LIFT *papers*

REVISTA DO LABORATÓRIO
DE INOVAÇÕES FINANCEIRAS
E TECNOLÓGICAS

2ª EDIÇÃO

Fenasbac | BANCO CENTRAL DO BRASIL

LIFT Papers

Revista do Laboratório de Inovações Financeiras e Tecnológicas

Volume 2 • Número 1 • Maio 2020

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

FinID – Gestão de Identidades Financeiras Descentralizadas

Fernando Marino [*], *Lucas Mori* [**], *MSc. Reynaldo Formigoni* [***], *Sérgio Ribeiro* [****], *Vitor Oliveira* [*****]

A implementação do sistema financeiro aberto (***open banking***) e da nova plataforma de pagamentos instantâneos será uma evolução do setor financeiro brasileiro que acontecerá no curto ou médio prazo. Um grande desafio associado a esta evolução é a proteção e a portabilidade de dados pessoais dos clientes, desde informações cadastrais a dados relativos a contas de depósito e operações de crédito.

Este projeto visa criar uma identidade única, portável e segura para as instituições financeiras, com o cliente no controle dos seus próprios dados pessoais e viabilizando o acesso facilitado de contratação de serviços financeiros. A solução permitirá também que, por meio dessa identificação financeira e suas conexões, os clientes possam inicializar transações, como por exemplo, transferências bancárias e pagamentos, para outros usuários ou instituições da rede da solução FinID.

[*] fmarino@cpqd.com.br
[**] lmori@cpqd.com.br
[***] reynaldo@cpqd.com.br
[****] sribeiro@cpqd.com.br
[*****] vpoliveira@cpqd.com.br

Introdução

A transformação digital está ocorrendo de forma rápida e mudando profundamente a forma com a qual se interage em vários setores da economia, com destaque para o setor financeiro, digitalizando e automatizando de forma sem precedentes os respectivos processos.

Nesse contexto, este projeto tem por objetivo desenvolver uma solução de gestão de identidades financeiras descentralizada, contemplando:

- a criação e o gerenciamento de identidade;
- o credenciamento digital de contas, aqui denominado *onboarding*;
- a autenticação de identidades e informações.

Para atender aos objetivos propostos, seguem os principais endereçamentos:

• **Desburocratizar o processo de identificação para o tomador final, possibilitando a utilização de uma credencial financeira única para a identificação e acesso a serviços financeiros**. Isso facilitará o acesso dos tomadores finais aos serviços financeiros ofertados pelas instituições financeiras, permitindo que os serviços contratados sejam tratados de forma personalizada para cada cliente; seja possível, dentre outras coisas, aplicar uma tarifação transparente e justa por serviços de fato contratados e que se ofereça um atendimento exclusivo, que hoje é cenário distante para a maioria dos consumidores.

• **Dar poder ao tomador final para controlar o uso de seus dados financeiros** de modo a permitir que o tomador final possa gerenciar com quais instituições financeiras deseja compartilhar seus dados, quais dados e para quais fins esses dados serão utilizados, por meio de notificações e requisições de consentimento ao acesso às informações gerenciadas pela solução.

• **Facilitar e automatizar o processo de admissão de novos clientes para instituições financeiras,** também denominado como *onboarding*, por meio do gerenciamento descentralizado de chaves e a utilização de credenciais únicas para diversos setores. Isso auxiliará principalmente o processo de *onboarding* para as *startups* do setor financeiro (as denominadas *fintechs*), uma vez que, por serem novas, emergem sem carteira de clientes. A *fintech* que participar da rede do FinID poderá considerar como potenciais clientes todos os tomadores de serviço que possuírem uma credencial válida.

• **Viabilizar a implantação do conceito de *Know your Customer* – KYC (conheça seu cliente)**. Uma vez que as instituições financeiras poderão, por meio da solução FinID, solicitar diretamente ao tomador final suas credenciais verificáveis emitidas por outras instituições - sejam elas financeiras ou não – também poderão aferir a posse, o emissor e a autenticidade das informações, tendo acesso às informações pertinentes de cada um de seus clientes. Isso permitirá um conhecimento maior e mais bem definido do perfil dos usuários de seus serviços, possibilitando assim a criação de serviços específicos ou customizados para o tomador dos serviços financeiros, melhorando, portanto, os relacionamentos no Sistema Financeiro Nacional (SFN).

• **Transformar os meios de credenciamento e autenticação no setor financeiro**. O desenvolvimento de uma solução descentralizada, baseada em *blockchain*, gera um mecanismo confiável para a emissão de credenciais verificáveis para os tomadores finais do Sistema Financeiro Nacional, viabilizando a automatização dos processos de autenticação e autorização com a utilização de tais credenciais sem a necessidade de um serviço terceiro ou autoridade central. Além disso, a solução visa facilitar e automatizar o processo de *onboarding* digital dos consumidores junto às instituições financeiras, permitindo que essas instituições possam focar no desenvolvimento de novos serviços digitais para seus consumidores em vez de gastar tempo e recurso no desenvolvimento dessas tecnologias e entregando uma nova forma de credenciamento para os tomadores de serviços financeiros, obtendo, portanto, a desburocratização e alternativas para o relacionamento entre essas partes no setor financeiro.

1 Objetivos

Atualmente, para poder usufruir de produtos ofertados por instituições financeiras, faz-se necessário ao consumidor brasileiro criar uma identificação em cada instituição com as quais queira ter vínculo. Por vezes, esses processos são entediantes, burocráticos e longos.

É comum encontrar casos em que um produto ofertado por uma instituição financeira, que é do interesse e perfil de um determinado consumidor, não seja adquirido pelo simples fato de o cidadão não possuir uma identificação válida junto à instituição proponente, criando assim uma barreira virtual para a realização de bons negócios tanto para o consumidor quanto para as instituições financeiras.

O processo de identificação utilizado pelas instituições financeiras é anacrônico e demanda que o potencial consumidor passe por um processo de cadastramento em cada instituição com a qual deseje se relacionar. Fazendo uma analogia com um viajante, seria como se este tivesse que tirar um passaporte específico, para cada país que desejasse visitar.

O FinID visa fornecer uma identidade digital financeira única, descentralizada, segura, aderente às leis de proteção de dados pessoais (tais como Lei Geral de Proteção da Dados e General Data Protection Regulation), podendo ser interoperável com soluções de várias organizações. Trata-se de uma solução segura, confiável, sob controle do consumidor e que visa facilitar o acesso a produtos financeiros de instituições com as quais ele não necessariamente tenha vínculo, estimulando a competitividade do mercado financeiro.

Como objetivos específicos, a solução deverá:

a) Ao tomador de serviços financeiros:

- Fornecer identidade digital financeira, que será emitida por uma instituição de sua confiança, por meio de processo eletrônico que verifique a autenticidade da identidade solicitada pelo consumidor, que tenha seus dados comuns ao setor financeiro e que sua exposição e uso no mercado esteja sob seu controle.
- Fornecer identidade digital financeira que possa: (i) evoluir conforme seu uso e relacionamento com organizações e contatos, (ii) gerar registros de informações a

serem apresentadas, com o seu consentimento, para instituições financeiras, a fim de disponibilizar uma análise de crédito segura.
- Criar relacionamentos com instituições financeiras com as quais o tomador nunca teve uma conexão, de forma amigável, intuitiva e ágil, com segurança, controle e confiança.
- Certificar que a entidade financeira com a qual está prestes a se relacionar é de fato a instituição que acredita ser e não um possível embuste digital.
- Iniciar um relacionamento financeiro digital seguro com outra pessoa, para realização e consolidação de pagamentos instantâneos.
- Oferecer um novo modelo de negócio onde o consumidor possa receber uma receita pelo compartilhamento dos seus dados pessoais, ou seja, uma parcela dos eventuais serviços ou taxas para o acesso a informações de sua identidade, como por exemplo, seu *score* de crédito, criando assim um modelo "ganha-ganha" para informações, o que até então é explorado e comercializado sem seu consentimento ou benefício.

b) Ao fornecedor de serviços financeiros:

- Oferecer maior capilaridade aos seus serviços financeiros, uma vez que eles contemplarão, além de seus clientes cativos, aqueles que possuam uma identidade financeira digital válida.
- Analisar de forma simples, transparente e confiável as informações financeiras da identidade digital dos tomadores de serviços financeiros, conseguindo assim conhecer melhor o perfil, padrões e reputação desses tomadores.
- Trazer mais transparência aos seus novos consumidores, comunicando-se com eles solicitando seu consentimento ao acesso às informações necessárias.
- Poder evoluir a identidade financeira dos tomadores, gerando novas informações para eles, criando maior laço de confiança e utilidade à informação gerada para o cidadão.
- Quando cabível, viabilizar a criação de produtos específicos para os consumidores, baseados nas necessidades e perfis de cada cliente, podendo, assim, realizar cobranças de taxas de acordo com a real necessidade dos serviços adquiridos.
- Desburocratizar de maneira geral processos, como o credenciamento de novos consumidores, oferecendo maior agilidade na análise de informações dos consumidores que agora vão além daquelas geradas pela própria instituição.
- Participar dos ganhos de produtos adquiridos por meio da utilização das credenciais que por ela forem emitidas, por meio de comissão ou afins, considerando que a instituição financeira também seja uma emissora de credenciais verificáveis. Por exemplo, a entidade emissora poderá receber uma comissão por um contrato de outra instituição cuja celebração tenha utilizado a credencial por ela emitida.

c) Ao emissor de identidades financeiras:

- Proporcionar o desenvolvimento de novos modelos de negócio de emissão de credenciais, desde identidades básicas para acesso e usufruto de serviços ordinários,

até análises mais detalhadas para emissão de identidades a serem usadas no mercado financeiro.
- Oferecer serviços de monitoramento e análise das informações geradas pelas instituições financeiras a fim de criar classificadores para análise de crédito e reputação da identidade, em informações geradas pelas mais diversas instituições financeiras, aumentando consideravelmente a acurácia dessa informação.
- Oferecer serviços para *backups* de credenciais financeiras, que possam garantir a recuperação dessas credenciais em situações de crises, tais como perda, dano ou demais sinistros com dispositivos móveis pessoais pelos quais os consumidores façam o gerenciamento de suas identidades.
- Oferecer serviços de armazenamento de alta disponibilidade para as credenciais, visando segurança e privacidade das informações, garantindo também que elas fiquem disponíveis aos agentes financeiros autorizados.

d) Ao Banco Central do Brasil:

- Realizar a governança da rede *blockchain*, junto às demais instituições financeiras e regulatórias, a fim de regulamentar e agenciar a gestão e o uso dessas identidades digitais financeiras, com o objetivo de proteger o mercado financeiro, trazendo ganhos aos consumidores brasileiros.
- Ser protagonista no mercado financeiro ao trazer as regras para a desintermediação e para o uso do controle descentralizado dessas identidades, criando maior competitividade no mercado financeiro.
- Propiciar maior agilidade na rastreabilidade de valores e ativos entre as instituições e consumidores, trazendo assim maior eficiência, confiança e transparência ao setor financeiro.

2 Fundamentação teórica

A fundamentação teórica da solução FinID é a identidade digital descentralizada, também conhecida como identidade digital autossoberana. Trata-se de uma evolução da identidade digital federada e tem como principais características:

• a não existência de uma autoridade central como soluções anteriores de identidade digital;
• ser baseada em *Distributed Ledger Technology* (DLTs) ou Tecnologia de Livro de Registros

Distribuída;

• ser centrada no usuário uma vez que ele define quais, como e onde os seus dados serão utilizados;
• apresentar elevados níveis de segurança e privacidade;

• ser compatível com o Regulamento Geral de Proteção de Dados da União Europeia (RGPD ou GDPR em inglês) e Lei Geral de Proteção de Dados Pessoais (LGDP), versão brasileira de Lei Geral de Proteção de Dados, uma vez que dados pessoais não são colocados no *ledger*;
• apresentar-se como camada de identidade da internet que não foi projetada na sua origem.

Um dos pilares do funcionamento das soluções atuais de identidade digital descentralizada é a DLT. Neste capítulo serão apresentados os conceitos, iniciativas, aspectos legais e de padronização das principais tecnologias utilizadas na solução FinID, com ênfase na identidade digital descentralizada e DLTs.

2.1 Conceitos da *Distributed Ledger Technology*

A rigor, pode-se dizer que DLT é uma combinação de várias tecnologias (ou uma metatecnologia), algumas com mais de dez anos, que suportam um sistema distribuído de base de dados, mantido e gerido de forma compartilhada e descentralizada por meio de uma rede *peer-to-peer* – P2P, na qual todos os participantes são responsáveis por armazenar e manter a base de dados de forma confiável e segura.

Atualmente, existem várias definições de DLTs. Segundo o Banco Mundial, DLT refere-se a uma abordagem inovadora e de rápida evolução para registrar e compartilhar dados em vários bancos de dados (ou *ledgers*) distribuídos. Essa tecnologia permite que transações e dados sejam gravados, compartilhados e sincronizados em uma rede distribuída entre os diferentes participantes da rede. *Blockchain* é um tipo específico de DLT que armazena e transmite dados em pacotes chamados "blocos" que são conectados entre si em uma "cadeia" digital. As cadeias de blocos empregam métodos criptográficos e algorítmicos para registrar e sincronizar dados em uma rede de maneira imutável (WORD BANK GROUP, 2017).

Na visão da *International Telecommunication Union* (ITU), DLTs, cuja implementação mais proeminente é a *Blockchain*, permitem que nós em uma rede distribuída cheguem a um acordo e registrem informações sem a necessidade de uma autoridade central. *Blockchain* é um tipo de DLT composta de dados gravados digitalmente organizados como uma cadeia de blocos em crescimento sucessivo, com cada bloco criptograficamente vinculado e reforçado contra adulteração e revisão (ITU-T, 2019).

Segundo o *Cambridge Centre for Alternative Finance*, a tecnologia de contabilidade distribuída (ou DLT) estabeleceu-se como um termo genérico para designar sistemas multipartes que operam em um ambiente sem operador ou autoridade central, apesar das partes que podem não ser confiáveis ou mal-intencionadas ("ambiente adversário"). A tecnologia *Blockchain* é frequentemente considerada um subconjunto específico do universo DLT, que utiliza uma estrutura de dados específica que consiste em uma cadeia de blocos de dados vinculados por meio de uma técnica de criptografia denominada hash (RAUCHS, 2018).

A metatecnologia de *blockchain* foi construída tendo em mente quatro principais características arquiteturais: (i) segurança das operações, (ii) descentralização de armazenamento e computação; (iii) integridade de dados e (iv) imutabilidade de transações.

