lab

Laboratório de Inovação Financeira

Considerações Teóricas: Finanças Descentralizadas (DeFi) e Identidade Digital

ABDE Associação Brasileira de Desenvolvimento

BID

CVM Comissão de Valores Mobiliários

cooperação alemã

giz

Supported by: Federal Ministry for Economic Affairs and Climate Action; IKI International Climate Initiative

on the basis of a decision by the German Bundestag

Agradecemos a todas as instituições que participam da Frente de Trabalho de DeFi & Criptoativos no tema de Identidade Digital do Subgrupo de Inovação e Soluções do Mercado do Grupo de Trabalho Fintech do LAB (GT Fintech) e que contribuíram direta ou indiretamente para o conhecimento adquirido e elaboração desta publicação.

Rio de Janeiro, Janeiro de 2023

Coordenação da publicação:
Paloma Sevilha - BEE4

Agradecimentos especiais aos participantes:
Carlos Maurício Mirandola - Consultor Independente
Courtnay Guimaraes Junior – Avanade
Daniel de Paiva Gomes - VDV Advogados
David Casz Schechtman – Consultor Independente\
Eduardo de Paiva Gomes - VDV Advogados
Fernando Marino - CPQD
Gladstone Arantes – BNDES
Janaina Moraes - CIP
Jose Reynaldo Formigoni Filho - CPQD
Maria Teresa Aarão - CPQD
Paloma Sevilha - BEE4

Consultora do GT Fintech:
Gabriela Goulart

As opiniões expressas neste documento são uma manifestação técnica do conjunto de entidades do Subgrupo de Inovação e Soluções do Mercado e não representam necessariamente a opinião das instituições, das entidades gestoras do LAB ou dos seus associados ou membros, individualmente.

SUMÁRIO

1. Introdução

DeFi e Criptoativos e Identidade Digital

Atentos à importância e aos avanços das discussões e possíveis aplicações de tecnologias denominadas por DLTs *(Distributed Ledger Technologies)*, o GT Fintech, do Laboratório de Inovação Financeira (LAB), vem se dedicando ao estudo do tema há algum tempo. Após dois anos de pesquisa que deram origem à publicação *"Descentralizar para desintermediar: estudo sobre emissão, distribuição e negociação de valores mobiliários digitais no Brasil"*[1] e ao documento que consolida o resultado da consulta pública sobre essa publicação[2], o GT Fintech decidiu avançar no debate sobre Finanças Descentralizadas (DeFi) e Criptoativos.

O objetivo foi aprofundar o estudo, a análise e o desenvolvimento de modelos e estruturas conceituais no mercado financeiro e de capitais brasileiro que se utilizem de criptoativos e de funcionalida-

[1] Disponível aqui: https://labinovacaofinanceira.com/2022/08/12/relatorio-de-conclusao-do-trabalho-sobre-valores-mobiliarios-digitais/

[2] "Relatório de Conclusão do Trabalho sobre Valores Mobiliários Digitais". Disponível aqui: https://labinovacaofinanceira.com/wp-content/uploads/2022/08/lab_valores_mobiliarios_digitais.pdf

des e modelos adotados pelas Finanças Descentralizadas, preservando a proteção aos investidores, a eficiência dos mercados e demais objetivos da regulação nacional. O desenvolvimento de modelos e estruturas conceituais também tem como propósito possibilitar a criação de protótipos no mercado financeiro e de capitais brasileiro.

De modo geral, o trabalho avançará em quatro eixos específicos: identidade digital, tema desse documento, e infraestrutura de mercado, cujo debate está ocorrendo em paralelo, além de dois outros, que serão endereçados mais à frente, sobre questões jurídicas, envolvendo o estudo de alternativas em ambiente DLT para registros cartoriais, e o último que terá o desafio de testar, por meio de pilotos, a emissão de valores mobiliários tokenizados, a partir dos estudos do grupo.

No eixo sobre Identidade Digital, o objetivo foi analisar e propor soluções para a aplicação de soluções de identidade digital auto soberanas e centradas no usuário, tanto para pessoas físicas quanto para pessoas jurídicas, no âmbito de operações do sistema financeiro e mercado de capitais. Neste sentido, os trabalhos foram divididos em duas grandes etapas: (1) estruturação de estudos teóricos, consolidados no presente documento; e (2) estruturação de testes de casos de uso (pilotos / protótipos). Tratam-se de etapas subsequentes e encadeadas entre si. Para além de cumprir a função de estimular o debate e disseminar conhecimento sobre o tema, espera-se que os resultados dos estudos teóricos sobre identidade digital sejam a base e subsidiem a etapa seguinte, de estruturação de pilotos e testes.

