de dados que serão analisados.
2. Tratamento dos dados (mapeamento, anonimização etc...).
3. Análise dos dados.

Para melhor compreensão da arquitetura, alguns elementos e funções precisam ser definidos. O Azure *Data Factory* fornece uma camada de transformação e integração de dados.

O *software development kit (SDK)* Python Fernet garante que os dados confidenciais sejam gerenciados de maneira adequada. É ele que anonimiza informações sensíveis, como: números de cartão de crédito, nomes, endereços, carteiras *bitcoins*, números de telefone, dados financeiros e outros, tendo com finalidade garantir a segurança de dados sensíveis, em conformidade com a Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/2020).

O *Azure Machine Learning Studio,* por sua vez, é o serviço que fornece uma plataforma completa de ciência de dados. Foi utilizada a infraestrutura do Azure ML Studio para executar um algoritmo com base na Lei de Benford. Esse algoritmo efetua a análise da distribuição de dígitos em conjunto de dados estatísticos que, juntamente com o anel de fraude, formam a principal função para a análise dos dados transacionais, atuando como os principais responsáveis pela identificação e supressão das transações fraudulentas. A Lei de Benford pode ser utilizada para o realizar a análise probabilística do primeiro e do segundo dígitos.

O *Azure Cosmos DB* fornece um serviço de banco de dados de grafo por meio da API do Gremlin em um serviço de banco de dados totalmente gerenciado criado para qualquer escala. Utilizamos o *Azure Gremlin API Cosmos DB* para a execução das análises contidas no Anel de Fraude e exposição do resultado por meio de grafos para a demonstração de relacionamentos entre as análises.

3.1.1 Jornada do usuário

De maneira prática, considerando a jornada do usuário, a proposta do projeto pode ser resumida no esquema a seguir:

1. Pontos de contato: o usuário do cartão de crédito não terá acesso em nenhum momento à arquitetura de PLD proposta no projeto Simplificando Pagamentos Digitais. As únicas entidades a ter acesso às informações provenientes do Microsoft *Azure Functions (resultados das an*álises da arquitetura de PLD*)* são os PSPs participantes da transação e o provedor de cartão de crédito.
2. Etapas: o usuário decide realizar o pagamento da fatura do seu cartão de crédito via Pix e escolhe seu banco/carteira de preferência para isso.
3. Faz: por meio do emprego de diferentes técnicas de aprendizado, algoritmos estatísticos e de grafos, é possível detectar anomalias nas transações Pix para pagamento de faturas de cartão de crédito.
4. Pensa e sente: as transações são instantâneas, logo, o usuário sente a praticidade e facilidade em realizar os pagamentos e transferências via Pix.
5. Dores: o ponto de dor do cliente é basicamente o motivo pelo qual ele está buscando ajuda na solução. Questionamentos sobre a segurança e confiabilidade do processo, além da possibilidade de ocorrência de transações ilícitas.
6. Oportunidades: para o cliente, a maior oportunidade é realizar o pagamento da sua fatura por meio do Pix com segurança e ter o crédito liberado instantaneamente, ao contrário do pagamento via boleto.

4 Escopo do Protótipo

Como premissa maior do presente projeto, está a criação de uma arquitetura que utiliza serviços de nuvem para a PLD nas transações do ecossistema Pix. Contudo, o escopo desenvolvido *a priori* enfatiza o emprego desse modelo de PLD no pagamento de faturas de cartão de crédito, via Pix.

A delimitação do escopo tem em vista a maior facilidade de prototipar com um número mais restrito de transações e fora do mundo físico do comércio. Geralmente, a LD feita por meio de estabelecimentos comerciais é transacionada em espécie. Contudo, na fase de ocultação, a movimentação dos ativos acontece de forma eletrônica com destino a contas de diferentes titularidades, a fim de "legitimar" o dinheiro de origem ilícita. Outra razão para a escolha do escopo do protótipo é a praticidade de aplicação da referida arquitetura, nas transações dos parceiros comerciais da Shipay.

Além dessas justificativas, cumpre destacar que, à medida que o sistema for alimentado com dados constantes por meio das transações, ele será aperfeiçoado na detecção de LD por meio da aprendizagem da máquina.

Tendo em vista o escopo apresentado, a seguir encontram-se os principais indicadores de desempenho que deverão ser observados em determinado momento do estágio evolutivo do projeto – indicadores de desempenho, de acurácia e eficiência do sistema, de falso positivos, da quantidade de chamadas e do alcance da solução. Importante salientar que não será possível observar todos os indicadores nesta etapa de prova de conceito.