Dito de outra forma, *blockchain* é uma "*ledger of facts*" replicada em computadores que participam de uma rede *peer-to-peer*, onde (NAKAMURA, 2019):

- o *ledger* é um livro de registros digital, no qual, uma vez validado um registro, este nunca mais poderá ser apagado;
- um fato (*fact*) pode significar várias coisas, desde uma transação monetária, a um conteúdo de determinado documento, ou até mesmo um programa de computador, contendo, em algumas plataformas, até uma base de dados pequena;
- os membros participantes da rede podem, ou não, ser anônimos e são chamados *peers* ou "nós";
- toda operação ou transação dentro do *ledger* é protegida por tecnologias criptográficas de assinatura digital, inclusive para identificar os nós emissores e receptores das transações;
- quando um nó deseja adicionar ao *ledger* um fato novo, é necessário um consenso entre todos ou alguns nós previamente determinados da rede, para decidir se um fato pode ser registrado no *ledger*;
- havendo consenso, o fato será escrito e nunca mais poderá ser apagado, em tese, um processo levemente semelhante à escritura e registro de um imóvel no Brasil.

Conforme apresentado na figura 1, uma rede *blockchain* possui os seguintes elementos essenciais:

- **fato (*fact*)**: pode ser uma transação, um conteúdo digital ou um programa de computador, este último também denominado contrato inteligente (*smart contract*);
- **bloco:** conjunto de fatos, geralmente em um número fixo predefinido;

• **cadeia de blocos (*blockchain*)**: conjunto de blocos encadeados (conectados um a um) seguindo uma lógica matemática, ou seja, não são independentes.

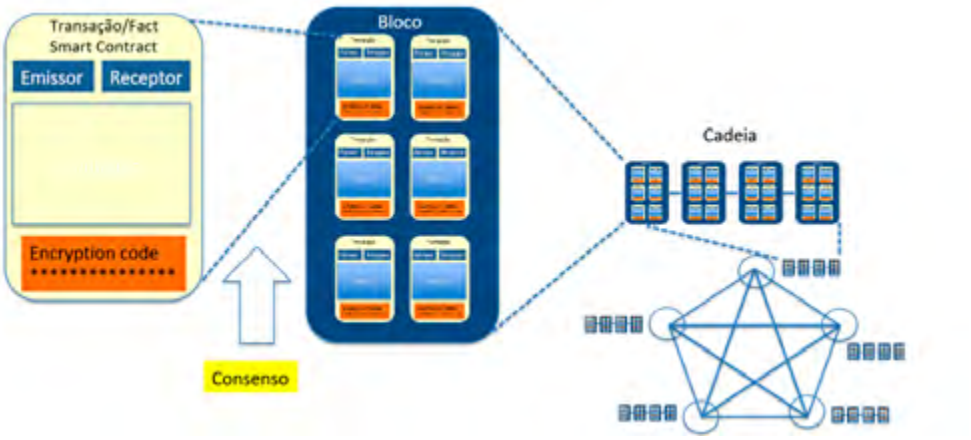

Figura 1 – Fato, bloco e cadeia de blocos

Do ponto de vista de aplicação, *blockchain* passou por uma grande evolução com a possibilidade de uso dos contratos inteligentes que são programas de computador replicados e executados por todos os nós da rede, ou por um conjunto predeterminado de nós denominados validadores. Aplicações baseadas em contratos inteligentes são chamadas *Decentralized Applications* ou Dapps.

Atualmente, as redes DLTs são classificadas considerando-se dois aspectos, conforme apresentado na figura 2:

• acesso aos serviços suportados: o acesso poderá ser (i) público, ou seja, qualquer usuário poderá ter acesso ao serviço, ou (ii) privado, ou seja, o usuário, para participar da rede na condição de usuário do serviço, deverá passar por um processo de cadastro e subsequente análise e aprovação feita pela entidade que governa a rede;

• participação na rede: se houver necessidade de algum tipo de autorização para a pessoa (física ou jurídica) se tornar um nó da rede, seja como validador de transações ou mero observador, tem-se então (i) uma rede permissionada, caso contrário será (ii) uma rede não permissionada.

Figura 2 – Classificação das Redes DLTs.

A maioria das redes que suportam as transações de criptomoedas (Bitcoin, Ether e Ripple, por exemplo) são de acesso público e não permissionadas, apresentando as seguintes características:

- qualquer pessoa (física ou jurídica) pode participar da rede como nó validador da rede sem permissão;
- qualquer pessoa pode baixar o código e começar a executar um nó em seu dispositivo local, validando transações na rede, participando do processo de consenso;
- qualquer usuário pode enviar transações através da rede e esperar vê-las incluídas no *ledger* se elas forem válidas;
- qualquer usuário pode ler transações no *ledger*. As transações são transparentes, porém são anônimas ou pseudoanônimas.

Grande parte das soluções do mundo corporativo está usando redes permissionadas (*Hyperledger Fabric* e Corda, por exemplo) e de acesso privado, apresentando as seguintes características:

Duas inciativas globais muito relevantes se encaixam no grupo das redes permissionadas de acesso público. A mais conhecida é a criptomoeda Libra que será lança em 2020. Prevê-se que nos primeiros cinco anos de funcionamento, o acesso à rede para se tornar um nó validador será no modo permissionado, porém o acesso às carteiras será público desde o seu início (LIBRA, 2019). Toda a governança da Libra é feita pela Associação Libra, que é uma organização de membros independente e sem fins lucrativos com sede em Genebra, na Suíça.

A segunda iniciativa é a Sovrin, rede que suporta aplicações de identidade digital autossoberana desenvolvidas sobre o *framework* Indy, do projeto Hyper*ledger*. O acesso às aplicações pode ser público, ou seja, o usuário pode baixar o aplicativo da carteira em seu *notebook* ou *smartphone* e sair usando. Porém, os nós que processam os indicadores descentralizados constituem uma rede permissionada. Atualmente, o CPQD é um nó validador da rede Sovrin.

A classificação da solução FinID dependerá do modelo de negócio e de operação a ser adotado. Em relação ao acesso à rede, ela será permissionada, podendo inclusive executar suas aplicações na rede Sovrin (depende do modelo de negócio). Em relação ao acesso ao serviço, muito provavelmente será, pelo menos num primeiro momento, de acesso privado (SOVRIN, 2018).

Acredita-se que a DLT tem o potencial de ser a força motora que irá democratizar a economia mundial, e será considerada uma das tecnologias mais importantes na história do presente século. Pelo modelo desenvolvido, nenhuma autoridade central é necessária, criando assim, a maior quebra de paradigma à qual precisamos nos habituar e entender, pois o método de consenso utilizado para registrar as transações no livro de registros (*ledger*) será decentralizado (TAPSCOTT, 2016).

2.2 Blockchain e a segurança

Apesar dos problemas de segurança, divulgados, utilizando DLTs, mais especificamente *blockchain*, seja na operação de criptomoedas ou em iniciativas como da DAO[6] (FALKON, 2017), vale ressaltar que os ataques foram direcionados às aplicações que utilizam o *blockchain*, e não especificamente à tecnologia ou ainda ao algoritmo empregado.

Além disso, observa-se que os ataques bem-sucedidos, relatados até o momento, a plataformas baseadas em *blockchain*, como por exemplo Bitcoin, ocorreram devido a vulnerabilidades nas aplicações e não no core da tecnologia *blockchain* propriamente dito. Sendo assim, com relação ao aspecto de segurança, até o presente momento, não são conhecidas vulnerabilidades contra a construção empregada e algoritmos utilizados nativamente no *blockchain*, podendo-se assim dizer que a segurança ainda é um dos pontos fortes da solução.

[6] DAO – *Decentralized Autonomous Organization*

Para que isso ocorra, o algoritmo prevê que, no processo de inserção de novos blocos, um novo bloco, composto por um conjunto de transações, seja ligado criptograficamente aos blocos anteriores por meio de um processo chamado de validação, que, nos casos específicos de criptomoedas, Bitcoin, por exemplo, é conhecido como mineração. O processo é computacionalmente intensivo e é o que faz com que seja improvável que modificações maliciosas possam ser realizadas por um atacante.

2.3 Camadas de segurança de um framework DLT

Um *framework* DLT e as aplicações construídas com ele devem adotar a segurança em camadas. Há seis camadas de segurança a serem consideradas. Essas camadas são o resultado da compilação de boas práticas presentes na área de segurança da informação e são apresentadas na figura 3 e descritas a seguir (RIBEIRO, 2019).

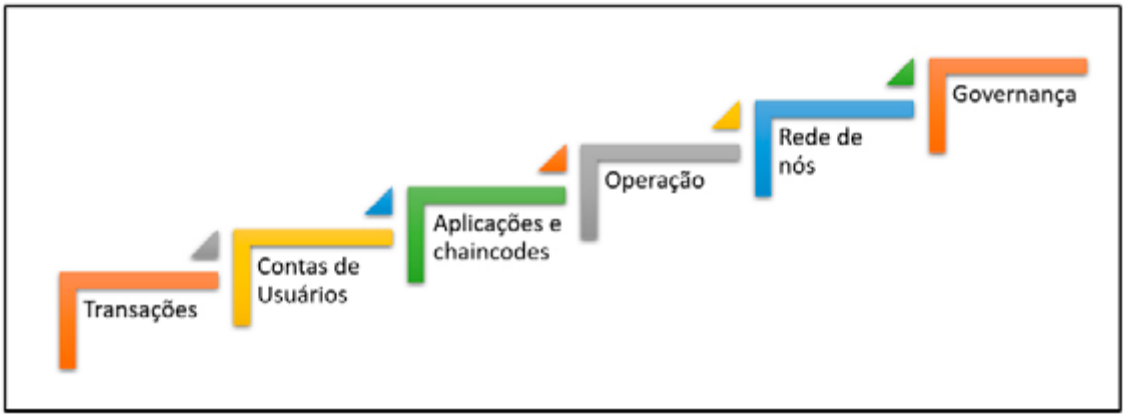

Figura 3. Camadas de segurança para um desenvolvimento *blockchain*.

1. A camada fundamental é a **primeira camada**, nela está a segurança da transação, requisito mínimo sem o qual o DLT não faz sentido. O DLT deve validar as transações com confiança e previsibilidade ao final do consenso. O consenso vai confirmar a finalidade e a imutabilidade de transação.

Trata-se de proteções sintática e estrutural para as transações e os blocos que as contêm. Essas proteções não impedem fraudes semânticas associadas à lógica da aplicação.

2. A **segunda camada** oferece segurança da conta de usuário. A conta do usuário é geralmente gerenciada pelo próprio usuário em aplicativos de uso pessoal (*eWallets*). Muitas vezes, a proteção da conta do usuário é confundida com a segurança do *software* cliente.

Essa camada de segurança é influenciada por dois fatores: a conscientização dos usuários no uso seguro da tecnologia, e a implementação correta dos mecanismos de segurança para dispositivos móveis e sistemas *web*.

3. A **terceira camada** contempla a segurança da aplicação e dos *chaincodes*. Fazem parte dessa camada as boas práticas de desenvolvimento seguro de *software*, incluindo a

codificação segura de *smart contracts* e a definição de requisitos de segurança, avaliação de arquitetura e testes de segurança da aplicação.

4. A **quarta camada** atende a segurança de implantação e de operação da aplicação. Fazem parte dessa camada os testes de aceitação e homologação da aplicação e dos *chaincodes* antes da implantação em produção. Uma vez no ambiente de produção, a aplicação deve ser monitorada para detecção de anomalias de funcionamento e comportamento. Monitoramentos avançados podem até detectar fraudes.

5. A **quinta camada** cobre a segurança da rede P2P de seus nós. Nessa camada, os mecanismos de proteção tradicionais das redes de computadores (tais como sistemas de *firewall*, IDS, IPS, etc.) podem ser aplicados para proteção dos nós da rede P2P do DLT. Além disso, proteções específicas devem ser aplicadas para a segurança do protocolo de comunicação e de consenso. Ainda, deve ser observada a quantidade mínima necessária de nós disponíveis para garantir o consenso.

6. **A sexta camada** de segurança se refere à governança da aplicação e do DLT. Essa camada abriga aquelas decisões sobre a estrutura e projeto do DLT, que afetam o funcionamento com segurança, incluindo ainda controles antifraude, auditoria, privacidade e até conformidade a normas e padrões específicos do nicho de aplicação.

2.4 Identidade digital e DLTs

As aplicações relacionadas à identidade digital utilizando DLT permitem a verificação, autorização e gerenciamento de identidade inalterados, resultando em eficiências significativas e redução de fraudes.

DLT fornece o mecanismo ideal para identidades digitais. Enquanto as identidades digitais estão emergindo como uma parte inevitável do nosso mundo conectado, a forma como protegemos nossas informações *on-line* está sendo submetida a um intenso escrutínio. Os sistemas de identidade baseados em DLT podem fornecer uma solução para esse problema com criptografia rígida e *ledger*s distribuídos.

Os recentes casos de violações de dados, vazamentos e uso indevido dominaram as manchetes ao longo do ano passado, trazendo nova proeminência às questões de proteção

de dados pessoais. O escândalo do *Facebook-Cambridge Analytica*, a violação de dados do provedor LocationSmart e outros levaram os usuários e os reguladores a examinarem mais de perto como as empresas privadas estão lucrando – e às vezes abusando – dos dados de identidade do cliente. No campo da DLT para identidade, vimos as empresas reagirem com um modelo de negócios relativamente novo: o mercado de identidades pessoais (OWI, 2019).

Um pequeno, mas crescente contingente de empresas e, principalmente *startups*, está desenvolvendo serviços para mudar a monetização de dados pessoais de empresas digitais e anunciantes para os próprios usuários, que são os reais donos da identidade. Esses *players* dão aos consumidores mais controle sobre como eles "usam" seus dados, combinando funções de identidade e criptomoeda, de forma que os usuários são compensados por atributos individuais que escolhem compartilhar com empresas privadas. *Startups* como Datum, DataVest e Wibson, por exemplo, surgiram em 2018 com base nessa funcionalidade. Ainda outras empresas, como Civic e Procivis, planejam lançar um novo mercado de *token* totalmente voltado para transações de dados pessoais (OWI, 2019).

Mercados de dados pessoais baseados em DLTs são uma proposta intrigante, mas exigem que uma base de consumidores particularmente importante, motivada e digitalmente experiente utilize e consequentemente mude significativamente a economia de dados pessoais.

2.5 Identidade digital autossoberana

Mais de 25 anos se passaram desde que Peter Steiner mostrou ao mundo pela primeira vez que "na Internet, ninguém sabe que você é um cachorro" (Figura 4), mas esse famoso *cartoon* ainda continua atual e válido, pois representa o desafio de identificar pessoas *on-line*.

Figura 4. Na Internet, ninguém sabe que você é um cachorro. Peter Steiner.

Hoje, estamos muito longe da visão de diretórios públicos que era a expectativa da criptografia de chave pública nos anos 1970 ou do grande esquema de certificação hierárquica previsto nos anos 1980. O gerenciamento de identidades (IdM) na Internet ainda conta com o que Cameron (2005), há mais de uma década, chamou de uma "colcha de retalhos de identidades únicas", compreendendo vários tipos de sistemas IdM que são restritos a domínios específicos e não interagem entre si.