Objetivo do documento

Como apontado acima, o presente documento consolida os resultados do estudo teórico do GT Fintech com foco em identidade digital que se utilize de criptoativos e de funcionalidades e modelos adotados pelas Finanças Descentralizadas e que tenha como foco soluções para os mercados financeiro e de capitais.

Esse relatório tem como objetivos específicos, dispostos nas próximas seções do texto: (i) fornecer contextualização geral do tema, destacando a sua importância e possíveis benefícios; (ii) explorar os conceitos e princípios do que é Identidade Digital, com foco em Identidade Autossoberana; (iii) trazer um diagnóstico sobre as soluções e iniciativas em andamento sobre o tema, em âmbito nacional e internacional; e (iv) discorrer sobre oportunidades e desafios da aplicação de solução de ID Autossoberana, tanto no contexto de pessoas físicas quanto pessoas jurídicas.

A seção sobre Desafios e Oportunidades na Aplicação de Solução de Identidade Autossoberana aponta os modelos e es-

truturas conceituais, cujo propósito final é embasar a criação e o desenvolvimento de protótipos no mercado financeiro e de capitais brasileiro, deixando claros os benefícios tanto para os investidores quanto para as entidades reguladas.

Espera-se assim que, a partir deste estudo, a próxima etapa seja discutir e priorizar a implementação teórica de uma solução de identidade digital específica, com base no caso de uso a ser proposto, ou outros casos de uso que possam surgir durante a discussão. Nessa próxima etapa, será necessário aprofundar o debate e os estudos, principalmente no que tange a quais credenciais serão emitidas, que tipo de instituição será responsável pela emissão, e sugestões de "ID Wallets" que serão utilizadas, entre outros aspectos que possam surgir ao longo da discussão. Após esta etapa, espera-se avançar em testes práticos e pilotos dos casos de uso priorizados.

Identidade Digital no âmbito de arranjos descentralizados e potenciais benefícios

O estudo sobre as soluções de identidade digital auto soberana e como funciona sua aplicabilidade é imprescindível, principalmente no contexto de um país emergente na Era Digital, como o Brasil. Além de ser uma das principais bases para a futura arquitetura de aplicações, negócios e instituições da Internet, a chamada Web3, suas implementações (ou variações) também estão na base de movimentos ainda mais disruptivos como o DeSoc (Decentralized Society).

Considerando que o país não logrou êxito à altura de seu porte nas ondas anteriores da Internet (Web 1 e Web 2) e que a descentralização proposta por esta nova arquitetura se propõe a distribuir mais poder e renda (como buscaremos expor mais abaixo), essa nova fase pode ser uma oportunidade de inserção benéfica do país (e, principalmente, dos seus cidadãos) na sequência de revoluções tecnológicas digitais.

As soluções de identidade digital autossoberana são a evolução do que possuímos hoje com a identidade federada, caminhando para a descentralização, colocando o usuário no centro e pela primeira vez, no controle de suas informações. Os conceitos são baseados na ideia de que um usuário deve ser o principal agente responsável pela gestão de sua identidade digital, o que requer não apenas a capacidade do usuário de usar uma identidade em vários locais, mas também de ter um verdadeiro controle sobre essa identidade digital, criando autonomia, afinal os usuários são e devem ser os controladores de seus dados.

Como pano de fundo para o desenvolvimento dessas soluções, as características para a utilização da identidade digital

como a ausência de uma autoridade central, padronização, desenvolvimento utilizando conceitos de security-by-design, privacy-by-design e privacy-by-default, mecanismos de governança para garantir a confiança entre os membros da rede e conformidade com LGPD estão sendo amplamente estudadas, em especial pela W3C e DIF. Questões que serão abordadas também mais à frente.

Uma identidade auto soberana deve permitir também que os usuários façam reivindicações para ajustes nas informações contidas na identidade para incluir dados ou atributos pessoais, incluindo informações sobre o usuário que foram afirmadas por outros. No processo de criação de soluções de identidade digital autossoberana, deve-se ter o cuidado com a proteção de direitos do consumidor e proteção de dados de modo geral.

De modo similar, soluções de identidade digital corporativa têm o potencial de simplificar a identificação e verificação de empresas, com capacidade de redução dos riscos e custos para utilizar serviços financeiros e não financeiros. Adicionalmente, aumenta a capacidade de acesso à informação sobre a empresa para contrapartes, clientes, reguladores e prestadores de serviços.

De acordo com estudo da McKinsey em seu paper "*Digital identification: A key to inclusive growth*[3]", a consultoria projeta que, em 2030 a ID digital tem o potencial de criar valor econômico equivalente a 6% do PIB em economias emergentes por país, e 3% em economias maduras, assumindo altos níveis de adoção. Nas economias emergentes, grande parte do valor pode ser capturado mesmo por meio de identificação digital básica com funcionalidades essenciais.