1. Indicadores de desempenho estratégico – o projeto pretende que, num futuro próximo, por meio de diferentes técnicas de aprendizado dinâmico com governança de modelos

de acordo com a perturbação do sistema, algoritmos estatísticos e de grafos, a arquitetura seja capaz de identificar uma transação de LD antes de sua ocorrência.

2. Indicadores de desempenho de processos – o projeto conta com **viabilidade,** uma vez que envolve a aplicação de uma arquitetura de referência, utilizando serviços *serverless*, banco de dados; quanto à **eficácia**, nossos desenvolvedores do projeto observaram, nos primeiros testes de produção, que a arquitetura é capaz de suportar a análise de um grande volume de transações sem ultrapassar o período médio de tempo necessário para a transação Pix; em relação à **efetividade**, considera-se a capacidade do projeto em estabelecer um método preventivo, facilmente aplicável e célere de PLD no ecossistema Pix; quanto à **produtividade**, o analista de PLD obterá um relatório completo para exercer sua função; e em termos de **valor**, o projeto considera que, quando o algoritmo de aprendizado de máquina estiver treinado com a quantidade suficiente de dados, poderá ser aplicado a qualquer transação Pix, contando com um *output* em milissegundos.
3. Indicadores de qualidade – quanto às **finanças**, os custos com a arquitetura são menores quando comparados a um ambiente implantado localmente, em função dos recursos-chave em nuvem do *Azure Functions (serverless)*; em relação às **vendas**, a infraestrutura do projeto poderá ser ofertada para provedores de cartão de crédito, instituições financeiras e plataformas de e-commerce. Até o próprio Banco Central poderá utilizá-la no ecossistema Pix; quanto aos **recursos humanos**, destaca-se a relevância do papel dos colaboradores responsáveis pelo supervisionamento da arquitetura, além do trabalho colaborativo dos analistas de PLD que contribuem para a aprendizagem da máquina.

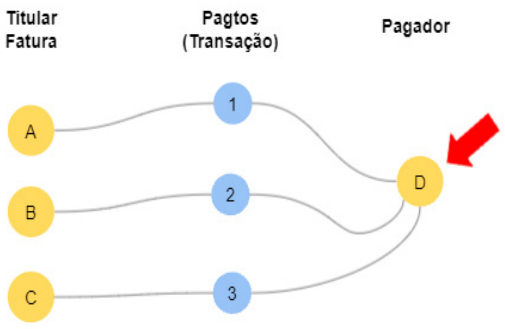
4.1 Resultados da prova de conceito da arquitetura de lavagem de dinheiro

O projeto Simplificando Pagamentos Digitais propõe, em seu protótipo, o emprego de diferentes técnicas de aprendizado, além de algoritmos estatísticos e de grafo, para a detecção de lavagem de dinheiro no pagamento de faturas de cartão de crédito.

Para fins de realizar a prova de conceito, nossos desenvolvedores realizaram inúmeros testes, com resultados bastante promissores, na arquitetura em conjunto com serviços gerenciados na nuvem do Azure.

A Arquitetura utilizada possui como resultado uma combinação de quatro *outputs* diferentes que, juntos, constituem o *score* que rotula a transação como suspeita.

Figura 4



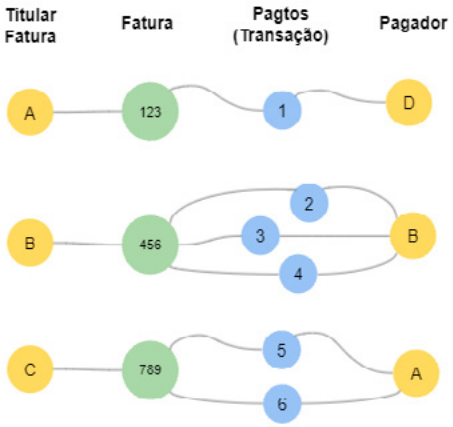
Fonte: Elaborada pelo autor.

Como é possível observar na Figura 4, trazemos os grafos, uma das formas de visualização dos resultados da arquitetura, que permitem traçar relações entre os titulares e os pagadores da fatura. Observem que existem inúmeras possibilidades de múltiplos pagamentos para a mesma fatura, e é possível que haja múltiplos pagadores, fatos estes que podem ser indícios de que esteja ocorrendo lavagem de dinheiro.