Os modelos centralizados de IdM enfrentam atualmente inúmeros desafios, devido à crescente legislação relacionada às violações de dados, que levam a danos de reputação, fraude de identidade, mas, acima de tudo, a uma perda de privacidade de todos os envolvidos. Esses eventos recorrentes destacam a falta de controle e de gestão que os usuários experimentam com suas identidades digitais.

A pesquisa de abordagens alternativas à IdM está sendo conduzida por iniciativas que buscam ampliar a confiabilidade e o alcance das formas digitais de identidade. A Estratégia Nacional dos Estados Unidos para Identidades Confiáveis no Ciberespaço visa acelerar o desenvolvimento de novas tecnologias que podem aumentar a confiança nas transações *on-line* (THE WHITE HOUSE, 2011). Além disso, o ID2020 procura alavancar tecnologias digitais emergentes para expandir o alcance de identidades legais (espelhando as metas das Nações Unidas de "fornecer até 2030 identidade digital para todos, incluindo o registro de nascimento" (UNITED NATIONS, 2015). O surgimento do Bitcoin (NAKAMOTO, 2008) também inspirou um novo pensamento sobre a identidade digital, devido à sua subjacente tecnologia de *ledger* distribuída (DLT), que não precisa de uma autoridade central para validar as transações.

Assim, uma rede globalmente descentralizada é capaz de chegar a um consenso sobre o estado atual das transações. Dado que o DLT é adequado para assegurar o consenso, a transparência e a integridade das transações que ele contém, vários benefícios da aplicação do DLT ao IdM já foram propostos:

- **descentralizada:** as informações de identidade são referenciadas em um livro-razão que nenhuma autoridade central possui ou controla;
- **inviolável:** atividades históricas no DLT não podem ser adulteradas e transparência é dada a todas as mudanças nesses dados;
- **inclusivo:** novas maneiras de se criar identidade do usuário podem ser concebidas para expandir o alcance de identidades legais e reduzir a exclusão;
- **redução de custos:** as informações de identidade compartilhada podem levar à redução de custos para as partes confiáveis, juntamente com o potencial de reduzir o volume de informações pessoais que são replicadas em bancos de dados;
- **controle de usuário:** os usuários não podem perder o controle de seus identificadores digitais, mesmo se perderem o acesso aos serviços de um determinado provedor de identidade.

2.6 Identidade digital autossoberana baseada em DLT

O Gerenciamento de Identidade (IdM) abrange os processos e políticas envolvidos no gerenciamento do ciclo de vida de atributos em identidades para um domínio particular (ISO/IEC, 2019).

Na atualidade, a maioria dos modelos de IdM são centralizados, uma única entidade controla todo o sistema. No entanto, as próprias identidades geradas podem ser federadas além de uma única organização, como quando os governos emitem carteiras de identidade nacionais.

Nos sistemas de identidade federada, os usuários podem usar informações de identidade estabelecidas em um domínio de segurança para acessar outro. Esquemas de *login* único, como o *Facebook* e o *Google*, por exemplo.

O gerenciamento de identidade centrado no usuário coloca a administração e o controle das informações de identidade diretamente nas mãos dos indivíduos. Os exemplos incluem gerenciadores de senhas (por exemplo, *1Password*, *Less-Pass*, entre outros) que gerenciam, de maneira segura, as diferentes credenciais nos sites da internet.

Apesar das diferentes abordagens, uma função que é fundamental para o IdM é a vinculação segura de um identificador único: um valor que distingue inequivocamente um usuário de outro em um mesmo domínio, bem como atributos (às vezes chamado de certificações ou declarações): direitos ou propriedades de um usuário como nome, idade, classificação de crédito etc.

Os primeiros passos tomados para adequar o uso de DLT para estabelecer um mapeamento de identificador seguro e descentralizado foram adotados no *design* do *Namecoin* que é um dos *fork* mais longínquos do Bitcoin. O Namecoin fornece um *namespace* legível, descentralizado e seguro para o domínio ".bit". Essa conquista contradizia a sabedoria convencional de que um sistema de nomenclatura exibindo todas as três características não poderia ser projetado (ZOOKO, 2017). Ali (2016) ampliou o esquema do Namecoin, para criar uma infraestrutura de chave pública (PKI) descentralizada que registra ligações entre uma chave pública e um identificador legível.

Recentemente, surgiram vários modelos de identidade descentralizada que se estendem além da nomenclatura e visam fornecer um conjunto mais completo de funções de IdM. No entanto, até o momento, não houve uma avaliação direta e ampla dessas propostas.

Atualmente existem basicamente duas categorias de propostas de IdM baseado em *blockchain*:

a) ***Self-Sovereign Identity* (SSI)**: uma identidade que pertence e é controlada por seu proprietário sem a necessidade de depender de qualquer autoridade administrativa externa e sem a possibilidade de que essa identidade possa ser removida. Pode ser ativado por um ecossistema de identidade descentralizado que facilita o registro e a troca de atributos de identidade e a propagação da confiança entre as entidades participantes. Exemplos incluem Sovrin, uPort e OneName.

b) **Identidade confiável descentralizada:** uma identidade fornecida por um serviço centralizado que realiza a prova de identidade de usuários com base em credenciais

confiáveis existentes (por exemplo, passaporte) e registra atestados de identidade em um DLT para validação posterior por terceiros. Exemplos incluem ShoCard, BitID, ID.me e IDchainZ.

2.7 Iniciativas globais em identidade digital autossoberana

Após a apresentação das Leis da Identidade – Seção 2.7.1, serão resumidamente apresentadas, como exemplo, duas iniciativas globais baseadas em SSI: (i) Sovrin – Seção 2.7.2, e (ii) ShoCard – Seção 2.7.3.

Acredita-se que, com a apresentação dessas duas iniciativas globais, seja possível identificar o modelo de atuação, decisões de *design* predominantes e também os desafios encontrados. Interessante notar que esses dois exemplos servem a um propósito similar para o cenário mais amplo do IdM baseado em DLT.

Essas iniciativas foram escolhidas por fornecerem, de forma clara, os detalhes técnicos de seus projetos. Além disso, são iniciativas sustentadas por comunidades de grande porte ou possuem notável nível de financiamento.

2.7.1 Leis da Identidade

As conhecidas "Leis da Identidade" (CAMERON, 2005) são usualmente utilizadas como parâmetros para identificar os sucessos e fracassos dos sistemas de identidade digital. Essas leis, apresentadas a seguir, compõem uma estrutura conhecida e representam um espectro completo de preocupações com IdM, abrangendo segurança, privacidade e experiência do usuário:

- **Lei 1** - Controle e consentimento do usuário: as informações que identificam o usuário só devem ser reveladas com o consentimento desse usuário;
- **Lei 2** - Divulgação mínima e para uso restrito: as informações de identidade só devem ser coletadas em uma base de "necessidade de conhecimento" e mantidas em uma base de "necessidade de reter";
- **Lei 3** - Partes justificáveis: As informações de identidade só devem ser compartilhadas com partes que tenham direito legítimo de acessar informações de identidade em uma transação;
- **Lei 4** - Identidade dirigida: o suporte deve ser fornecido para compartilhar informações de identidade publicamente ou de maneira mais discreta;
- **Lei 5** - *Design* para um pluralismo de operadores e tecnologia: uma solução deve permitir a interoperabilidade de diferentes esquemas de identidade e credenciais.
- **Lei 6** - Integração humana: a experiência do usuário deve ser consistente com as necessidades e expectativas para que os usuários possam entender as implicações de suas interações com o sistema;
- **Lei 7** - Experiência consistente em contextos: os usuários devem ser capazes de esperar uma experiência consistente em diferentes contextos de segurança e plataformas de tecnologia.

2.7.2 *Self-Sovereign Identity* – Sovrin

A rede Sovrin (SOVRIN, 2018) é uma rede de identidade descentralizada de código aberto construída sobre a tecnologia DLT (Figura 5), considerada uma rede pública/permissionada, na qual, apenas as instituições confiáveis chamadas de *stewards* ou *writers* - que podem ser bancos, universidades, governos, instituições de pesquisa, etc. – são os nós que participam do consenso e executam a gravação no *ledger*. Já os nós observadores só possuem atributo de leitura do *ledger* e atuam como intermediários entre o usuário final e a rede.

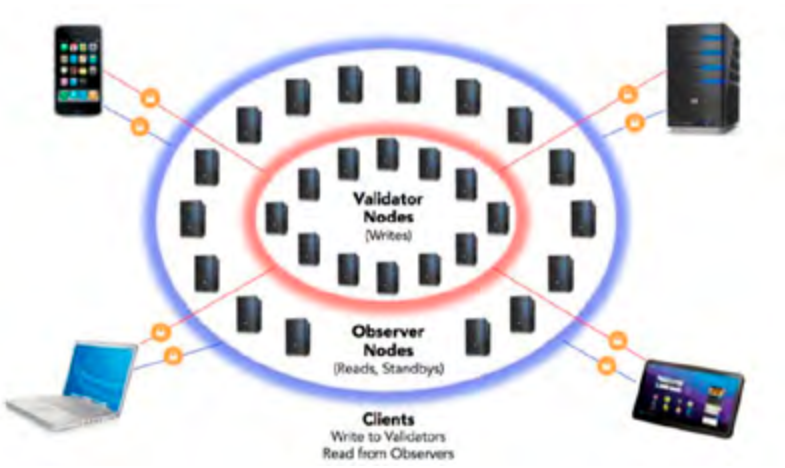

Figura 5. Sovrin: Nós validadores e nós observadores.

A governança da rede é feita pela *Sovrin Foundation*, fundação sem fins lucrativos, que assegura a governança adequada e o respeito ao acordo legal denominado Sovrin *Trust Framework* firmado entre a fundação e os *stewards/writers*. Atualmente a *Sovrin Foundation* é quem fornece o códigobase para o projeto *Hyperledger Indy* (HYPERLEDGER).

2.7.3 Identidade confiável descentralizada – ShoCard

ShoCard (SHOCARD SITA, 2016) fornece uma identidade confiável que aproveita a tecnologia DLT para vincular um identificador de usuário, uma credencial confiável existente (por exemplo, passaporte, carteira de habilitação) e atributos de identidade adicionais, por meio de *hashes* criptográficos armazenados em transações *bitcoin*. Os principais casos de uso da ShoCard são de verificação de identidade em interações presenciais e *on-line*.

2.8 Conceitos da Identidade Digital Autossoberana

- DID: os Identificadores Descentralizados ou *Decentralized Identifiers* (DIDs), são um novo tipo de identificadores para Identidade Autossoberana verificável, ou seja, foram projetados para serem controlados pelo seu dono ou portador (*holder*), sem nenhum meio centralizado, como por exemplo, uma autoridade certificadora (W3C, 2019). DIDs podem ser considerados um tipo de URLs que descrevem certificados (documentos),

seus tópicos e métodos que podem ser usados. Com eles, é possível verificar o conteúdo dos certificados e seus métodos criptográficos (provas) disponíveis.

- *Endpoint* dos Agentes: o registro de um DID também possui um *endpoint* (endereço IP persistente e sua respectiva porta) de seu agente. Esse endereço é utilizado pela solução de identidade para se comunicar diretamente com outros agentes, sem a necessidade da utilização de sistemas ou bases terceiras, apenas consultando a *blockchain* para verificar qual o endereço do agente daquela identidade para começar uma comunicação direta entre agentes.
- DIDs públicos e privados: DIDs públicos são registrados na *blockchain* e são utilizados para iniciar as conexões de uma identidade. A partir deles pode-se gerar DIDs privados, que não são registrados no *ledger*, mas que foram gerados com a assinatura de DIDs pública, podendo assim, quando utilizados, serem rastreados até o(s) seu(s) DID(s) de origem. DIDs privados podem ser usados para a criação de documentos ou certificados para operações privadas, como por exemplo, a identificação bancária de uma pessoa física, o que é considerado um dado privado e, portanto, não deve ser registrado em uma *blockchain*.
- Esquemas de dados (*schemas*): os esquemas nada mais são do que a estrutura de dados que especifica os atributos a serem criados para um documento ou certificado da solução. Por exemplo, o Registro Geral Brasileiro (RG) deve ter obrigatoriamente os campos: nome, número, data de nascimento, data de emissão, cidade de nascimento, estado e órgão emissor e, opcionalmente, nome da mãe e do pai do portador da identidade. Essa semântica e suas ontologias devem ser registradas na *blockchain* para o momento de sua geração e também para suas provas (seja de todos os dados ou não).
- Definição de credencial: uma vez que o esquema da credencial está registrado na *blockchain*, os agentes interessados podem se registrar no *ledger* como emissores de credencial daquele esquema;

- Autenticação via DID (DID *Auth*): método pelo qual um DID e seu certificado são utilizados como um *token* para autenticar um usuário e informar, por meio do documento de seu certificado, quais são suas permissões e autorizações. Essa autenticação é realizada por meio de uma série de componentes e agentes, por exemplo, um navegador da *web* e um dispositivo móvel.
- Credenciais Verificáveis: uma credencial verificável representa as mesmas informações que uma credencial física, mas adicionando tecnologias como assinaturas digitais, o que as torna mais seguras, difíceis de fraudar e mais confiáveis do que uma versão física. Os portadores dessas credenciais podem oferecer provas e as compartilhar com entidades verificadoras. Sua grande inovação se dá ao dispensar consultas a terceiros para verificar sua integridade, posse e autenticidade, pois todas essas comprovações são realizadas apenas por meio de verificação dos DIDs do emissor, receptor na *blockchain* e por análises criptográficas, permitindo, assim, que todo o processo seja automaticamente executado por máquina.
- Sistema de Gerenciamento de Chaves Descentralizado (DKMS): abordagem para o gerenciamento de chaves criptográficas em que não existe uma autoridade certificadora central. O grande habilitador do DKMS foi o advento das *blockchains*, pois é por ela que advém a segurança, imutabilidade, disponibilidade e resiliência, atributos imprescindíveis e essenciais para a criação desse mecanismo de gerenciamento de chaves, que fornece a distribuição, verificação e recuperação das chaves sem a necessidade de uma autoridade central.

Esses mecanismos juntos habilitam a criação e a aplicação da identidade digital autossoberana, permitindo uma disrupção de outros modelos de gerenciamento de identidades que até aqui por definição dependiam de uma autoridade centralizada para validar e verificar a identidade de pessoas e coisas, sempre observando pelo controle e privacidade do portador dessa identidade. A sessão 2.9 descreve o que é registrado no *ledger* da *blockchain*.

2.9 O que vai ou não no *ledger*

Um dos grandes desafios ao desenvolver uma solução baseada em DLT é definir quais são as informações que serão armazenadas no *ledger*. Dadas as características intrínsecas do *ledger*, tais como ser replicado em todos os nós da rede distribuída e a impossibilidade de ter seus registros apagados, procura-se colocar nele somente dados considerados essenciais da solução.