Seguindo a análise, a McKinsey projeta que apenas as identidades digitais devem criar valor econômico equivalente a 3% a 4% do PIB em 2030. Esse impulso econômico em todo o ecossistema virá, em parte, de ganhos de eficiência, da redução de fraudes, de modelos inovadores de negócios, e da capacidade de fornecer informações confiáveis e de maior qualidade sobre as credenciais apresentadas.

O referido paper buscou analisar diferentes maneiras de utilizar a identificação, organizadas pelos papéis desempenhados por indivíduos e instituições, e concluiu que os indivíduos podem usar a identificação digital para interagir com empresas, governos e outros indivíduos em seis funções, conforme demonstra a figura abaixo:

(i) consumidores;
(ii) trabalhadores;
(iii) microempresas;
(iv) contribuintes e beneficiários;
(v) indivíduos engajados civilmente; e
(vi) proprietários de ativos.

[3] Disponível em: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

Figura 1 - Diferentes tipos de uso de ID Digital que podem criar valor

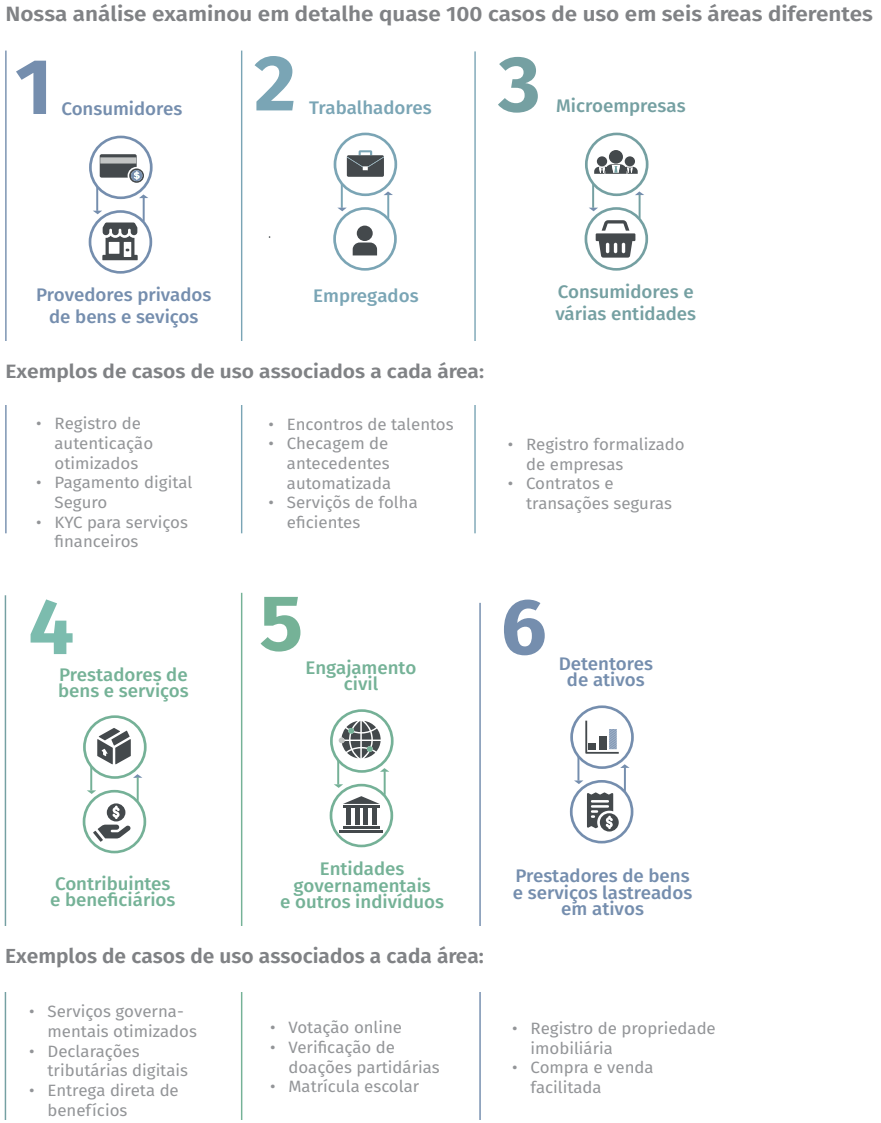

Figura 1 - Fonte: McKinsey “Digital identification: A key to inclusive growth” - tradução livre

De forma análoga, as figuras mostram que instituições também podem usar a identidade de um indivíduo em várias posições:

(i) como fornecedores comerciais de bens e serviços, interagindo com os consumidores;
(ii) como empregadores, interagindo com os trabalhadores;
(iii) como fornecedores públicos de bens e serviços, interagindo com os beneficiários;
(iv) como governos, interagindo com indivíduos de mentalidade cívica; e
(v) como registros de ativos, interagindo com proprietários de ativos individuais.