Para fins exemplificativos, gostaríamos de abordar adiante três cenários possíveis que o protótipo rotularia como suspeito de LD.

Na Figura 5, nota-se que o pagador "D" está realizando o pagamento da fatura de outros diferentes titulares (A,B,C).

Figura 5

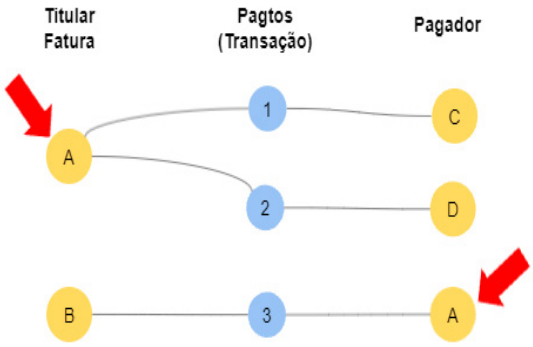


Fonte: Elaborada pelo autor.

Contudo, vale ressaltar que, nessa hipótese, a arquitetura irá identificar a transação como suspeita, porém, caso seja avaliado que existe, por exemplo, algum vínculo familiar, essa rotulação será corrigida e desconsiderada no cálculo do *score final*.

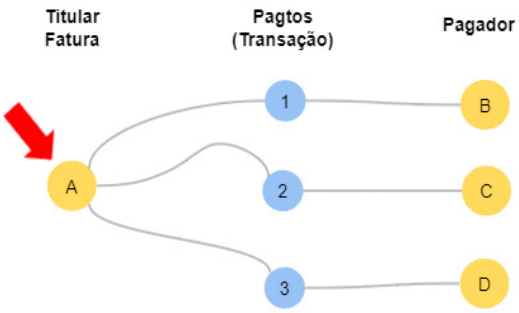
Outro cenário provável refere-se à hipótese de o titular da fatura ter sua fatura paga por mais de três pagadores diferentes (vide figura 6).

Figura 6



Fonte: Elaborada pelo autor.

Figura 7



Fonte: Elaborada pelo autor.

Fato este considerado como suspeito de que está ocorrendo LD, para fins de análises, pois é muito comum que, na fase de ocultação, os fraudadores utilizam diversas contas de terceiros para movimentar os ativos e, assim, esconder a sua origem ilícita.

Por fim, o último cenário a ser abordado trata-se da hipótese de um titular da fatura ter sua fatura paga por outros e, mesmo assim, pagar a fatura de terceiros, conforme na Figura 7.

Portanto, nota-se que a arquitetura de PLD proposta neste protótipo trabalha com inúmeros fatores e hipóteses, e, por meio da utilização contínua da solução, o sistema terá um aumento exponencial de sua precisão em prevenir que ocorra LD.

Vale ressaltar que, para fins desta prova de conceito, não implementamos ainda o *machine learning*, devido ao restrito volume de dados utilizados no protótipo.

Por meio do Anel de Benford, mediante a criação de um histograma com a análise do primeiro e do segundo dígitos, a arquitetura é capaz de detectar anomalias probabilísticas de a transação ter sido originada na LD.

Tabela 1

Transação	*Score*	Lei de Benford	AF - Titular	AF - Pagador	*Machine Learning**	Determinístico
123	4	1	2	0	1	0
456	3	0	3	0	0	0
789	3	1	1	1	0	0

No que tange à visualização dos *scores*, a arquitetura pode ser observada conforme a Tabela 1. Nota-se que o risco de cada transação é rotulado de acordo com a somatória da pontuação final após todos os algoritmos da arquitetura atribuírem seus *scores*.

Destaca-se que a arquitetura de PLD do projeto permite o estabelecimento de regras fixas para serem aplicadas no *score* da transação, as quais podem ser exemplificadas pelas seguintes *Queries:*