No caso das soluções de identidade digital descentralizadas de pessoas, o desenvolvimento deve ser feito utilizando a metodologia de Privacidade por Projeto (*Privacy by Design*), visando aumentar a segurança e a privacidade dos usuários. Nesse sentido, um cuidado adicional que deve ser tomado, já na fase de especificação de requisitos, é não colocar no *ledger* nenhum tipo de dado pessoal, mesmo que anonimizado, com o objetivo de atender aos requisitos presentes nas leis gerais de proteção de dados pessoais, tais como GDPR da União Europeia e LGPD do Brasil.

Na solução do FinID, as seguintes informações são armazenadas no *ledger*:

- DIDs públicos e o *endpoint* persistente de seu agente;
- esquema de estrutura de dados e definições de credenciais;
- registro de revogação de credenciais;
- autorizações para atividades automatizadas dos agentes em nome do seu portador, isto é, o que um agente pode ou não fazer automaticamente em nome de quem ele representa.

O que não vai no *ledger*:

- DIDs privados (por exemplo, o DID usado para inicialização de pagamentos ou ainda de informações pessoais);
- credenciais privadas;
- registros de consentimentos, de provas ou transações realizadas diretamente pelos agentes.

2.10 A importância e os desafios das Carteiras Digitais (*Digital Wallets*)

Carteiras Digitais são peças-chave para soluções de Identidade Digital Autossoberana. Elas servem para guardar, de forma segura e confiável, nossas credenciais, chaves privadas e informações. Além disso, elas servem também para a gestão de agentes terceiros, os quais podem, com o consentimento do usuário, acessar suas credenciais e dados, possibilitando a verificação de quem possui tais permissões e também podem revogar permissões que não fazem mais sentido.

Além disso, Carteiras Digitais são responsáveis por fazer o gerenciamento das credenciais dos usuários, desde comprovantes de conclusão de cursos, que devem ficar por um longo tempo (pelo menos enquanto forem relevantes), e até mesmo simples ingressos para eventos (por exemplo, cinema e teatro), que poderão ser descartados (ou movidos para um arquivo morto) depois de seu uso.

Apesar de ser incontestável que carteiras digitais serão amplamente utilizadas para o gerenciamento e controle de nossas identidades e dados, seu conceito tem mais de duas décadas. Um exemplo de uma carteira digital criada no início da década passada, é o Microsoft Passport (OPPLIGER, 2019), que se propunha a ser a solução de informações para "*Single Sign-On*" e de cartões de créditos em um único lugar. O Microsoft Passport fracassou, sem nunca ter chegado perto da quantidade de usuários e aplicações integradas que um dia se pensou para ele. Assim como o Microsoft Passport, inúmeras outras soluções de carteiras digitais fracassaram ao longo dos últimos vinte anos. Em geral, os principais motivos dos fracassos foram, dentre outros:

- as carteiras digitais criadas nesse período, em sua maioria, foram iniciativas fechadas, não possuíam padronização e ou meios para portabilidade, fazendo com que os usuários se tornassem reféns dessas soluções;
- problemas de segurança, como os reportados para a abordagem de *Single Sign-On* (KORMANN, 2000);

- essas iniciativas foram ambiciosas demais, propondo-se a gerenciar e a controlar todas as credenciais dos usuários de uma única vez, inevitavelmente se tornando soluções complexas demais e, em geral, tediosas de se usar.

Além dos aspectos citados acima, que continuam sendo uma realidade a ser enfrentada por carteiras digitais modernas, também vale ressaltar os seguintes desafios (O'DONNELL, 2019):

- portabilidade entre carteiras (o usuário, tendo controle de sua identidade, deve ser capaz e ter meio de portar e controlar suas credenciais na solução que preferir e mais confiar);
- padronização de credenciais, sendo que, em tese, o modelo (*schema*) de uma credencial financeira emitida por um agente, deveria ser minimamente compatível com o modelo da credencial de outro agente do mesmo segmento;
- facilidade para realizar *backup*, uma vez que acidentes acontecem como: perda de dispositivos móveis (onde, eventualmente, as carteiras digitais de pessoas físicas poderiam ficar armazenadas) ou até mesmo em caso de dano de aparelho ou exposição da carteira. Em todos esses casos, deveria ser possível ao usuário revogar suas credenciais expostas, conseguir emitir novas e recuperar os dados perdidos;
- e por último, e tão crucial quanto os demais desafios, é a usabilidade das carteiras digitais. Carteiras digitais confusas, com baixa usabilidade são forte barreira de entrada para adesão a este tipo de serviço.

Além dos desafios acima demonstrados, será também necessário o desenvolvimento de metodologias de análise de vulnerabilidade para mitigação de risco de ataques cibernéticos bem-sucedidos e, eventualmente, até mesmo a adoção de certificação de segurança para carteiras digitais, a fim de garantir mais segurança ao usuário da carteira.

2.11 Os esforços de padronização

Atualmente, existem ações globais no sentido de buscar padronização para os diferentes protocolos e agentes que constituem as soluções de identidade digital autossoberana. Conforme apresentado na Figura 6 (REED, 2018) existem vários órgãos envolvidos nestes esforços de padronização, com destaque para o W3C[7] (*World Wide Web Consortium*) envolvido na padronização dos DIDs e das *Verifiable Credentials*.

Figura 6. Esforços de Padronização.

[7] W3C - O *World Wide Web* Consortium é a principal organização de padronização da *World Wide Web*.

Muitos desses padrões ainda estão em fase de discussão. Um exemplo é a própria padronização dos DIDs, com o W3C lançando recentemente a versão V.1 do Data Model and Syntaxes (W3C, 2019).

DKMS (*Decentralized Key Management System* ou Sistema de Gerenciamento de Chaves Descentralizado) é um padrão aberto emergente para gerenciar DIDs e chaves privadas. O DKMS se aplica às carteiras nas quais se armazenam DIDs e chaves privadas, assim como aos agentes que leem/escrevem nessas carteiras. A ideia do DKMS é padronizar as carteiras para que o usuário nunca precise se preocupar com a segurança, a privacidade ou o bloqueio de fornecedores. A arquitetura inicial do DKMS está agora em análise pública no repositório da *Hyperledger Indy* (REED *et al.*).

O DID Auth é uma forma padrão simples para um proprietário de DID se autenticar, comprovando o controle de uma chave privada. Em novembro de 2017 foi formado o grupo de trabalho denominado DID *Auth* pela *Decentralized Identity Foundation*[8]. Em fevereiro de 2018, foram lançadas as especificações e implementações preliminares do padrão. Em abril de 2018, foi apresentado o primeiro protótipo do padrão no Internet Identity Workshop.

Verifiable Credentials é um formato para credenciais digitais interoperáveis e criptograficamente verificáveis que estão sendo definidas pelo *Verifiable Claims Working Group* do W3C, criado em maio de 2017. A missão do grupo é tornar mais fácil e mais segura a divulgação e troca de credenciais que foram verificadas por terceiros.

Por enquanto, a discussão sobre padronização de identidade digital autossoberana no Brasil está sendo contemplada na comissão ABNT/CEE-307 - *Blockchain* e Tecnologias de Registro Distribuídas, que possui no seu âmbito de atuação a normalização no campo de *blockchain* e tecnologias de registro distribuídos, no que concerne a terminologia e generalidades. Essa comissão é um espelho do ISO/TC-307 – *Blockchain* and *Distributed Ledger Technologies* (ABNT/CEE).

Recentemente, a comissão divulgou a versão preliminar do documento "*Blockchain* e tecnologias de registro distribuídos – Conceitos e elementos da tecnologia *blockchain*", que é composto por seis partes. O tema identidade está sendo abordado na sexta parte do documento (segurança, privacidade e identidade).

2.12 Aspectos legais e padronização da Identidade Digital Autossoberana

Um dos grandes desafios da Identidade Digital Autossoberana é o atendimento aos requisitos das principais leis relacionadas com a proteção de dados pessoais. Vários países adotaram um modelo jurídico para proteção de dados pessoais por meio de um regime legal de proteção de dados, na forma de uma lei geral. Com exceção dos Estados Unidos, a maioria dos países desenvolvidos, e também o Brasil, aprovaram leis abrangentes contemplando os setores público e privado. Embora alguns países possuam suas leis gerais, essas podem coexistir com normas setoriais, regulando setores específicos de forma complementar as leis gerais (BENNET, 1992).

[8] O DIF é uma organização focada no desenvolvimento dos elementos fundamentais necessários para estabelecer um ecossistema aberto para a identidade descentralizada e garantir a interoperabilidade entre todos os participantes.

Dentre estas leis, destaca-se o Regulamento Geral de Proteção de Dados da União Europeia também conhecido como GDPR, que foi elaborado pelo Parlamento Europeu e Conselho da União Europeia e publicado no dia 4 de maio de 2016. Ele foi implementado nos 28 países membros da União Europeia em 25 de maio de 2018. Ele se aplica à proteção das pessoas naturais no que diz respeito à proteção de dados e também ao livre movimento desses dados e revoga a Diretiva de Proteção de Dados Pessoais de 1995 (95/46/CE). O regulamento, que na União Europeia tem força de lei, possui um conteúdo bastante extenso, com 173 considerandos e 99 artigos.

No Brasil, foi criada a Lei 13.709/2018, também conhecida como LGPD, que foi publicada em 14 de agosto de 2018 e, segundo COTS, com esta publicação "o Brasil se integrou, não sem um certo atraso, ao grupo de países que possuem legislações específica para proteção de dados pessoais" (COTS, 2018). Pode-se afirmar que a grande fonte de inspiração para a elaboração da LGPD foi o GDPR, sendo a primeira mais genérica e, consequentemente, menos detalhada que o regulamento.

Seguem algumas questões relevantes das leis gerais de proteção de dados pessoais que podem impactar soluções que utilizam *blockchain*, com destaque para a identidade digital autossoberana:

- direito de apagar ou direito de ser esquecido: em algumas situações, o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada. Portanto, tal direito inviabiliza o registro de dados pessoais no *ledger*. Nas propostas de identidade autossoberana, os dados pessoais nunca são colocados no *ledger*. Em vez disso, são colocados somente identificadores pseudônimos e descentralizados denominados *Decentralized Identifiers* (W3C), chaves públicas pseudônimas, endereços de agentes e as estruturas das credenciais emitidas (*schemas*), conforme especificado pela W3C. Isso permite que a troca de dados pessoais ocorra inteiramente fora do *ledger*. Vale destacar que, diferentemente do GDPR, na LGDP não há previsão específica para tratamento do direito de ser esquecido. Segundo o ministro do STJ, Paulo de Tarso Sanseverino: "A LGPD abrange todos os dados

pessoais, inclusive digitais. O Marco Civil tem a preocupação somente com os efeitos da Internet. Apesar disso, a nova legislação não tem previsões importantes, como é o caso do Direito ao esquecimento" (LEORATTI, 2018).

- direito de retificação: O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Como os dados pessoais não são colocados no *legder* e, geralmente, ficam sobre a gestão do titular. Este requisito também é atendido pelas soluções de identidade digital autossoberana;
- direito de acesso: Isto significa que os titulares de dados têm o direito de perguntar a um controlador de dados se seus dados pessoais estão sendo processados e, caso estejam, receber detalhes sobre como este processamento se dá e onde. No caso da identidade digital autossoberana, quem controla o acesso aos dados é o próprio titular através dos DIDs;
- portabilidade dos dados: O direito à portabilidade de dados (artigo 20.º do GDPR, por exemplo) permite que um titular de dados receba dados de um responsável pelo tratamento, a fim de transmiti-los a outro controlador (ZYSKING, 2015). O Grupo de Trabalho do Artigo 29, por exemplo, considera que o "principal objetivo da portabilidade de dados é aumentar o controle dos indivíduos sobre seus dados pessoais e garantir que eles desempenhem um papel ativo no ecossistema de dados". A maioria das soluções atuais não fornecem aos proprietários tal funcionalidade. Isso não se aplica à identidade digital autossoberana, na qual a gestão dos dados (armazenamento e controle de acesso) é definida pelo próprio usuário dos dados. Esses dados podem ser armazenados nos seus próprios dispositivos por meio de um *Mobile Edge Agent* ou ainda na nuvem, usando um *Hub* que armazena e compartilha dados em nome dos seus proprietários, podendo ser concebido como uma carteira remota, que armazena todos os dados anonimamente criptografados, mas não as chaves.

3 Visão geral

Solução que, por definição, gera a camada de identidade para autenticação e conexão entre agentes financeiros e os tomadores de serviços do sistema financeiro. A solução preconiza uma maior facilidade de acesso aos serviços financeiros ofertados no varejo, automatizando o processo de registro dos consumidores junto às instituições financeiras e disponibilizando meios para que o consumidor gere sua credencial financeira junto à organização emissora de sua preferência. Essa credencial deve conter as informações ordinariamente usadas para a criação de identidades junto ao setor financeiro (e.g.: nome, comprovante de pessoa física, endereço, renda, etc.)

Tal credencial gerada por meio da solução fica sob controle e custódia do próprio consumidor. Tal controle viabiliza que o usuário agora consinta ou deliberadamente a apresente para instituições financeiras com as quais porventura queira vir a ter uma conexão, seja desde a criação de conta até mesmo a contratos específicos, como aplicações financeiras ou empréstimos, por exemplo.

Uma vez que a conexão entre o consumidor e a instituição financeira é estabelecida, esse relacionamento passará a compor a própria identidade financeira do consumidor, que

receberá credenciais acerca das informações geradas em função das interações e serviços adquiridos junto às instituições financeiras. Uma vez que agora essas credenciais estão sob posse e controle do consumidor, ele pode apresentá-las para outras instituições, novamente, de forma deliberada ou por meio de solicitação de acesso, aderente assim ao conceito de *open banking*.

Para isso, a solução deverá permitir sua integração pelos atores existentes no setor financeiro e também para os novos que possam vir a surgir com o advento da tecnologia, por exemplo, as instituições emissoras de credenciais financeiras. Tal integração possibilita que as aplicações bancárias já existentes para dispositivos móveis possam, então, tornarem-se efetivamente carteiras digitais para o controle da identidade financeira.

Essa inovação traz transparência e poder ao consumidor acerca do que é feito com sua identidade, trazendo segurança ao acesso da informação. Não obstante, às instituições financeiras é dado o benefício de vender produtos a quaisquer consumidores que tenham uma credencial válida, aumentando assim a capilaridade de seus produtos. Além disso, aumenta consideravelmente a confiança das instituições, que agora podem ter acesso de forma segura e confiável às informações bancárias e comportamentais dos usuários.