Ainda citando o paper da McKinsey, os quatro maiores fatores que contribuem para o valor econômico gerado diretamente para os indivíduos são: (i) o aumento do uso de serviços financeiros; (ii) melhor acesso a emprego; (iii) aumento da produtividade agrícola; e (iv) economia de tempo. Por sua vez, as cinco maiores fontes de valor para as instituições – tanto no governo quanto no setor privado – são: (a) economia de custos; (b) redução de fraudes; (c) aumento das vendas de bens e serviços; (d) aumen-

to da produtividade do trabalho; e (e) aumento da receita tributária.

Como citado acima, o paper aponta que, no caso das economias emergentes, o benefício potencial médio da adoção de identidade digital, por país, é de aproximadamente 6% do PIB em 2030. Grande parte desse valor poderia ser alcançado por meio de identificação digital básica com funcionalidades essenciais. No caso específico do Brasil, a McKinsey estimou um potencial de 13% de impacto no PIB em 2030, e apontou que a identidade digital pode ajudar 39 milhões de adultos a melhorar o acesso a serviços financeiros e facilitar o aumento da concessão de crédito para pessoas físicas e micro, pequenas e médias empresas.

Outro potencial benefício apontado por eles é que a ID digital pode ajudar a reduzir a fraude em diversos tipos de transações, como a redução da fraude de identidade nas interações do consumidor, contribuinte e beneficiário, até a redução da fraude na folha de pagamento nas interações do trabalhador. Para o Brasil, estima-se cerca de USD 90 bilhões de redução de fraudes em benefícios públicos de modo geral, com a adoção de soluções de ID Digital nesse processo.

Além disso, em seu estudo, a McKinsey estima que pouco mais da metade do valor econômico potencial da ID digital poderia ser acumulado pelos próprios indivíduos, tornando-se um elemento chave para o crescimento inclusivo, enquanto o restante poderia fluir para o setor privado e instituições governamentais. Além dos benefícios econômicos quantificáveis citados, a identificação digital pode trazer benefícios qualitativos aos indivíduos, tais como capacidade de impulsionar a inclusão social e política, auxiliar na proteção de direitos e aumentar os níveis de transparência. Há assim um maior potencial de impactos positivos por meio de maior inclusão social (como identificação e formalização do trabalho) e bancária de populações minorizadas, notadamente sobre mulheres. Há assim possíveis impactos com relação também às questões ASG (Ambiental, Social e Governança).

Ao longo do presente documento, será evidenciado como os estudos e as aplicações ao redor do mundo estão avançando, como o protocolo da W3C, no triângulo da confiança do sistema de identidade autossoberana, foi desenvolvido para aplicação da Identidade digital e como a rede blockchain se insere nesse contexto.

Como conclusão, , é esperado que esse documento explique o conceito de identidade digital e o valor de sua aplicabilidade, bem como aprecie os casos de usos já implantados e possa identificar possíveis oportunidades dentro desse novo cenário para o contexto local.

2. Principais conceitos sobre Identidade Digital

O que é identidade autossoberana

Identidade autossoberana (também conhecida pela sigla SSI derivada de *self-sovereign identity*) é uma abordagem para identidade digital composta por um conjunto de credenciais, características e identificadores que permitem que o sujeito da identidade tenha controle singularizado de quem terá acesso a estes aspectos da identidade. SSI, de acordo com as definições da *European Blockchain Service Infrastructure Self-Sovereign Identity*[4] ("EBSI"), é o próximo passo além da identidade centrada no usuário.

Ambos os conceitos, de identidade centrada no usuário e de identidade autossoberana, são baseados na ideia de que o usuário deve ser central para a administração de sua identidade digital, o que requer

[4] https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Terminology

não apenas a capacidade do usuário de usar uma identidade em vários locais, mas também ter um verdadeiro controle sobre essa identidade digital, criando autonomia. A diferença entre SSI e identidade centrada no usuário reside no fato de que no caso da identidade autossoberana, a mesma deve ser transportável, ou seja, respeitar o princípio da portabilidade. Dessa forma, a SSI não pode ser bloqueada em um único site ou localidade, aplicação ou fornecedor específico.

Uma identidade autossoberana também deve permitir que os usuários façam reivindicações, que podem incluir dados ou atributos pessoais, e podem até conter informações sobre o usuário que foram afirmadas por outros. Na criação de uma identidade autossoberana, devemos ter o cuidado de proteger o indivíduo, defendê-lo contra perdas financeiras e outras e apoiar os direitos humanos, como o direito de ser você mesmo e de se associar livremente.

O SSI permite que os cidadãos criem, controlem e usem sua própria identidade digital (incluindo identificação, autenticação e muitos outros tipos de informações relacionadas à identidade) sem precisar depender de uma única autoridade centralizada. A administração pública e outras organizações podem viabilizar o fornecimento de serviços que sejam juridicamente vinculativos e compatíveis com a regulação.