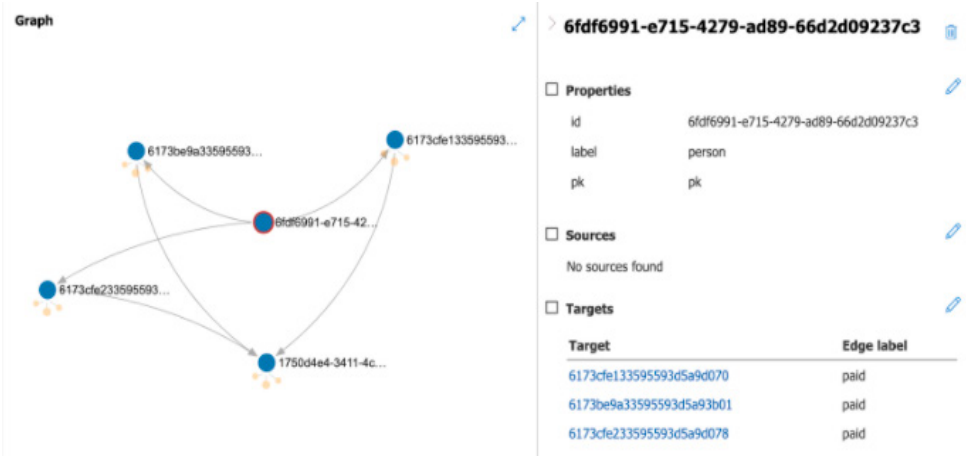
1. Múltiplos pagamentos em um mês (> 3).
2. Um pagamento acima do valor da fatura (> 50%).

3. Dois pagamentos consecutivos acima do valor da fatura (> 25%).
4. Dois pagamentos acima do valor da fatura em meses consecutivos (> 25%).
5. Somatório dos pagamentos no mês excedem o valor da fatura (> 20%).

Por fim, gostaríamos de compartilhar o resultado de um dos testes que realizamos em que a arquitetura de PLD foi capaz de identificar um caso um tanto quanto peculiar e que fortemente pode ser enquadrado como lavagem de dinheiro.

No caso em questão, um usuário pagou três faturas de sua titularidade e, mais adiante, todas essas contas transferiram ativos para pagar a fatura de outro titular da fatura, conforme pode ser observado na Figura 9. Fato que o rotula como possível suspeito, conforme as regras fixas que estabelecemos para a arquitetura e representam indícios de ocorrência de LD.

Figura 8



Fonte: Elaborada pelo autor.

4.2 Próximas etapas da arquitetura de PLD

Para traçar o futuro dessa arquitetura e sua aplicabilidade no mercado, o projeto Simplificando Pagamentos Digitais precisa, primeiramente, estabelecer as bases de referência do que a sua arquitetura é capaz de oferecer ao mercado e, depois, determinar as expectativas e os objetivos futuros da arquitetura inovadora.

V1. Solucionar o problema da LD no pagamento de faturas de cartão de crédito

Atualmente, a arquitetura não utiliza o aprendizado da máquina, pois nossos desenvolvedores perceberam a necessidade de pilotar a prova de conceito com uma arquitetura simplificada. Tal escolha se deve ao baixo volume de dados utilizados para fins deste piloto e o escopo do protótipo restrito pelo qual se optou de início.

Contudo, é interesse do projeto que, ainda nesta etapa, seja implementado o ML para que a arquitetura – que hoje se mostra importante para as análises de PLD – passe a captar esses dados e apreender com eles para, assim, ser capaz de interromper a transação fraudulenta antes de sua ocorrência. Isso será feito por meio da análise dos dados da transação que, normalmente, passa pela Shipay no desempenho de suas atividades cotidianas.

Para melhor compreensão de como a arquitetura será capaz de detectar as transações suspeitas e, assim, mitigar os casos de LD no ecossistema do Pix, segue uma breve explicação quanto aos *scores* obtidos, após a análise dos dados:

1. Por meio dos grafos, é possível traçar as relações e a conexão entre os participantes da transação e, assim, destacar as diversas movimentações de ativos oriundos de LD na fase de ocultação.
2. Por meio da Lei de Benford, é possível, mediante a criação de um histograma com a análise do primeiro e do segundo dígitos, detectar anomalias probabilísticas de a transação ter sido originada pela movimentação de ativos na LD.
3. Por meio da análise do comportamento, é possível estabelecer perfis transacionais para cada usuário e, assim, detectar as transações anômalas do cotidiano de maneira personalizada.
4. Por meio dos *labels* (rótulos) fornecidos como *output* da arquitetura, é possível rotular e identificar as transações suspeitas e, assim, facilitar o trabalho do analista de PLD.

V2. Utilização da arquitetura no ecossistema do Pix

Conforme afirmado anteriormente, o Pix representa um avanço tecnológico no setor bancário e está promovendo mudanças no aspecto social ao digitalizar uma das mais antigas criações humanas: a moeda.

Contudo, as medidas de segurança no ambiente Pix ainda estão sendo testadas e desenvolvidas. Até mesmo as bases regulatórias estão em constante atualização. Nesse sentido, a arquitetura do projeto pode ser facilmente utilizada pelos participantes no ecossistema Pix devido à celeridade que será capaz de promover na detecção de LD, contribuindo como uma camada de segurança adicional.