3.1 Casos de uso

3.1.1 Escolher instituição emissora de credencial

O consumidor está com o aplicativo FinID devidamente instalado no dispositivo móvel e realiza o primeiro acesso à aplicação; um termo de uso e privacidade é exibido e deve ser aceito; o consumidor deve cadastrar um código PIN para acesso ao aplicativo; e, opcionalmente, habilita o uso da biometria como facilitador ao uso do PIN. Isto feito, uma lista de instituições emissoras de credenciais financeiras é apresentada ao consumidor, que poderá:

- acessar informações sobre as opções de credenciais emitidas pelas instituições, assim como o custo e modelo de cada credencial;
- buscar pela instituição de sua preferência, usando para isso o nome dessa instituição;
- selecionar a instituição emissora desejada para realizar o processo de *onboarding* e emissão de uma identidade digital financeira.

3.1.2 Solicitar emissão de credencial financeira

Com a instituição emissora selecionada, o solicitante deverá preencher as informações obrigatórias e realizar o processo de geração do conteúdo para análise, ou seja, tirar fotos de documentos, comprovantes e *selfies*.

3.1.3 Operar emissão de credencial

O operador do *backoffice* de emissão de credencial financeira está identificado e autenticado. O sistema exibe as solicitações pendentes por data, então o operador pode selecionar uma solicitação da lista e visualizar seu conteúdo. Caso julgue o pedido procedente, ele emite a credencial, caso contrário, ele a rejeita. Em ambos os casos, os dados pessoais trafegados para a solicitação são desconsiderados na plataforma, ficando registrado apenas o número da requisição e seu *status* (emitida ou rejeitada).

3.1.4 Gerar convite

O operador do agente institucional financeiro está identificado e autenticado. O sistema apresenta uma opção para gerar um convite para criar uma conexão com a instituição via identificadores descentralizados (DID), o operador seleciona essa opção e em sequência seleciona o tipo do convite:

- autenticação, usado para autenticar usuários por meio de Identificadores Descentralizados em vez de usuário e senha;
- conexão, gera uma conexão com um usuário que ainda não tenha vínculo com a instituição.

O convite pode ser sintetizado em um *QR-Code*, para leitura em aplicativos de carteiras digitais.

3.1.5 Criar conexão com instituição financeira

O consumidor está identificado, autenticado e de posse de uma credencial financeira válida no aplicativo de carteira digital FinID. O consumidor acessa a opção de ler *QR-Code* para conexão com a câmera do dispositivo móvel que lê o *QR-Code*. O aplicativo interpreta o *QR-Code*, confirma a identidade do autor na *blockchain* de identidade, recupera na mesma *blockchain* o endereço para requisições das instituições e assina a requisição com seu identificador.

O agente institucional da organização assina a requisição, verifica a assinatura mediante consulta da *verkey* da identidade do consumidor na *blockchain* e gera um identificador descentralizado (DID) para a conexão com o consumidor, requisitando em seguida acesso às informações da credencial financeira do consumidor. O consumidor então é notificado quanto à solicitação às informações de sua credencial financeira e consente o acesso. O aplicativo envia a credencial verificável com as informações via conexão segura criada pelo DID com a instituição e a organização recebe e acessa as informações.

3.1.6 Realizar autenticação com identificadores descentralizados

O consumidor está identificado, autenticado e com um identificador descentralizado criado previamente com a organização desejada. O consumidor acessa o *website* da instituição financeira e seleciona a opção para autenticar-se com sua identidade FinID. Um *QR-Code* então é exibido e o consumidor seleciona a opção para autenticar-se com o FinID no aplicativo de carteira digital. O *QR-Code* é lido com a câmera do dispositivo móvel, que então solicitará a confirmação por biometria ou código PIN. Uma vez autenticado, uma requisição de autenticação é assinada com o identificador descentralizado privado da conexão com a organização. Então a requisição é entregue ao agente institucional que verificará a autenticidade junto à *blockchain*, e constatada a autenticidade, o acesso ao portal é liberado.

3.1.7 Controlar identidade

O consumidor está identificado, autenticado e de posse de uma credencial financeira válida no aplicativo de carteira digital FinID. O consumidor seleciona a opção para listar todas as suas conexões; seleciona a conexão com a qual quer interagir e seleciona a opção para revogar conexão. A conexão é então revogada e um registro é acrescentado na *blockchain*, Então a instituição financeira correspondente à conexão é notificada da revogação.

O operador do agente institucional financeiro está identificado e autenticado. O operador seleciona a opção para listar todas as suas conexões, seleciona a conexão com a qual quer interagir e seleciona a opção para revogar conexão. A conexão é então revogada, um registro é acrescentado na *blockchain* e o consumidor correspondente à conexão é notificado da revogação.

4 Escopo do protótipo

O consumidor receberá, por meio digital ou via *QR-Code*, um convite para criar relacionamento com uma instituição financeira, por meio de uma conexão registrada no *ledger* de uma *blockchain*, especializada no gerenciamento de identidade descentralizada. Para isso, o consumidor acessa o aplicativo do FinID em seu dispositivo móvel pessoal para, então, se comunicar diretamente com o agente financeiro institucional. Esse processo registrará na *blockchain* um identificador descentralizado único (aqui chamado de DID) e público. Esse processo visa formalizar a criação de um vínculo entre dois agentes e também será usado para a comunicação entre ambos.

Esse DID será criado por meio da assinatura digital do DID privado do proponente (ou seja, da instituição financeira) e também pela assinatura do DID privado do proposto (ou seja, consumidor).

Com a conexão criada e registrada na *blockchain* de maneira automatizada, o agente institucional solicitará ao proposto os atributos pertinentes ao serviço ofertado. O consumidor deverá, se assim fizer sentido, consentir no acesso às informações solicitadas, que serão enviadas por meio da conexão preestabelecida. Com a credencial recebida, o agente da instituição financeira irá consultar a *blockchain* para verificar o emissor e o destinatário da

credencial apresentada, a fim de averiguar a origem e a posse da credencial. Depois dessa fase, o agente irá confirmar a autenticidade das informações.

A prova da origem, posse e também da autenticidade dos atributos da credencial apresentada se dará por meio de técnicas avanças de criptografia que são verificadas por meio de consultas utilizando os DIDs e suas chaves públicas disponibilizados na *blockchain* de identidades descentralizadas, como ilustrado na figura a seguir:

:

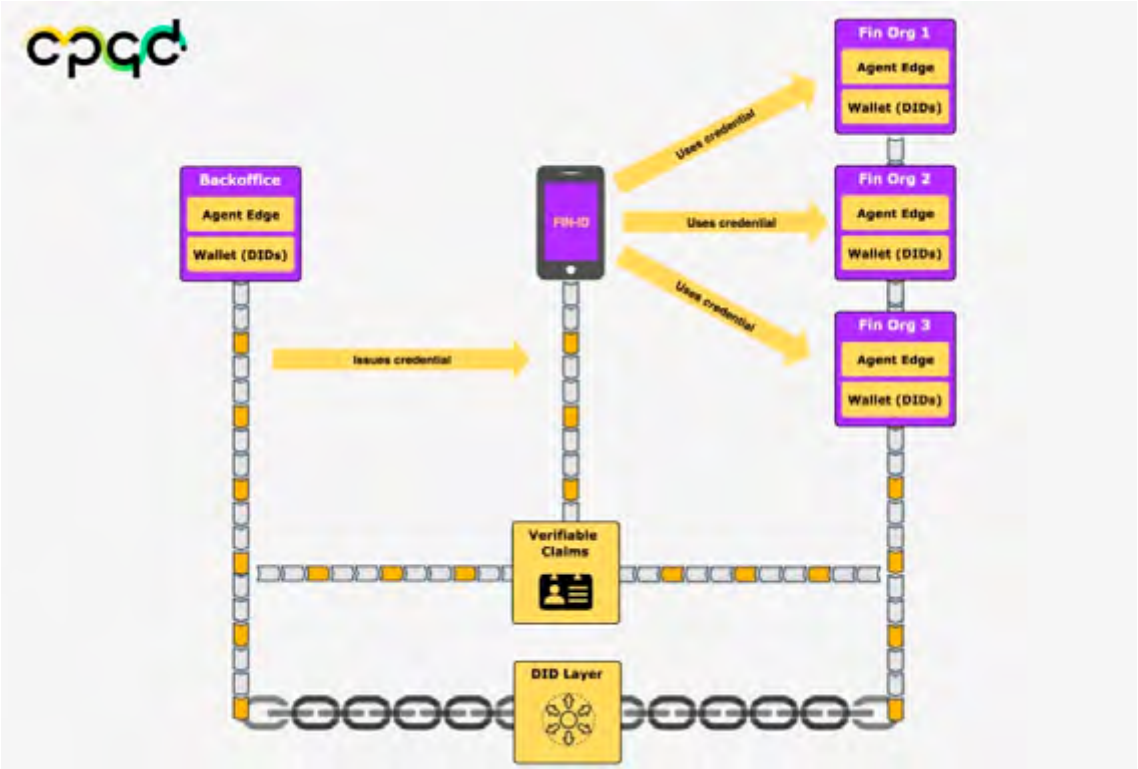

Figura 7. Visão da solução do FinID.

A solução FinID tem seus pilares em quatro principais componentes tecnológicos:

- Agente Institucional Emissor: agente independente que recebe solicitações via API para geração de credenciais; geração essa realizada via processo no módulo de aplicação *web* de *backoffice*;
- Agente Institucional Financeiro: agente que representará as instituições financeiras que farão parte da rede, tendo como principal atribuição gerar convites para conexões, a fim de autenticar as credenciais financeiras que serão utilizadas na contratação de serviços e, além disso, emitir credenciais pertinentes aos serviços contratados;
- Agente Móvel: é a carteira digital que manipulará a identidade financeira pessoal em nome do seu proprietário. Terá como principais atributos ser meio para o processo automatizado da criação da carteira digital, receber convites para conexão e também poder controlar suas conexões e consentimentos.

4.1 Emissão de credencial

A solicitação da credencial se dará por meio do agente móvel do tomador final, isto é, do aplicativo FinID, que para tanto, deverá estar devidamente instalado no dispositivo móvel (Android ou iOS) e com os termos de uso devidamente aceitos.

A solução, como demonstrado no protótipo, abrangerá a emissão de credenciais financeiras e sua utilização para autenticação e autorizações com vários agentes financeiros verificadores, ou seja, simulando instituições financeiras que aceitem a identidade do FinID.

Os atores e as instituições envolvidos nesse processo são, necessariamente, o requerente da identidade, que é quem a solicita; a instituição emissora, que é quem recebe a solicitação; o operador do sistema aqui denominado como *backoffice*, que é quem constata a autenticidade, valida a solicitação e emite a identidade. Por fim, outro recurso necessário neste processo é a presença de um *ledger* de uma *blockchain* para o gerenciamento das conexões e identidades envolvidas no processo (no caso, a identidade da instituição emissora e do requerente).

Para isso, é necessário realizar um processo de cadastramento, também denominado *onboarding* do tomador final, que deverá informar seus dados, por meio de fotos de comprovantes, documentos e *selfies*, os quais deverão ser analisados com o objetivo de validar que ele, de fato, está realizando a operação de cadastramento e que é ele o detentor daquelas informações.

Após a completude dessa ação, um operador de *backoffice* receberá uma requisição para emissão de credencial FinID. Ele então a analisará e decidirá se a credencial deve ser emitida ou não.

Todo esse processo se dá por meio de convites para geração de DID para relacionamento entre o emissor da credencial e o tomador final (conexão) e será descrito nos tópicos subsequentes.

4.1.1 Processo de informação dos dados a serem considerados no FinID:

O usuário deverá preencher as informações solicitadas que comporão a identidade da credencial a ser gerada. Essas informações solicitadas são as mesmas registradas no esquema de dados no *ledger* da solução do FinID. Para a demonstração, esse protótipo solicita as seguintes informações:

- nome;
- sobrenome;
- CPF;
- data de nascimento;
- logradouro residencial;
- número;
- complemento (opcional);
- bairro;

- cidade;
- UF;
- CEP.

4.1.2 Processo de registros fotográficos para autenticação e comprovação das informações:

Após o registro das informações, descritos no tópico 4.1.1, o usuário será solicitado a registrar fotograficamente os documentos e comprovantes necessários para comprovar a autenticidade das informações necessárias, como, por exemplo, o registro frente e verso de sua Carteira Nacional de Habilitação (CNH).

Além disso, faz-se necessário, a fim de evitar fraudes, que o requerente da identidade tire uma foto de si no momento da solicitação da credencial, a conhecida *selfie*. Esse procedimento visa possibilitar a conferência desta *selfie* com a fotografia presente no documento utilizado no processo.

4.1.3 Processo de requisição da credencial FinID:

Com a execução do passo 4.1.2, o aplicativo FinID exibirá os dados informados para a conferência do requerente que, após análise e confirmação das informações, irá disparar o processo eletrônico da requisição para emissão da credencial. Esse processo ocorre de forma automatizada e transparente, mas contemplando os quatro passos a seguir:

1. envio dos dados informados: por meio de uma requisição HTTPS, usando uma interface REST. O aplicativo móvel envia os dados informados pelo usuário para a instituição emissora;
2. envio das fotografias dos documentos necessários para a emissão da credencial e a *selfie*;
3. geração de um convite para a criação de um DID para o relacionamento (conexão) entre o emissor e o requerente;
4. envio do convite gerado no passo 3, via requisição HTTPS para a instituição emissora.

Após a execução desse processo, a solicitação da credencial foi realizada para um emissor registrado e a aplicação desse protótipo entrará em um estado de "aguardando".

4.1.4 Recebimento e análise da solicitação de credenciamento.

A instituição receberá, por meio de requisições HTTPS, uma solicitação de credenciamento de identidade FinID, que será então enfileirada e encaminhada para os operadores do *backoffice*.

O operador do *backoffice*, devidamente autenticado no sistema, receberá a solicitação em seu painel principal, selecionando-a e visualizando-a em uma tela para análise e sua posterior emissão ou rejeição.

Tanto em caso de sucesso, isto é, emissão, como no cenário alternativo de rejeição, todos os dados informados pelo usuário e as fotos enviadas serão definitivamente apagadas do sistema e do servidor da solução emissora, nesse caso, para evidenciarmos a inexistência de silos persistentes e respeito às práticas e normas de leis e regulações como a LGPD e a GDPR.

Após o operador concluir sua análise e constatando que a solicitação é regular, ou seja, é autêntica, o cenário principal (de emissão) é iniciado ao selecionar a opção para a emissão da credencial, o que dispara os seguintes processos:

1. o agente da instituição emissora aceita o convite para criar um DID de relacionamento (conexão) com o requerente, gerando um identificador descentralizado único para isso e assinando-o com a chave privada de seu DID público registrado no *ledger*;
2. o agente da instituição emissora emite uma credencial e suas provas (assinaturas criptográficas) utilizando sua própria chave mais o DID da conexão gerado para aquela credencial;
3. com a credencial gerada e a conexão via DID ativa, o agente emissor se comunica diretamente com o agente do requerente. Essa comunicação se dá por meio dos endereços e portas do agente registrados no *ledger*, para o envio criptografado via o DID da conexão para o agente do requerente, que será o único a conseguir abrir a mensagem e, então, armazenar a credencial em sua carteira digital.