Desta forma, defini-se assim os princípios da identidade autossoberana - SSI:

1. **Existência**: a identidade deve existir, independentemente de quem a emitiu;
2. **Controle**: realizada pelo usuário e gerida pelo próprio com quem ele quer compartilhar suas informações;
3. **Acesso**: acessibilidade e permitir que ela seja utilizada;
4. **Transparência**: como e para quais fins os dados estão sendo utilizados;
5. **Persistência**: não pode ser apagada, precisa ter uma perenidade;
6. **Portabilidade**: pode portar a identidade, o que não dá para fazer hoje, exemplo com ativos digitais, poder portar de uma carteira A para uma carteira B;
7. **Interoperabilidade**; capacidade e estruturação de meios para que diferentes sistemas se comuniquem entre si, buscando se beneficiar de conexões transparentes e padronizadas;
8. **Consentimento**: os dados só serão acessados, mediante consentimento do usuário;
9. **Minimização**: apresentação de dados que são realmente necessários;
10. **Proteção :** apresentação de dados que são realmente necessários;
10. **Proteção:** conjunto de mecanismos, infraestrutura e protocolos cujo objetivo é mitigar e minimizar a concretização de riscos, de forma a garantir a segurança e integridade dos dados armazenados, trafegados e processados.

Além dos princípios citados acima, a Gartner traz em uma de suas análises[5], a possibilidade de um princípio adicional, o da **Neutralidade.** De acordo com a matéria, a *Digital Identity Neutrality* consiste em permitir o uso, a emissão e a guarda do ID Digital e seus dados de uma forma inclusiva, justa, e segura. Isso significa permitir, ou até mesmo exigir, que organizações aceitem qualquer Identidade Digital que seja comprovada e verificada, sem necessariamente favorecer a ID Digital emitida por ela mesma.

Dessa forma, o conceito de neutralidade vai um pouco além do princípio da Portabilidade, ao passo que o primeiro consiste em organizações aceitarem qualquer identidade digital que seja comprovada e verificável, sem qualquer preconceito ou favorecimento apenas à identidade digital emitida em suas próprias plataformas. A Gartner explora o conceito de neutralidade da ID Digital fazendo uma analogia com a neutralidade da rede, ou seja, modelo no qual os provedores de serviços da Internet devem tratar todas as comunicações da Internet igualmente. De forma semelhante ao que o modelo de neutralidade da rede conseguiu atingir, ao permitir a economia conectada, a neutralidade da identidade seria a base para viabilizar a economia programável, por meio da propriedade digital e da responsabilidade no mundo físico e virtual.

De modo resumido, podemos dizer que Identidade Autossoberana é uma solução de identidade digital na qual o usuário assume um papel central na administração de sua identidade, o que significa deter o controle sobre a mesma. A solução deve permitir que os usuários criem, controlem e usem sua própria identidade digital, incluindo identificação, autenticação e outros tipos de informações relacionadas à identidade, sem precisar depender de uma única autoridade centralizada.

O metassistema de identidade autossoberana (uso por meio de DLT)

As primeiras referências relacionadas com o conceito de SSI datam de 2012, porém as primeiras iniciativas de desenvolvimento ocorreram a partir de 2015 (Reed 2021). Do ponto de vista tecnológico, pode-se dizer que SSI é um conjunto de tecnologias que se baseiam em conceitos de gerenciamento de identidade, computação distribuída, DLT e criptografia. Esses conceitos centrais foram estabelecidos ao longo de décadas. A novidade é como eles são reunidos para criar um novo modelo de gerenciamento de identidade digital.

Embora a SSI esteja muito relacionada com a identidade de pessoas e suas necessidades individuais de segurança, privacidade e controle de dados pessoais, o modelo também se aplica às organizações e coisas. Na verdade, se aplica a qual-

[5] Gartner. Some Thoughts on Why Digital Identity Neutrality Matters. Disponível em: https://blogs.gartner.com/homan-farahmand/2022/08/02/some-thought-on-why-digital-identity-neutrality-matters/

quer entidade que precise de identidade segura na internet. Seguem as principais características de um sistema SSI:

a. Ausência de uma autoridade central;
b. Infraestrutura baseada em blockchain;
c. Uso de tecnologias baseadas em padrões;
d. Foco no usuário, uma vez que ele define quais, como e onde os seus dados serão utilizados;
e. Elevados níveis de segurança e privacidade;
f. Mecanismos de governança para garantir a confiança entre os membros da rede; e
g. Conformidade com o Regulamento Geral de Proteção de Dados da União Europeia (GDPR em inglês) e a Lei Geral de Proteção de Dados (LGPD) brasileira, uma vez que dados pessoais não são colocados na rede blockchain.