V3. Aplicações no Open Finance

Com a criação do Open Finance e sua aplicação no cenário financeiro nacional, existem benefícios eminentes de sua utilização de maneira segura para o cliente que, ao compartilhar seus dados bancários, gera a oportunidade de que os bancos o conheçam melhor. Com um maior volume de dados, as instituições financeiras poderão oferecer as melhores condições de acordo com o perfil do consumidor.

Dessa forma, devido às sensibilidades dos dados financeiros, é importante garantir a segurança efetiva do sistema financeiro aberto. Portanto, a arquitetura de PLD do projeto será útil em função de sua moderna infraestrutura de anonimização dos dados.

Além disso, o volume de dados poderá ser, como explicado anteriormente, utilizado para traçar o perfil transacional de cada usuário. O compartilhamento desses dados entre as instituições financeiras contribuirá para a maior precisão da arquitetura do projeto na identificação de anomalias referente ao perfil transacional do usuário.

5 Características Inovadoras

Conforme afirmado na fundamentação teórica, existe um limite nos sistemas tradicionais de monitoramento em função da dificuldade de mantê-los e da dependência de regras facilmente testadas e contornadas pelos criminosos. Esses sistemas tendem a envolver processos de investigação altamente manuais, ou baseados em regras fixas, que resultam em lentidão e custo elevado.

Diferente dos sistemas tradicionais, e além dos mecanismos já existentes de segurança do ambiente Pix, a implementação de uma arquitetura de referência baseado em serviços do *Azure,* como *serverless,* banco de dados em grafo, para fins de PLD, amplia o horizonte de prevenção, além de ter aprendizado dinâmico e contínuo – em lugar de repressão somente – por meio da detecção de atividades potencialmente suspeitas não definidas por uma regra.

A presente proposta destaca e descreve quatro características inovadoras. A primeira é o reconhecimento da LD antes da ocorrência da transação. O sistema conta com o aprendizado e treinamento para identificação de possíveis práticas de LD em frações de segundo, o que, como benefício futuro, resulta em redução dos custos operacionais com PLD e alavancagem de sua efetividade. Todavia, é importante ressaltar que esta característica só será materializada quando a arquitetura V1 estiver concluída e acumulado volume de dados.

Em segundo lugar, é preciso enfatizar o fato de o ML permitir o aperfeiçoamento constante da ferramenta de PLD. Quanto maior o uso e aprendizado da máquina, maiores os ganhos em termos de melhoria do mecanismo de combate à LD. A curva de aprendizagem de máquina é exponencial em contraste com os métodos tradicionais, cujo fator humano envolve uma curva de aprendizagem linear e falível.

A terceira característica inovadora da proposta está na utilização do sistema na nuvem da Microsoft. Esse é o ambiente adequado para a construção de sistemas a serem integrados ao SPI do BC, pois fornece escalabilidade dos serviços de acordo com o volume de transações. Além disso, mantém um melhor controle dos custos, ao mesmo tempo que garante o desempenho necessário para o processamento dos sistemas. Tal capacidade elástica da nuvem do Azure torna-se ainda mais importante em função da imprevisibilidade do volume de transações do Pix (MITTELSTAEDT, 2021).

Finalmente, embora os serviços da nuvem do Azure não sirvam exclusivamente à PLD, ele foi aplicado recentemente nos EUA para este fim. A proposta de aplicação no Brasil não encontra precedentes, e tem o potencial de providenciar mais uma camada de segurança ao ambiente Pix, em conformidade com o proposto na Resolução n° 147/2021 do BCB.

6 Contribuições para o SFN

A indústria financeira é uma das mais visadas por *hackers* e tentativas de fraudes. A democratização da internet ocasionou inúmeros avanços no contexto social. Se, por um lado, vivemos a era dos dados, por outro lado, a ambição humana transgride qualquer barreira, fato que reforça a presença dos *hackers* e fraudadores em qualquer ambiente digital.

Apenas no ano passado, em decorrência da pandemia da covid-19, os crimes financeiros digitais de invasão de conta-corrente aumentaram 650% globalmente, e a fraude em *online banking* cresceu 250%, de acordo com o Relatório de Crimes Financeiros divulgado pela Feedzai, empresa de ciência de dados (CISO ADVISOR, 2021). Por isso, é tão importante o desenvolvimento de soluções de segurança que estejam em total conformidade com a regulamentação prevista pelo Banco Central e que acompanhem a evolução das tentativas de ataques cibernéticos que se sofisticam ao longo do tempo.