Após a conclusão desse processo, o agente, como explicado no passo 3 do processo 4.1.4, é contatado e recebe sua credencial, habilitando-o assim a sair do estado de "aguardando" para o estado de "pronto para uso", onde nesse protótipo lhe é mostrada a opção para ler *QR-Codes* para iniciar a utilização de suas funções.

4.2 Utilização da credencial FinID.

A utilização da credencial FinID é exemplificada por meio da automatização do processo para criação de vínculo entre os tomadores finais e as instituições financeiras.

Nesse processo, as organizações e atores envolvidos são a instituição financeira, que habilita o processo para conexão de vínculo por meio da geração de convites para criação de DIDs; o tomador final, que recebe convites das instituições e consente na utilização de sua credencial e na consequente criação de vínculo entre ambos; e, por fim, o *ledger* da *blockchain*.

É salutar ressaltar que este processo independe e não tem nenhuma interação com o emissor da credencial financeira, não havendo necessidade de vínculo ou consultas da instituição verificadora, isto é, a instituição financeira e a referida organização emissora da credencial. Isso porque toda a verificação e validação da credencial se dá por meio de consultas ao *ledger* e validações criptográficas das assinaturas utilizadas para a criação da credencial.

Para essa automatização de criação de vínculos para autenticação e contratação de serviços ocorrer, os processos nos itens a seguir devem ser executados.

4.2.1 Geração de conexão entre instituição financeira e tomador final

A instituição financeira gera um convite público por meio de seu DID público a fim de conectar-se com tomadores finais que tenham uma credencial FinID. Esse convite é apresentado por meio de um *QR-Code*.

O tomador final, munido de seu aplicativo FinID, acessa a opção para iniciar uma conexão, o que habilita o leitor de *QR-Code* da aplicação; ele o lê; recebe o convite e automaticamente o aceita, gerando um DID para criação do vínculo com a instituição e, assim, criando também um canal exclusivo e seguro para comunicação direta entre seu agente e o agente digital da instituição.

4.2.2 Solicitação de prova para os dados da credencial FinID.

O agente da instituição financeira recebe a conexão ativa com o agente do tomador final e, por meio de seu DID público mais o DID da conexão criada, assina digitalmente uma solicitação de prova para uma credencial do FinID e envia essa solicitação diretamente ao agente do tomador.

O agente do tomador final recebe a solicitação de prova da credencial FinID e, por meio das assinaturas digitais utilizadas para a sua criação, além do fato dela ter sido criptografada pelas chaves do DID da conexão com a instituição, constata que a solicitação é de fato da instituição e consulta o tomador sobre a apresentação da credencial.

4.2.3 Consentimento para apresentação da credencial FinID

O tomador é notificado por meio de seu aplicativo FinID acerca da solicitação da instituição financeira. Por meio dessa notificação ele visualiza para quais dados da credencial a instituição está solicitando acesso e provas; analisa sua pertinência e, na perspectiva de um cenário principal, consente no acesso e na realização das provas, por meio de um *pincode* ou ainda por biometria em sua apresentação.

Em um cenário alternativo, o tomador pode divergir acerca da necessidade ou dos critérios solicitados pela instituição financeira e não consentir no acesso à credencial e às provas dos dados que a compõem. Nesse cenário o caso de uso encerra-se aqui.

4.2.4 Apresentação da credencial e consentimento de sua utilização.

Em caso de execução do cenário principal do processo 4.2.3; o agente financeiro envia a credencial FinID, assinada digitalmente com o DID criado no processo 4.2.1, diretamente para o agente da instituição financeira que solicitou acesso à credencial.

Também é enviada de volta ao agente da instituição financeira a solicitação de acesso aos dados, provas e credencial geradas pelo próprio agente da instituição, mas agora com a assinatura digital da

chave privada do DID público do agente do tomador final, a fim de registrar o consentimento da utilização da credencial e consequentemente de suas informações.

O agente da instituição financeira recebe a credencial e as assinaturas utilizadas para a criação de seus atributos, ou seja, os dados da credencial. Por meio de criptografia e consultas ao *ledger* da *blockchain* ele constata quem foi o emissor que a assinou, a autenticidade de sua posse e a integridade das suas informações, decidindo então acerca da criação do vínculo institucional e o consequente acesso a serviços para o tomador.

Ao fim da execução desse processo, fecham-se os casos de uso contemplados pelo protótipo do FinID.

5 Avaliação de riscos na solução FinID

Uma avaliação de risco pode ser realizada em diferentes contextos, de acordo com a visão de riscos desejada e os atores envolvidos. A metodologia utilizada [NAKAMURA, 2018] possui dez fases (Figura 8) e define o caso de uso da solução FinID como o contexto para a avaliação de riscos.

A análise de risco efetuado na solução FinID levou em consideração o fato de que a solução está em desenvolvimento no modelo de prova de conceito (*Proof of Concept* – PoC), no qual nem todos os aspectos técnicos e de negócio estão definidos.

Assim, as seções a seguir apresentam como resultado um plano de ação de segurança da solução, incluindo os controles identificados e priorizados, ou seja, no desenvolvimento da solução FinID para o mercado, é altamente recomendável que esses controles sejam implementados. Além disso, um novo ciclo de avaliação de riscos deve ser realizado, devendo incluir os novos ativos definidos durante a fase de arquitetura e *design* da solução final, tais como: tecnologia e versão da base de dados utilizada, versão do S.O. dos servidores, tecnologia de segregação e serviços, *peers* e tecnologia *blockchain* empregada, usuários da solução e privilégios, entre outros.

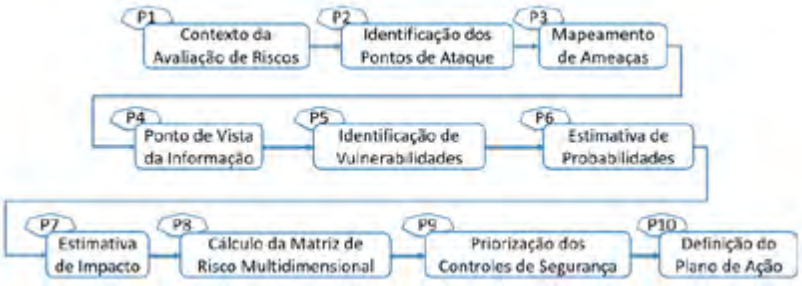

Figura 8 - Metodologia de avaliação de riscos. Fonte: Nakamura (2018).

5.1 Conclusão e recomendações de segurança para a solução FinID

A análise de riscos apresentada foi aplicada na solução FinID. Com isso, temos como resultados a tabela 1 que é a matriz de risco da solução FinID, a qual apresenta sete riscos classificados como nível de risco insignificante, dezesseis como nível de risco baixo, quinze como nível de risco médio, nove como nível de risco alto e dois como nível de risco extremo.

Probabilidade / Impacto		1	2	3
		Baixo	Médio	Alto
1	Baixo	7	9	0
2	Médio	7	15	3
3	Alto	2	6	2

Tabela 1 - Matriz de riscos da solução FinID.

Já a tabela 2 apresenta a ordenação dos controles de segurança mais otimizados que devem ser aplicados na solução FinID para mitigar as vulnerabilidades identificadas durante a avaliação de riscos no contexto definido e apresentado.

Posição	Índice	Controle de Segurança	*Score*
1	SC12	Política de segurança	364
2	SC13	Segurança e gerenciamento de riscos	364
3	SC5	Monitoramento	248
4	SC4	Desenvolvimento seguro	225
5	SC11	Política de privacidade	193
6	SC6	Identificação	152
7	SC7	Autenticação	152
8	SC8	Autorização	152
9	SC16	Segurança plataforma (rede) *blockchain*	106
10	SC10	Segurança física	83
11	SC3	Criptografia	70
12	SC2	Segurança de rede	50
13	SC14	Resposta a incidentes	42
14	SC1	Avaliação de segurança	41
15	SC15	Operações de segurança	12
16	SC9	Segurança de ativos	6

Tabela 2 - Controles de segurança - Score.

Os controles de segurança que mais influenciam na redução dos níveis de risco da solução FinID são a política de segurança (SC12) e a gestão de segurança e risco (SC13), seguidos pelo monitoramento (SC5) e desenvolvimento seguro (SC4). São ainda relevantes para o FinID a política de privacidade (SC11) e todo o processo de identificação (SC6), autenticação (SC7) e autorização (SC8).

Cada um dos controles de segurança listados a seguir, contempla uma recomendação específica para a solução FinID, o que é considerado o plano de ação de segurança da solução.

5.1.1 Política de segurança (SC12)

Inicia-se pelo estabelecimento de uma política de segurança (SC12) a qual deve abordar assuntos relacionados à segurança no processo de desenvolvimento de *software*, incluindo a devida diligência nos componentes de *software* ou *hardware* de terceiros, quando existir.

Usando os resultados da avaliação de riscos, a política de segurança define as regras e as responsabilidades de todas as partes interessadas e parceiros para evitar vulnerabilidades e definir e implementar corretamente os controles de segurança necessários para criar a solução FinID que possua a proteção adequada contra ameaças e preserve a segurança e a privacidade.

A política de segurança deve adicionar minimamente as seções destacadas pela avaliação de risco:

- codificação segura aplicada aos desenvolvedores;
- técnicas de segurança para proteger as informações e a importância de estar em conformidade com as leis e regulamentos de privacidade (LGPD por exemplo).
- atividades regulares para monitorar e avaliar os ativos da solução FinID e desenvolver a arquitetura de segurança.
- um modelo de gerenciamento baseado no ciclo PDCA (Planejar, Fazer, Verificar, Agir).

A solução FinID também deve adicionar seções sobre os problemas de segurança após a solução estar em operação e usada amplamente. O foco nesse estágio evolui do processo de desenvolvimento para produção, o que deve incluir os elementos de segurança, confiabilidade, resiliência e privacidade da solução.

5.1.2 Gerenciamento de riscos e segurança (SC13)

O gerenciamento de riscos e segurança se aplica a todos os ativos da solução FinID. Esse controle é essencial para preservar efetivamente os objetivos de segurança da solução, pois estabelece a base cíclica para iniciar, evoluir e aderir aos diferentes aspectos para criar e usar o FinID na perspectiva de segurança, privacidade, resiliência e confiabilidade.

O modelo e o processo de gerenciamento devem ser incluídos na política de segurança (SC12) e vinculados às regras, responsabilidades, processos e atividades relacionados. Dessa maneira é criada uma cultura de segurança e o gerenciamento de segurança e riscos tem um peso considerável em sua eficácia.

Uma recomendação é que o gerenciamento de riscos e segurança defina um período determinado regularmente para executar pontos de verificação. Um exemplo dessa recomendação é que uma avaliação de risco regular seja executada pelo menos uma vez por semestre, combinada com uma avaliação de segurança, ou sempre que ocorrer uma alteração substancial na solução FinID.

5.1.3 Monitoramento (SC5)

O monitoramento se aplica a todos os ativos da solução FinID. O monitoramento compreende diferentes níveis, incluindo rede, aplicativo, processo entre outros. Um *malware* como vírus ou *worm*, por exemplo, pode contaminar uma rede ou alcançar um aplicativo ou um componente da solução, proveniente de uma versão vulnerável do sistema operacional por exemplo. Na solução FinID, o monitoramento está relacionado aos ativos do lado dos servidores. No nível do processo, o monitoramento é importante para garantir a conformidade com a política de segurança estabelecida (SC12) e para garantir que componentes de terceiros não incluam componentes maliciosos (quando existir).

O monitoramento no nível do aplicativo está relacionado à identificação, que pode ser inclusive em tempo real, das atividades suspeitas na solução FinID que podem indicar um ataque em andamento ou ainda investigar um incidente. Esse controle de segurança está mais relacionado à fase operacional da solução FinID e não ao processo de desenvolvimento que é o atual, porém, mecanismos necessitam ser estabelecidos desde a fase de concepção da solução.

Recomenda-se que os componentes da solução FinID estabeleçam mecanismos de monitoramento que incluam, de acordo com a estratégia de segurança, aspectos desde a criação dos logs até as ferramentas e processos para correlacionar e analisar os eventos, em tempo real ou *offline*.

5.1.4 Desenvolvimento seguro (SC4)

O desenvolvimento seguro se aplica ao conjunto de ativos da solução FinID relacionados ao processo de desenvolvimento desde a etapa de concepção e projeto.

Por um lado, há controle sobre os processos de desenvolvimento dos módulos, função, algoritmo ou sistema desenvolvido e usados pela solução FinID. A segurança do desenvolvimento deve considerar as técnicas e os mecanismos para definir e codificar o *software*, evitando possíveis vulnerabilidades, como: autenticação quebrada (V1), controle de acesso interrompido (V2), XXE (V3), XSS (V4), desserialização insegura (V5), injeção (V6), especificação de *software* insegura (V7), projeto e arquitetura inseguros (V8), implementação de *software* incorreta ou insegura (V9), falta de proteção contra *malwares* (V10), exposição de dados confidenciais (V14), registro e monitoramento insuficientes (V15) ou falta de gerenciamento de chaves (V22). Um método (melhores práticas) que deve ser implementado é analisar os códigos imediatamente antes da confirmação, liberando todas as versões logo após a solução dos principais problemas de segurança identificados. Outro controle de segurança possível é executar análise de código estático ou análise de segurança dinâmica, procurando vulnerabilidades.

Por outro lado, as vulnerabilidades em potencial mencionadas anteriormente podem existir nos componentes de terceiros quando esses existirem. Os controles de segurança, nesse caso, são estabelecer mecanismos que forcem os fornecedores a seguir um ciclo de vida de desenvolvimento de segurança (*software* e *hardware*) e validar as suposições com avaliações de segurança (SC1).

A recomendação é estabelecer um ciclo de vida de desenvolvimento de segurança (SDL) para a solução FinID aplicado a todos os parceiros e estabelecer na política de segurança (SC12) os requisitos de segurança para os fornecedores de componentes de terceiros, incluindo o prazo para as avaliações de segurança (SC1). O SDL considera não apenas a codificação, mas também outras fases, como a definição do conceito, arquitetura, *design*, implementação, validação, implantação e suporte, que transformam um modelo conceitual em um produto real.

5.1.5 Política de privacidade (SC11)

A política de privacidade se aplica a todos os ativos da solução FinID, pois eles processam, transmitem ou armazenam dados que podem ser considerados "dados privados", como: Dados Cadastrais (CS02/AS05), e Registro de Credencial (CS06/AS09).

De acordo com leis e regulamentos como a GDPR (Europa) ou a LGDP (Brasil), os dados privados devem ser protegidos com base nos riscos e nos requisitos de negócios e, do ponto de vista técnico, a solução FinID deve, na etapa de produto, incluir mecanismos de anonimização e/ou pseudonimização, juntamente com criptografia quando aplicável.