Um sistema SSI é flexível, permitindo que seja usado em uma ampla variedade de aplicações e fornece controle e privacidade em sua arquitetura e implementação.

Conforme mostra a Figura 2, existem três atores fundamentais:

a. O usuário, que é proprietário da identidade que terá sua identidade digital constituída por uma ou mais credenciais verificáveis, as quais serão estar armazenadas em uma carteira digital, sob o controle dele;
b. O emissor de credenciais, que poderá ser, por exemplo, um órgão de governo, uma concessionária de energia, uma prestadora de serviços de telecomunicações ou uma instituição bancária, dentre outros;
c. O verificador de credenciais, que demanda informações do usuário para prestar-lhe algum tipo de serviço digital.

Figura 2 - Triângulo da confiança do sistema SSI

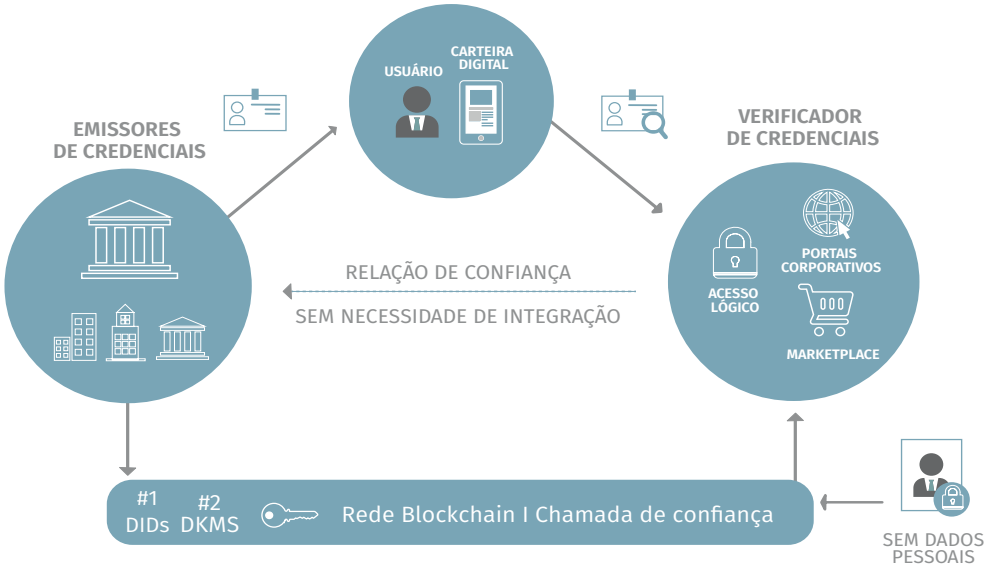

Figura 2 - Fonte: CPQD

Os principais elementos de um sistema SSI são:

a. **Carteira digital**: uma carteira digital consiste em software que permite que o usuário gere, armazene, gerencie e proteja chaves criptográficas, credenciais verificáveis, identificadores descentralizados (DIDs) e outros dados privados confidenciais. As carteiras podem ser instaladas em diferentes dispositivos, tais como smartphones e notebooks;
b. **Identificador Descentralizado (DID)**: são considerados um novo tipo de identificador global, não muito diferente das URLs. Os DIDs são a contrapartida criptográfica das credenciais verificáveis (VCs) e, juntos, são considerados os pilares da padronização SSI. Eles foram projetados para serem controlados por seu proprietário, sem qualquer meio centralizado, como uma certificação de autoridade;
c. **Credencial Verificável (VC)**: conjunto de uma ou mais reivindicações (claims) feitas por um emissor. É a representação digital de credenciais físicas, tais como uma Carteira Nacional de Habilitação (CNH), Registro Geral de Identidade (RG), diploma e certificados etc. A adição de tecnologias, tais como assinaturas digitais, torna as credenciais verificáveis menos vulneráveis e mais confiáveis do que suas credenciais físicas;
d. **Agente digital**: é um módulo de software que gerencia as interações da carteira com os demais atores do sistema, ou seja, os emissores e verificadores de credenciais. Um agente digital é para uma carteira digital o que um sistema operacional é para um computador ou smartphone;
e. **Local para registro de DIDs, chaves públicas e schemas de dados das VCs**: atualmente, grande parte das implementações utilizam blockchain para a gravação e verificação desses registros.
f. **Governança**: trata-se de um conjunto de regras mantidas por uma organização ou ainda um consórcio de organizações, que visam construir e manter as relações de confiança entre os participantes, como por exemplo, definindo quais são as instituições com o papel de emissor e, quais as credenciais estas estão aptas a emitir; ou ainda, quais carteiras digitais são seguras e podem armazenar as chaves, DIDs e credenciais verificáveis. A governança tem o objetivo de remover a necessidade da confiança sobre os dados e colocá-la na governança e tecnologia. Na figura a seguir, é possível observar o diamante da confiança baseado na governança do ecossistema.