A partir das fundamentações e contextualizações apresentadas no presente relatório, fica evidente, portanto, que as novas medidas do Banco Central referentes ao Pix estão em congruência com o projeto proposto ao LIFT Lab. Com o fim de avançar nas medidas de segurança no ecossistema Pix, este projeto é compreendido como uma barreira de segurança que une o que há de mais moderno, em termos de infraestrutura, às necessidades de celeridade na detecção de LD para a efetividade do Pix em tempo hábil.

7 Conclusão

Desde sua adoção no final de 2020, o meio de pagamento digital instantâneo representado pelo Pix agregou mais facilidade, rapidez e segurança às transações. Entretanto, mesmo com os mecanismos de segurança estabelecidos pelo Banco Central, e não obstante o volume crescente de adesão à ferramenta, ainda existe uma parcela da população e das empresas (especialmente as mais maduras) que têm um senso de incerteza e insegurança quanto à utilização do ambiente Pix. Além disso, as práticas de LD, já presentes na realidade do sistema financeiro, viram no pagamento instantâneo a possibilidade de aperfeiçoar e escalar sua atuação.

Com isso, o ambiente Pix perde não apenas em credibilidade, mas existem perdas para todo o ecossistema e a sociedade na medida em que práticas LD minam recursos financeiros, morais e de manutenção da integridade, uma vez que têm origem e financiam atos ilícitos e danosos.

Dessa forma, com vistas a trazer mais inclusão, competitividade e transparência para que o meio de pagamento instantâneo cumpra os objetivos para os quais foi criado e evolua para trazer ainda mais benefícios, o projeto propõe a utilização dos serviços da nuvem do Azure para simplificar o trabalho do analista de PLD e prover mais uma camada de segurança robusta para as transações Pix. Tanto a implantação do sistema quanto sua efetiva utilização estão em conformidade e são suportadas por todos os requisitos regulatórios do Banco Central e da Lei Geral de Proteção de Dados (LGPD).

Inicialmente, o foco do projeto é a PLD, por meio do pagamento da fatura do cartão de crédito, e pretende agir de maneira preventiva ao evento de LD, identificando e, em uma evolução posterior, impedindo a ocorrência da transação em tempo real, além da possibilidade de sua aplicação no ecossistema do Open Banking. É importante destacar que, embora o referido escopo seja um ponto de partida na aplicação inédita de diferentes técnicas de aprendizado, e algoritmos estatísticos e de grafo no Brasil para fins de PLD, o horizonte de benefícios se estende a todo o ecossistema de serviços financeiros por meio da maturação e do aperfeiçoamento da ferramenta.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE CARTÕES DE CRÉDITO E SERVIÇOS – ABECS. **Meios eletrônicos de pagamento:** Balanço 2020. São Paulo, 2021. 46 slides: ppt. Disponível em: https://api.abecs.org.br/wp-content/uploads/2021/02/Apresentacao-Balanco-2020.pdf. Acesso em: 30 set. 2021.

ACCENTURE. **Inteligência artificial:** quanto sua empresa poderia avançar se todas as interações com a tecnologia fossem inteligentes? 2021. Disponível em: https://www.accenture.com/br-pt/insights/artificial-intelligence-index. Acesso em: 30 set. 2021.

AZURE MICROSOFT. **Azure stream analytics:** análise em tempo real sem servidor, da nuvem para borda. 2021. Disponível em: https://azure.microsoft.com/pt-br/services/stream-analytics/#overview. Acesso em: 30 set. 2021.

BANCO CENTRAL DO BRASIL – BCB. **Resolução BCB nº 1, de 12 de agosto de 2020**. Institui o arranjo de pagamentos Pix e aprova o seu Regulamento. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo= Resolução%20BCB&numero=1. Acesso em: 30 set. 2021.

BANCO CENTRAL DO BRASIL – BCB. **Estatísticas do Pix.** 2021a. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/estatisticaspix. Acesso em: 30 set. 2021.

BANCO CENTRAL DO BRASIL – BCB. **DICT API (1.2.0).** 2021b. Disponível em: https://www.bcb.gov.br/content/estabilidadefinanceira/pix/API_do_DICT_v1-2-0.html. Acesso em: 30 set. 2021.