A recomendação é estabelecer uma política de privacidade para a solução FinID. Ela deve indicar quais dados pessoais são coletados dos usuários, por que e como os mantém em sigilo, informando todos os usuários sobre como os dados estão sendo tratados e a política de compartilhamento (quando existir). Os usuários devem dar o consentimento explícito para a solução FinID, concordando com a política de privacidade. Os direitos de proteção de dados pessoais incluem: direito de acesso, direito à retificação, direito ao apagamento ou direito a ser esquecido, direito à restrição de processamento, direito à portabilidade de dados, direito ao objeto, direito a não estar

sujeito à tomada de decisão individual automatizada, direito de registrar reclamações, e direito a compensação de danos. As políticas também devem estar sob revisão contínua para garantir que permaneçam atualizadas e relevantes. Ao ter tais políticas em vigor, a organização responsável pela solução FinID está demonstrando o devido cuidado e diligência com os dados dos usuários.

5.1.6 Identificação (SC6)

A identificação se aplica a um conjunto de ativos da solução FinID relacionados aos usuários e aos componentes. A identificação é o ponto de partida para todo controle de acesso, pois sem a identificação adequada, não será possível conceder recursos/permissão a nenhuma identidade.

Para o ponto de vista da solução FinID, a identificação entre componentes é importante, principalmente para estabelecer uma autenticação mútua entre esses componentes que interagem entre si. Isso evita o uso de componentes maliciosos os quais possam vir a substituir os originais, no intuito de executar ações não autorizadas, como modificar ou vazar dados particulares.

A recomendação é estabelecer um conjunto de métodos disponíveis de identificação e autenticação que faça parte da solução FinID, para usuários e componentes como um todo.

5.1.7 Autenticação (SC7)

Igual ao controle de segurança relacionado a identificação (SC6), a autenticação se aplica a um conjunto de ativos da solução FinID relacionados aos usuários e aos componentes. Autenticação é o processo de verificar a identidade de um usuário, estabelecendo um relacionamento confiável entre o usuário e o sistema ou entre os componentes da solução que interagem entre si.

Para os usuários, o método de autenticação é baseado na identificação (SC6), de forma que os usuários precisem escolher, lembrar e digitar a senha correspondente no caso do uso do nome de usuário tradicional. No caso de uso de biometria, o usuário utiliza suas características físicas, como impressão digital, face ou voz, por exemplo.

Para a autenticação mútua dos componentes da solução FinID, o método de autenticação pode ser baseado em uma identificação básica sem autenticação, em primitivas criptográficas ou no uso de certificados digitais.

A recomendação é estabelecer um conjunto de métodos disponíveis de identificação e autenticação que faça parte da solução FinID, para usuários e componentes. O ponto de atenção é usar a segurança adequada para proteger as credenciais de autenticação, como as senhas. O uso da biometria requer uma abordagem de segurança diferente, pois, diferentemente das senhas que podem ser substituídas, as referências biométricas não podem ser reemitidas diretamente. Existem técnicas de segurança específicas para proteger as referências biométricas corretamente, as quais devem ser utilizadas.

5.1.8 Autorização (SC8)

A autorização também se aplica a um conjunto de ativos da solução FinID relacionados aos usuários e aos componentes. A autorização é a etapa final do processo que inclui identificação (SC6)

e autenticação (SC7) e aloca controles e privilégios apropriados para as entidades autenticadas, com base na identidade na solução.

A solução FinID possui diferentes entidades que acessam o sistema e suas informações. A autorização é baseada em um modelo de controle de acesso que garante os acessos sem interferências entre diferentes entidades. Em um nível, um usuário A não pode acessar as informações do usuário B.

A recomendação é usar o modelo juntamente com o conjunto de métodos disponíveis de identificação e autenticação que fazem parte da solução FinID, para usuários e componentes. O ponto de atenção é que o modelo de controle de acesso implementado, que deve refletir o modelo estabelecido, necessita ser testado pela perspectiva de caso de abuso, além das técnicas e procedimentos de teste tradicionais. Vale ressaltar também que as vulnerabilidades em outros componentes ou camadas da solução FinID podem contornar o modelo de controle de acesso. Outro ponto importante é definir os processos para gerenciar os usuários na criação, atualização e exclusão, incluindo o monitoramento.

5.1.9 Segurança na plataforma rede *blockchain* (SC16)

Segurança na plataforma (rede) *blockchain* é um controle relacionado à proteção da plataforma (rede) *blockchain*, que envolve minimamente: (i) verificação e testes das regras de consenso, (ii) gerenciamento de chaves, (iii) implementação e uso de algoritmos criptográficos, (iv) segurança física ao sistema e (v) desenvolvimento seguro de contratos inteligentes. Além disso, a política de segurança para a solução FinID deve compreender um capítulo específico para tratar do tema, onde devem ser atribuídos responsáveis e prazos. Outro ponto importante é definir os processos para gerenciar e monitorar essa plataforma ou rede *blockchain*.

5.1.10 Segurança física (SC10)

As possíveis vulnerabilidades relacionadas são processuais e físicas, incluindo registro e monitoramento insuficientes (V14), detecção inadequada de eventos de segurança (V16), ambiente sem segregação (V17), dificuldade em garantir a conformidade com a política de segurança (V23), acesso físico não controlado (V24), fraqueza humana (V25), limitação humana (V26) e fenômeno natural (V27).

A recomendação é definir uma política de segurança que inclua os controles para estabelecer os perímetros físicos, o controle de acesso e os processos de monitoramento. Se um fornecedor externo for usado, é recomendável que os requisitos de segurança existam no contrato, juntamente com a verificação de conformidade.

5.1.11 Criptografia (SC3)

A criptografia está relacionada à proteção de dados e aos componentes correspondentes da solução FinID que processam, transmitem ou armazenam os dados. A criptografia protege os dados em trânsito, processados e os dados em repouso, fornecendo confidencialidade e integridade. Existem

diferentes algoritmos, baseados em chave simétrica ou assimétrica, que têm suas particularidades e refletem principalmente no desempenho e no ônus operacional. O gerenciamento de chaves, por exemplo, é um processo que afeta diretamente a operação da solução FinID e é um aspecto essencial do projeto, com a definição dos processos para inserir, renovar e revogar as chaves ou ainda certificados digitais usados internamente pelos componentes.

A recomendação é detalhar a estratégia de criptografia, incluindo o gerenciamento de chaves, para a solução FinID, alinhada aos requisitos de proteção de dados e aos resultados da avaliação de riscos, para fornecer confidencialidade e integridade aos dados em trânsito e aos dados em repouso.

5.1.12 Segurança de redes (SC2)

A segurança da rede está relacionada a todos os ativos que interagem entre si por meio da rede de comunicação. A internet é usada pelos usuários, mas não pode ser controlada, assim, a solução FinID deve se proteger contra as ameaças provenientes da internet.

Do ponto de vista do fluxo de informações, as informações vêm do terminal (App e *Dashboard* – AS02) por meio da internet para a solução FinID, armazenadas na plataforma (rede) *blockchain* (AS03) ou ainda nos aplicativos dos usuários e *Dashboard* (AS02) das instituições financeira e *backoffice*.

A internet tem dois pontos de vista principais: o primeiro são os ataques que podem surgir a partir dela, tanto no ponto de extremidade quanto no lado do servidor da solução. O segundo é a informação que flui dos endpoints para o servidor através da internet. No primeiro caso, os pontos de extremidade e os componentes da solução FinID devem estar adequadamente protegidos contra ataques, desde o controle de acesso à rede (*firewall*) até o desenvolvimento do *software* para evitar vulnerabilidades. No segundo caso, as informações dos terminais para os componentes da solução FinID devem usar um canal seguro para se comunicar.

Além disso, os controles de segurança devem proteger a comunicação interna entre os componentes da solução FinID contra ataques de indisponibilidade, modificação, vazamento, destruição e falha.

A recomendação é estabelecer uma arquitetura de rede considerando a segmentação, regras de controle de acesso à rede e monitoramento.

5.1.13 Resposta a incidentes (SC14)

A resposta a incidentes se aplica aos ativos da solução FinID que requerem uma resposta organizada no caso de um incidente de segurança para lidar com a situação, de maneira a limitar os danos e reduzir o tempo e os custos de recuperação.

A recomendação é definir um plano de comunicação e recuperação relacionado à disponibilidade operacional da solução FinID.

Outro ponto está relacionado à LGPD que, segundo a declaração relacionada aos direitos dos titulares dos dados, o art. 58 diz que "O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares". Isso ocorrerá num prazo ainda a ser definido pela ANPD (LGPD, 2019]. Dessa forma, a

recomendação é definir um plano de resposta a incidentes que também deve estar em conformidade com os regulamentos do LGPD.

5.1.14 Avaliação de segurança (SC1)

A avaliação de segurança é um controle que identifica as vulnerabilidades reais em todos os componentes da solução, identificando as vulnerabilidades técnicas, humanas ou físicas e faz parte da avaliação de riscos. Identificar a verdadeira fraqueza em cada componente é importante para evitar a falsa sensação de segurança (V28).

A recomendação é definir o escopo da avaliação de segurança na solução FinID, estabelecendo a periodicidade do vínculo com o gerenciamento de segurança e riscos (SC13). O escopo pode incluir avaliação de segurança específica, como análise de caixa branca, teste de mesa ou análise de código estático.

5.1.15 Operações de segurança (SC15)

Operações de segurança é um controle relacionado às atividades diárias de segurança executadas para garantir o nível de segurança da solução FinID.

A recomendação é definir as regras, responsabilidades e atividades relacionadas à manutenção da estratégia de segurança da solução FinID. Algumas questões principais nas operações de segurança são: monitoramento de segurança, avaliação de conformidade, gerenciamento de chaves criptográficas, gerenciamento de usuários e segurança de ativos.

5.1.16 Segurança de ativos (SC9)

Segurança de ativos é um controle geral que, no contexto da solução FinID, está relacionado diretamente ao controle das informações sobre o ativo.

A recomendação é estabelecer um mecanismo para gerenciar os ativos e seus atributos, a fim de auxiliar no processo de monitoramento e conformidade definidos na política de segurança (SC12).

6 Contribuições ao SFN

A inovação está presente na solução FinID não só nos seus aspectos técnicos, nos de cadastramento e uso da identidade digital, mas também nos modelos de negócio associados.

Do ponto de vista tecnológico, a grande inovação está associada à identidade digital autossoberana ou descentralizada. Trata-se da nova geração de identidade digital, com muitas iniciativas globais relacionadas com desenvolvimento de *frameworks* de desenvolvimento, construção de redes DLT globais e discussões de padronização. Neste contexto, vale destacar as seguintes inovações:

- uso de DLT para armazenamento de identificadores descentralizados e *schemas* e rede de computador distribuída para suportar a rede DLT;
- técnicas avançadas de criptografia e assinaturas digitais, com destaque para o uso de um sistema de gerenciamento de chaves criptográficas descentralizadas (DKMS);
- uso de credenciais verificáveis associadas à carteira eletrônica do consumidor;
- uso de inteligência artificial habilitando o uso de biometria.

A inovação nos processos de cadastramento e uso da identidade digital do consumidor é bastante ampla e disruptiva. Atualmente, o processo de criação de contas e outros tipos de credenciamento e identificação, por vezes, ainda é feito de forma presencial e nas agências das instituições financeiras, o que torna o processo caro, burocrático e pouco prático para o usuário, principalmente aquele que precisa ou deseja ter mais de um relacionamento institucional.

Com o advento dos bancos digitais, houve melhora significativa no processo de criação dessas contas, permitindo que o usuário possa, de forma remota e totalmente digital, solicitar a abertura de conta e consequentemente a geração de uma credencial para identificação.

A inovação dos bancos digitais, apesar de trazer evidentes ganhos em termos de praticidade e conforto ao usuário, ainda manteve o conceito de silos de credenciamento e identificação: para cada instituição com a qual o usuário queira relacionar-se, ele é obrigado a passar por um novo processo de identificação e credenciamento. A liberação de sua credencial e, por consequência, a criação de uma conexão/relacionamento entre instituição e tomador final ainda pode demorar dias para ser concluída.

Com a utilização da solução FinID dar-se-á a criação de uma credencial financeira única e a automatização por meio de recursos computacionais para a criação de vínculo institucional entre as partes, desde a criação formal de uma conexão institucional, o consentimento ao acesso à credencial, sua apresentação até a liberação de acesso aos serviços, de forma totalmente automática e transparente.

Além de trazer uma disrupção tecnológica e conceitual acerca do credenciamento e *onboarding* de novos usuários, a solução também visa trazer maior naturalidade para o processo de pagamentos, habilitando o usuário final da solução a criar conexão com pessoas e outras instituições por meio de seu aplicativo móvel, a exemplo do que hoje já acontece com as redes sociais. Ao criar conexões entre pessoas por meio das credenciais financeiras a solução permite uma nova forma de inicialização de pagamentos.

Essa nova abordagem permite que os clientes controlem suas identidades, seus relacionamentos com instituições financeiras e decidam o que, quando e com quem compartilhar essas informações por meio de *open banking*. Isso permite uma nova experiência aos clientes do sistema financeiro que agora podem abrir, portar e movimentar diversas contas e identidades com facilidade e transparência nunca antes vistas.

Do ponto de vista de modelos de negócios, o FinID inova ao criar um novo ecossistema de identidade digital, no qual seus atores poderão se beneficiar de diferentes formas, a depender dos modelos de negócio a serem adotados.

Seguem alguns exemplos:

- consumidores: os usuários do FinID poderão ser remunerados pelo compartilhamento dos seus dados pessoais pelos demais atores do ecossistema de identidade digital;
- emissores de credenciais verificáveis: o ecossistema de identidade digital poderá remunerar os emissores de credenciais verificáveis tais como os fornecedores de serviços financeiros e outras instituições consideradas confiáveis como as concessionárias de energia elétricas e prestadoras de serviço de telecomunicações, entre outras;
- emissor de identidade digital: poderá ser remunerado não só pela emissão da identidade digital como também pelo monitoramento e análise de informações e pela oferta de serviços de *backup* de credenciais;
- governança da rede DLT: a solução demanda a gestão, administração e operação da rede DLT, a qual poderá ser remunerada de diferentes formas, tais como taxa de adesão, pagamentos mensais de uso, emissão de credenciais, revogação de credencias, entre outras.

7 Contribuição para o SFN

A principal contribuição que a solução do FinID entrega diretamente ao SFN é a desburocratização no setor nos processos interativos de produtos e serviços financeiros, pois, por meio da reutilização de uma credencial para a criação de vínculos e credenciamento, os tomadores de serviços financeiros não precisarão mais dar preferência apenas às instituições com as quais já possuem relacionamento. Isso tornará o acesso aos serviços financeiros tão simples e prático quanto o acesso a serviços e produtos dos demais seguimentos, sejam eles digitais ou não.