Figura 3 - Diamante da Confiança

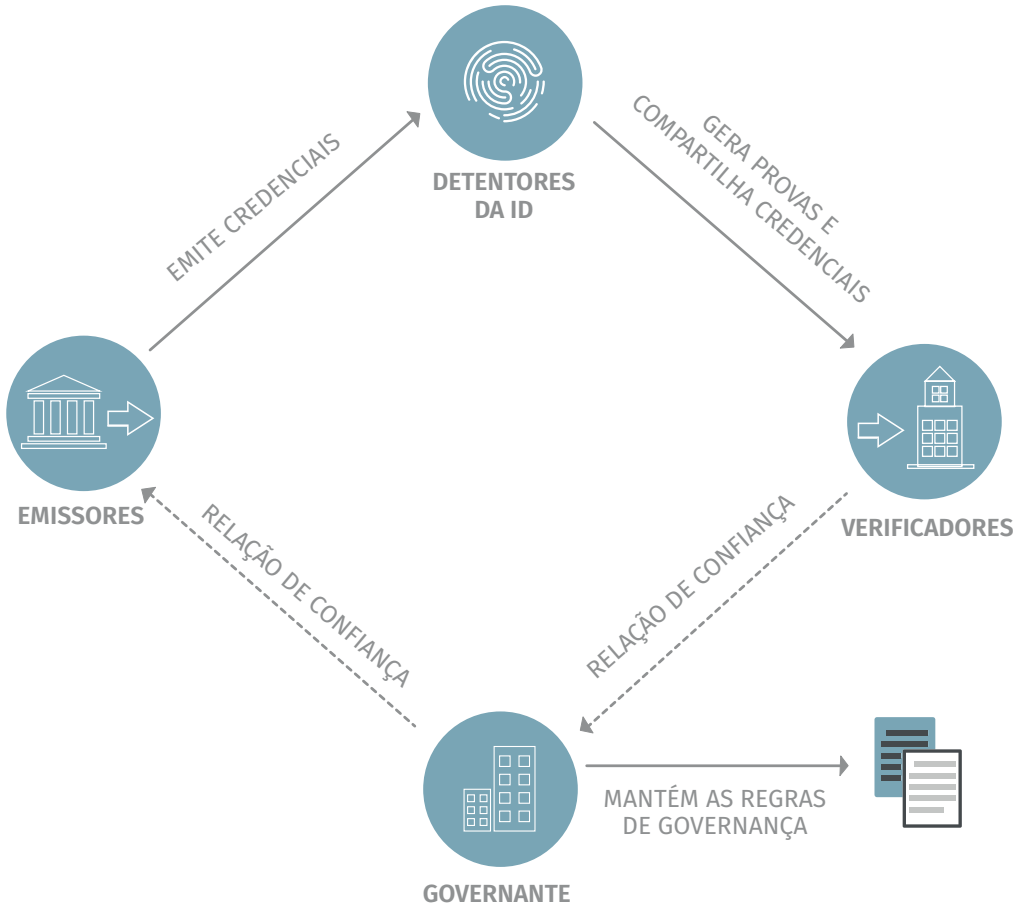

Figura 3 - Fonte: CPQD

Adoção da SSI pelo mercado

Em levantamento feito pelo W3C, órgão de padronização global da Web, os identificadores descentralizados, juntamente com as credenciais verificáveis padronizadas pelo W3C, estão sendo usados em vários segmentos onde a identificação e a autenticidade dos dados são uma preocupação[6]:

- **Governos**: os EUA, o Canadá e a UE estão explorando o uso de DIDs para fornecer documentação de identidade digital de proteção de privacidade para seus negócios e residentes, o que permite que essas entidades escolham como e quando seus dados são compartilhados;
- **Varejistas**: lojas de conveniência, mercearias, restaurantes, bares e empresas de bens de consumo nos EUA estão utilizando DIDs para novos programas de verificação de idade digital para aumentar a privacidade, a velocidade de checkout e combater o uso de documentos de identidade fraudulentos ao comprar produtos com restrição de idade;

[6] Decentralized Identifiers (DIDs) v1.0 becomes a W3C Recommendation. Disponível em: < <https://www.w3.org/2022/07/pressrelease-did-rec.html.en>. Acesso em : 05/10/2022.

- **As partes interessadas da cadeia de suprimentos**: reguladores governamentais globais, instituições de padrões comerciais, fornecedores, remetentes e varejistas - estão usando DIDs para explorar sistemas de próxima geração que verificam com mais precisão a origem e o destino de produtos e serviços, o que simplificará e permitirá que os relatórios projetados sejam aplicados para corrigir tarifas, evitar o dumping e monitorar o transbordo.
- **Força de trabalho**: universidades, programas de treinamento profissional e organizações de padrões educacionais estão adotando DIDs para emitir credenciais de aprendizado digital que são controladas e compartilhadas pelo graduado ao se candidatar a cargos de ensino superior ou força de trabalho.