BANCO CENTRAL DO BRASIL – BCB. **BC aprimora meios de pagamento eletrônicos.** 27 ago. 2021c. Disponível em: https://www.bcb.gov.br/detalhenoticia/17483/nota. Acesso em: 30 set. 2021.

BANCO CENTRAL DO BRASIL – BCB. **Resolução BCB nº 147, de 28 de setembro de 2021**. 2021d. Altera o Regulamento anexo à Resolução BCB nº 1, de 12 de agosto de 2020, que disciplina o funcionamento do arranjo de pagamentos Pix. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo= Resolu%C3%A7%C3%A3o%20BCB&numero=147. Acesso em: 30 set. 2021.

BANCO CENTRAL DO BRASIL – BCB. **Open Banking**. 2021e. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/openbanking. Acesso em: 20 out. 2021.

BONDY, John A.; MURTY, U.S.R. **Graduate Texts in Mathematics**: Graph Theory. [*S./l.*]: Springer, 2008. Disponível em: https://www.springer.com/gp/ book/9781846289699. Acesso em 20 out. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. LGPD. Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 30 set. 2021.

BRENOL, Lise. Open Banking e Open Finance: entenda a diferença**. Serasa Premium**, 2021. Disponível em: https://www.serasa.com.br/premium/blog/open-banking-e-open-finance-entenda-a-diferenca. Acesso em: 20 out. 2021.

CASTELLS, Manuel. **A era da informação, economia sociedade e cultura:** A sociedade em rede. 23. ed. São Paulo: Editora. Paz & Terra, 2013. 630 p. v. 1.

CISO ADVISOR. **Fraudes financeiras crescem 650% com uso maior de banco online e e-comerce.** 4 mar. 2021. Disponível em: https://www.cisoadvisor.com.br/ fraudes-financeiras-crescem-650-com-uso-maior-de-banco-online-e-e-commerce/. Acesso em: 30 set. 2021.

CNSEG. **A inteligência artificial e os processos de prevenção à lavagem de dinheiro.** 4 set. 2019. Disponível em: https://cnseg.org.br/noticias/a-inteligencia-artificial-e-os-processos-de-prevencao-a-lavagem-de-dinheiro.html. Acesso em: 30 set. 2021.

CONSELHO DE CONTROLE DE ATIVIDADES FINANCEIRAS – COAF. **O que é lavagem de dinheiro e financiamento ao terrorismo.** 2020. Disponível em: https://www.gov.br/coaf/pt-br/assuntos/o-sistema-de-prevencao-a-lavagem-de-dinheiro/o-que-e-o-crime-de-lavagem-de-dinheiro-ld. Acesso em: 30 set. 2021.

DEUTSCHE BANK. **The future of payments part 2:** moving to digital wallets and the extinction of plastic cards. Jan. 2020. Disponível em: https://www.dbresearch. com/PROD/RPS_EN-PROD/PROD0000000000504508/The_Future_of_Payments_-_Part_II__Moving_to_Digita. pdf?undefined&realload= gxFq0bRYLoVqkjhfBOGb ~j69f2v2sDdL8O7ZD6ieeJgxOJoEKW/eiRZ5O4R8kMmf. Acesso em: 30 set. 2021.

FEDERAÇÃO BRASILEIRA DE BANCOS – FEBRABAN. **Pesquisa Febraban de tecnologia bancária 2021.** 2021. 70 slides: ppt. Disponível em: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/pesquisa-febraban-relatorio.pdf. Acesso em: 30 set. 2021.

FLETES, Manuel Bermejo. **Pix e o risco do crime de lavagem de dinheiro.** 24 nov. 2020. Disponível em: https://www.ipld.com.br/editorial/pix-e-o-risco-do-crime-de-lavagem-de-dinheiro/. Acesso em: 30 set. 2021.

GOUVEIA, Caroline Jaszczuk. **Tipologia de lavagem de dinheiro:** saldo credor em cartão de crédito. 15 mar. 2021. Disponível em: https://www.ipld.com.br/editorial/ tipologia-de-lavagem-de-dinheiro-saldo-credor-em-cartao-de-credito/. Acesso em: 30 set. 2021.

INFRA NEWS TELECOM. Tentativas de fraude com serviços financeiros crescem 457% no Brasil na pandemia. **Redação Infra News Telecom**, 2021. Disponível em: https://infranewstelecom.com.br/tentativas-de-fraude- com-servicos-financeiros-crescem-457-no-brasil-durante-a-pandemia/. Acesso em: 30 set. 2021.