Além disso, com a utilização da solução, os bancos e os agentes financeiros poderão conhecer melhor os seus clientes. Ao tomar ciência do seu perfil e suas conexões com outras instituições, essas instituições estarão habilitadas a realizar propostas mais justas e aderentes

às aspirações dos tomadores finais, ofertando assim soluções mais pertinentes e podendo vir a fazer cobranças de taxas apenas para o que o tomador final realmente está utilizando.

Resolvendo o credenciamento e munindo os potenciais tomadores de serviços financeiros com uma credencial para utilização imediata, a solução entrega ao SFN uma facilidade, principalmente para *startups* do setor financeiro (*fintechs*), uma vez que ao iniciarem suas operações, em geral começam com pouca ou nenhuma carteira de clientes habilitados a interagirem com suas plataformas e soluções. Com o uso do FinID, as instituições automaticamente estarão aptas a interagir com os tomadores de serviços financeiros que estejam credenciados na solução.

Ao conectar de forma segura e transparente os tomadores de serviços financeiros entre si e com os agentes financeiros, a solução cria uma rede de relacionamentos que pode ser usada para habilitar e inicializar serviços financeiros como, por exemplo, a inicialização de pagamentos instantâneos. A solução também cria, por consequência, uma rede de confiança e reputação, na qual as conexões do tomador final podem atestá-lo como um bom participante ou não, beneficiando assim os bons tomadores e protegendo o setor dos maus consumidores.

Com isso, a solução trará a todo o SFN maior eficiência, desburocratização, agilidade e economia na execução dos processos para credenciamento de novos clientes no setor. Além disso, a solução trará liberdade aos tomadores finais, de poder adquirir serviços financeiros que sejam melhores, sem se restringirem aos serviços ofertados pelas instituições com as quais já têm vínculo, criando maior competitividade para o setor.

8 Restrições

A solução do FinID claramente traz um poder e controle ao usuário acerca de sua identidade de forma nunca antes experimentada no setor, principalmente na era digital. Mas também se faz necessário ressaltar as novas responsabilidades que essa abordagem traz, como a realização de *backups* e o armazenamento seguro dele, uma vez que a perda de sua carteira digital pode implicar em contratempos e custos com os agentes emissores envolvendo processos de revogação e remissão de credenciais.

Um dos principais desafios para a adoção dessa solução é a criação de uma rede *blockchain* para o gerenciamento descentralizado desse ecossistema. O modelo de governança e operação dessa rede ainda precisa ser desenvolvido e elaborado, trazendo os agentes participantes, tais quais as instituições emissoras, bancos e agentes financeiros, ainda que cada um com papéis específicos, para participarem dessa rede.

Estudos de usabilidade para aprimorar a experiência das pessoas com a solução precisam ser realizados, para garantir que o emprego desta tecnologia se torne mais natural, acessível e prático comparado ao conceito atual de silos para a interação com serviços financeiros.

Deverão ser desenvolvidas integrações com as APIs de *open banking* e também de pagamentos instantâneos, tanto para a emissão de credenciais mais elaboradas quanto para a utilização da solução para outros serviços além do gerenciamento de identidades e credenciais.

Por fim, atividades de *design thinking* e análises de mercados serão necessárias para melhor definir qual o modelo de negócio a ser proposto para o setor financeiro.

9 Conclusão

A transformação digital é um advento global que contempla várias dimensões, tais como a transformação do conhecimento, da comunicação e do tratamento de dados, por meio da implementação de novas tecnologias digitais. Tal revolução apresenta várias oportunidades para diferentes setores da economia, assim como vários desafios.

O governo brasileiro vem adotando algumas medidas para impulsionar a transformação digital beneficiando diferentes setores da economia. Dentre elas, destaca-se a "Estratégia Brasileira para a Transformação Digital", elaborada pelo Ministério da Ciência, Tecnologia, Inovações e Comunicação, com o apoio de todo o setor de produção, da comunidade científica, acadêmica e principalmente da sociedade civil.

No setor financeiro brasileiro a transformação digital também ocorre de forma intensa. Duas importantes iniciativas do Banco Central do Brasil estão em andamento e, uma vez implantadas, causarão uma grande transformação no setor: (i) sistema financeiro aberto (*open banking*) e (ii) a nova plataforma de pagamentos instantâneos, ambas já implantadas com sucesso em vários países.

A implantação de tais iniciativas vem trazendo grandes desafios para os fornecedores de soluções, tais como usabilidade, escalabilidade, performance, segurança, privacidade, entre outros. De forma mais específica, tais soluções devem estar aderentes à LGPD brasileira.

A implantação e utilização exitosa de tais iniciativas tem como caminho crítico a resolução de um problema intrínseco do mundo digital, desde a criação da internet. A inexistência de uma solução de identidade digital segura, de fácil utilização, com foco no usuário, de baixo custo oferece funcionalidades para que ele assuma o papel de gestor dos seus dados pessoais.

O surgimento das DLTs viabilizou o desenvolvimento de uma nova geração de soluções de identidade digital denominadas identidade digital descentralizada ou autossoberana, desenvolvida para resolver este problema. Por essa razão, o FinID foi desenvolvido com base na identidade digital descentralizada. Portanto, trata-se de uma solução totalmente alinhada com as mais recentes iniciativas globais de identidade digital de pessoas, que tem funcionalidades distintas das soluções convencionais disponíveis no mercado, trazendo benefícios para todos os atores envolvidos nas duas iniciativas do Banco Central.

O FinID fornece uma identidade digital financeira única para o consumidor, descentralizada, segura, aderente à LGPD do Brasil e possibilita a interoperabilidade com soluções de várias organizações. Trata-se de uma solução focada no consumidor, que facilita seu acesso a produtos financeiros de instituições com as quais ele não necessariamente tem vínculo, estimulando a competitividade do mercado financeiro. Destaca-se a utilização do conceito de carteira eletrônica armazenando o conjunto de certificações associadas aos seus dados pessoais, que constitui a sua identidade digital. A solução suporta um relacionamento financeiro digital seguro com outra pessoa, para inicialização e consolidação de pagamentos instantâneos.

Para o fornecedor de serviços financeiros, o FinID também traz benefícios, tais como a diminuição de custos associados aos processos de KYC, a possibilidade de ofertar serviços aos consumidores fora da sua base e receitas associadas à oferta de serviços relacionados à identidade digital descentralizada.

O FinID poderá viabilizar o surgimento de um novo ator no ecossistema, o emissor da identidade financeira, que será encarregado, entre outras atribuições, da emissão de credenciais, desde identidades básicas para acesso e usufruto de serviços ordinários,

até mesmo de análises mais detalhadas para emissão de identidades a serem usadas no mercado financeiro. Ele poderá oferecer serviços para *backups* de credenciais financeiras, assim como ofertar serviços de monitoramento e análise das informações geradas pelas instituições financeiras.

Para o Banco Central, o FinID traz a oportunidade de fazer a governança da rede DLT, junto às demais instituições financeiras, a fim de regulamentar e agenciar a gestão e o uso dessas identidades digitais financeiras, com o objetivo de proteger o mercado financeiro, trazendo ganhos aos consumidores brasileiros.

Em termos de modelos de negócio, a grande inovação trazida pelo FinID é a possibilidade da monetização de alguns atores do ecossistema. A depender do modelo adotado, o consumidor poderá receber uma receita pelo compartilhamento dos seus dados pessoais e a instituição financeira poderá também ter uma receita associada à emissão de credenciais verificáveis demandadas pelo ecossistema.

Por fim, o FinID apresenta-se como uma solução de identidade digital inovadora em vários aspectos, que trará benefícios para todos os atores associados à nova plataforma de pagamentos instantâneos e do sistema financeiro aberto, assim como oportunidades de surgimento de novos atores nesses ecossistemas.

Referências

ABNT/CEE-307. Blockchain e tecnologias de registro distribuídas – Conceitos e elementos da tecnologia Blockchain – Parte 6: Segurança, privacidade e identidade. Disponível em: <https://isolutions.iso.org/ecom/livelink/fetch/54235805/54235807/54250561/70060171/P_307.000.000-001_Parte_06_Ago19.pdf?nodeid=70043683&vernum=-2>. Acesso em 09/08/2019.

ALI, M., Nelson, J., Shea, R., Freedman, M. J. 'Blockstack: A Global Naming and Storage System Secured by Blockchains'. 2016 USENIX Annual Technical Conference (USENIX ATC 16), Denver, CO, 2016, pp. 181–194. Disponível em: https://www.usenix.org/node/196209. Acessado Agosto 2019.

ALLEN, Cristopher. The Path to Self-Sovereign Identity. Disponível em: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html. Acesso em: 24/10/2019.

BENNET, Colin. Regulating privacy: data protection and public policy in Europe and United States. Ithaca, New York: Cornell University Press, 1992.

CAMERON, K. The Laws of Identity. Microsoft Corporation. Nov 2005. Disponível em: https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf. Acessado Setembro 2019.

COTS, Márcio, Oliveira, Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. 1ª. Edição. São Paulo: Thomson Reuters Brasil, 2018.

FALKON, Samuel. The Story of the DAO — Its History and Consequences. Disponível em: https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences71e6a8a551ee. Acesso em: 26/10/2019.

HYPERLEDGER. Hyperledger Indy. Disponível em: https://www.hyperledger.org/projects/hyperledger-indy. Acesso em: 29/10/2019.

REED, Drummond, Law, Jason, Hardman, Daniel , Lodder, Mike. DKMS (Decentralized Key Management System) Design and Architecture V3. Disponível em: https://github.com/hyperledger/indysdk/blob/677a0439487a1b7ce64c2e62671ed3e0079cc11f/doc/design/005dkms/DKMS%20Design%20and%20Architecture%20V3.md .Acesso em: 09/08/2019.

ISO/IEC. ISO/IEC 24760-1:2019 – Information technology – Security techniques – A framework for identity management – Part1: Terminology and concepts. May 2019. Disponível em: https://www.iso.org/standard/77582.html. Acesso em: 29/10/2019.

ITU-T. TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU. Technical Specification FG DLT D1.1 - Distributed ledger technology terms and definitions Agosto, 2019. Disponível em: https://www.itu.int/en/ITUT/focusgroups/dlt/Documents/d11.pdf. Acesso em 26/10/2019.

LEORATTI, Alexandre. Para ministro do STJ, LGPD gera 'mais dúvidas do que certezas'. Jota, 11/12/2018. Disponível em: https://www.jota.info/paywall?redirect_to=//www.jota.info/justica/lgpd-revisaojurisprudencia-stj-11122018. Acesso em: 02/02/2019.

LGPD. Lei Geral de Proteção de Dados - Lei Nº 13.709, de 14 de Agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acessado em Setembro de 2019.

LIBRA, Whitehead. Uma introdução ao Libra. Disponível em: file:///C:/Users/reynaldo/Downloads/.LibraWhitePaper_pt_BR_Revised101319.pdf. Acesso em: 26/10/2019.

NAKAMOTO, S. A Peer-to-Peer Electronic Cash System. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 29/10/2019.

NAKAMURA, E.T., Ribeiro, S.L. A Privacy, Security, Safety, Resilience and Reliability Focused Risk Assessment Methodology for IIoT Systems. June 2018. IEEE Global Internet of Things Summit (GIoTS).

NAKAMURA, E.T., Ribeiro, S.L. Context-Based Blockchain Platform Definition and Analysys Methodology. The 18th International Conference on Security and Management (SAM19), Las Vegas, United States, July 2019.

O'DONNELL, D. The Current and Future State of Digital Wallets. 1ª Edição. Canadá, Creative Commons, 2019. Disponível em: https://www.continuumloop.com/get-digitalwallet-report. Acesso em: 29/10/2019.

OPPLIGEER, R. Microsoft .NET Passport and identity management. Information Security Technical Report, 2004. Disponível em: https://www.researchgate.net/publication/238470042_Microsoft_NET_Passport_and_identity_management. Acesso em: 29/10/2019.

OWI. Blockchain and Identity in 2018: A Year of Promise and Pilots. Disponível em: https://oneworldidentity.com/product/blockchain-identity-2018-year-of-promise-pilots/. Acesso em: 26/10/2019.

KOEMANN D, Rubin A. Risks of the passport single signon protocol. IEEE Computer Networks 2000. Disponível em : https://www.cs.jhu.edu/~rubin/courses/sp03/papers/passport.pdf. Acesso em: 29/10/2019.

RAUCHS, Michael *et al. Distributed Ledger Technology Systems - A Conceptual Framework.* Agosto, 2018. Disponível em:<https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternativefinance/downloads/2018-10-26-conceptualising-dlt-systems.pdf>. Acesso em: 26/10/2019.

REED, Drummond. The Story of SSI Open Standards Background on the Foundation of Self Sovereign Identity: DIDs, DKMS, DID Auth and Verifiable Credentials. Disponível em: https://ssimeetup.org/story-open-ssi-standards-drummond-reedevernym-webinar-1/. Acesso em: 09/08/2019.

RIBEIRO, S. L., Nakamura, E. T. Context-Based Blockchain Platform Definition and Analysys Methodology – Results from the application in the BlockIoT Project. International Conference on Advances in Cyber Security, Penang, Malaysia, August 2019.

SHOCARD SITA. Travel Identity of the Future – White Paper. 2016. Disponível em: https://shocard.com/wp-content/uploads/2016/11/travel-identity-of-the-future.pdf. Acesso em: 29/10/2019.

SOVRIN, Whitepaper. Sovrin™: A Protocol and Token for SelfSovereign Identity and Decentralized Trust. Disponível em: https://sovrin.org/wp-content/uploads/SovrinProtocol-and-Token-White-Paper.pdf. Acesso em: 26/10/2019.

STEINER, Peter. On the Internet nobody knows you are a dog. Disponível em: https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog. Acesso em: 26/10/2019.

TAPSCOTT, D.; Tapscott, A. 'Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World'. First edition. New York: Portfolio/Penguin, 2016.

THE WHITE HOUSE. National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy, Apr 2011. Disponível em: https://www.hsdl.org/?view&did=7010. Acesso em: 29/10/2019.

UNITED NATIONS. Transforming our world: the 2030 agenda for sustainable development. Sep 2015. Disponível em: https://www.unfpa.org/resources/transformingour-world-2030-agenda-sustainable-development. Acesso em: 29/10/2019.

W3C Community Group. Decentralized Identifiers (DIDs) v0.13 - Data Model and Syntaxes. Disponível em: https://w3c.github.io/did-core/ . Acesso em: 09/08/2019.

WORLD BANK GROUP. Distributed Ledger Technology (DLT) and Blockchain. Disponível em: http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WPPUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf. Acesso em: 26/10/2019.

ZYSKING, Guy et al, Decentralizing Privacy: Using Blockchain to Protect Personal Data (2015) IEEE Security and Privacy Workshops.

ZOOKO, W. Names: Distributed, Secure, Human-Readable: Choose Two. May 2017. Disponível: https://www.cs.princeton.edu/courses/archive/spr17/cos518/papers/zookotriangle.pdf. Acessado Setembro 2019.