LIMA, Marco Antônio Ferreira. O Pix diante dos crimes patrimoniais. **Revista Consultor Jurídico**, 14 ago. 2020. Disponível em: https://www.conjur.com.br/2020-out-14/marco-antonio-lima-pix-diante-crimes-patrimoniais. Acesso em: 30 set. 2021.

LIMA, Rafael Sousa; SERRANO, André Luiz Marques; CUPERTINO, Cesar Medeiros. Contabilidade Forense e Grafos no Combate à Lavagem de Dinheiro. *In*: USP INTERNATIONAL CONFERENCE IN ACCOUNTING: "ACCOUNTING AS A GOVERNANCE MECHANISM", 20., 2020, São Paulo. **Anais [...]. São Paulo:** Fipecafi, 2020. Disponível em: https://congressousp.fipecafi.org/anais/20UspInternational/ArtigosDownload/2205.pdf. Acesso em: 20 out. 2021.

MICROSOFT. **Open Finance:** arquiteturas de referência do Microsoft Azure para suportar os clientes nas ondas do sistema financeiro aberto. 2021. Disponível em: https://www.microsoft.com/cms/api/am/binary/RWFOzl. Acesso em: 20 out. 2021.

MITTELSTAEDT, Fabio. **Microsoft desenvolve arquitetura inteligente do Pix na nuvem para superar as expectativas do ecossistema bancário.** 18 fev. 2021. Disponível em: https://cloudblogs.microsoft.com/industry-blog/pt-br/financial-services/2021/02/18/microsoft-desenvolve-arquitetura-inteligente-do-pix-na-nuvem-para-superar-as-expectativas-do-ecossistema-bancario/. Acesso em: 30 set. 2021.

STATISTICAL ANALYSIS SYSTEM – SAS. **Como IA e Machine Learning estão redefinindo práticas anti-lavagem de dinheiro.** 2020. Disponível em: https://www.sas.com/content/dam/SAS/documents/marketing-whitepapers-ebooks/sas-whitepapers/pt/como-iaeml-estao-redefinindo-praticas-aml.pdf. Acesso em: 30 set. 2021.

SILVA, Ricardo Antunes; DA CRUZ, Caroline Quaresma Piccinato. O impacto do novo ecossistema democrático de pagamento instantâneo (Pix) no sistema financeiro nacional. **Unisul de Fato e de Direito – Revista Jurídica da Universidade do Sul de Santa Catarina**, v. 10, n. 21, p. 195-208, 2020. Disponível em: https://www.researchgate.net/publication/345414886_O_IMPACTO_DO_NOVO_ECOSSISTEMA_DEMOCRATICO_DE_PAGAMENTO_INSTANTANEO_PIX_NO_SISTEMA_FINANCEIRO_NACIONAL. Acesso em: 30 set. 2021.

TAYAR, Gustavo; FONTES, Cristiano; CRADDOCK, Christopher; MURATORE, Camila. **Pagamentos como alavanca de crescimento.** 21 maio 2021. Disponível em: https://www.mckinsey.com.br/our-insights/pagamentos-como-alavanca-de-crescimento. Acesso em: 30 set. 2021.

UOL. **PIX reduzirá pagamentos em dinheiro à metade do que é hoje em 10 anos.** 28 jul. 2020. Disponível em: https://6minutos.uol.com.br/economia/pix-reduzira-pagamentos-em-dinheiro-a-metade-do-que-e-hoje-em-10-anos/. Acesso em: 20 out. 2021.

VALENTE, Jonas. Brasil se destaca em uso de pagamentos digitais, segundo pesquisa. **Repórter Agência Brasil**, Nova Iorque, 1º ago. 2019. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2019-08/mais-de-60-dos-brasileiros-usam-meios-digitais-para-pagamentos. Acesso em: 30 set. 2021.

VAREJO S.A. **Circulação de dinheiro em espécie se reduz nos primeiros meses do Pix.** 18 jun. 2021. Disponível em: https://cndl.org.br/varejosa/circulacao-de-dinheiro-em-especie-se-reduz-nos-primeiros-meses-do-pix/. Acesso em: 30 set. 2021.

WIKIPEDIA. **Teoria dos Grafos**. 30 set. 2021a. Disponível em: https://pt.wikipedia.org/wiki/Teoria_dos_grafos#Hist%C3%B3rico. Acesso em 20 out. 2021.

WIKIPEDIA. **Lei de Benford**. 29 jul. 2021b. Disponível em: https://pt.wikipedia.org/wiki/Lei_de_Benford. Acesso em: 20 out. 2021.