Além dos mercados citados acima, que foram identificados dentro de levantamento feito pelo W3C, vale citar também os bancos e outras instituições financeiras, que coletam e verificam grandes quantidades de dados e documentos, para suas próprias operações e para atender a requisitos regulatórios. Um exemplo disso é o BankID[7] da Suécia, que permite aos cidadãos assinarem contratos, documentos de empréstimo, declaração de imposto de renda, além de poderem utilizar essa identidade eletrônica para efetuar pagamentos bem como se conectarem com plataformas.

[7] BankID: https://www.bankid.com/en

3. Iniciativas nacionais e internacionais

As primeiras implementações de sistemas SSI datam de 2016. Várias iniciativas de diferentes naturezas ocorreram desde então, tais como o desenvolvimento de componentes em comunidades de desenvolvimento de software, desenvolvimento de projetos pilotos, implantação de redes de testes e de produtos e discussões sobre padronização. A seguir são apresentadas algumas iniciativas relevantes relacionadas com SSI.

Iniciativas internacionais

3.1 Hyperledger Foundation

A Hyperledger Foundation[8], ligada à Linux Foundation, é focada no desenvolvimento de frameworks para blockchains permissionadas assim como no desenvolvimento de várias bibliotecas para facilitar

[8] About Hyperledger Foundation. Disponível em: <https://www.hyperledger.org/about>. Acesso em: 06/10/2022.

o desenvolvimento de soluções que utilizam tais frameworks. Atualmente são seis frameworks blockchain e oito projetos incubados.

Desde 2016, a Hyperledger Foundation, a partir de código doado pela startup Evernym, vem desenvolvendo infraestrutura para suportar o desenvolvimento de soluções SSI:

- Hyperledger Indy: trata-se de uma blockchain permissionada dedicada à SSI, sendo composta por ferramentas, bibliotecas e componentes reutilizáveis para fornecer identidades digitais em blockchains. A Indy é interoperável com outras blockchains ou pode ser usada de forma independente, potencializando a descentralização da identidade;
- Hyperledger Aries: fornece um kit de ferramentas compartilhado, reutilizável e interoperável, projetado para iniciativas e soluções focadas na criação, transmissão e armazenamento de credenciais digitais verificáveis.
- Hyperledger Ursa: é uma biblioteca criptográfica compartilhada, que possibilitam o desenvolvimento de soluções SSI mais seguras. A biblioteca consiste em subprojetos, que são implementações coesas de código criptográfico ou interfaces para código criptográfico.

3.2 Decentralized Identity Foundation (DIF)

A DIF foi fundada em maio de 2017 para apoiar o surgimento de um ecossistema de tecnologias em torno da SSI[9]. A DIF tem como missão promover os interesses da comunidade de identidade descentralizada, incluindo a realização de pesquisa e desenvolvimento para avançar em bases técnicas "pré-competitivas", assim como buscar o estabelecimento de padrões que viabilizem a interoperabilidade global entre as soluções SSI. Seguem suas principais atividades:

- Elaboração de especificações técnicas: grupos de trabalho desenvolvem especificações e padrões emergentes para protocolos, componentes e formatos de dados a serem utilizados pelos desenvolvedores de soluções SSI;
- Desenvolvimento de componentes: os membros da DIF desenvolvem implementações de referência de código aberto dos componentes técnicos e protocolos utilizados em soluções SSI;
- Coordenação do ecossistema SSI: como a organização líder no tema de identidade descentralizada, a DIF procura alinhar os participantes do setor para promover seus interesses comuns.

A realização de tais atividades ocorre atualmente em 10 grupos de trabalho e 3 grupos de interesse especial (financeiro, viagem e saúde). Os resultados alcançados por tais grupos colaboram direta-

[9] About Decentralized Identity Foundation. Disponível em: <https://identity.foundation/governance/about>. Acesso em: 06/10/2022.

mente nas discussões de padronização em outras entidades, tais como IETF, W3C e Trust-over-IP.

3.3 W3C

O World Wide Web Consortium (W3C) é o principal órgão de padronização da Web. Foi fundado por Tim Berners-Lee em 1994 e possui cerca de 450 membros entre fornecedores, órgãos de governos, academia e organizações independentes. Tem por objetivo "conduzir a World Wide Web para que atinja todo seu potencial, desenvolvendo protocolos e diretrizes que garantam seu crescimento de longo prazo"[10].

O W3C vem investindo na padronização de sistemas SSI, com principal ênfase em DIDs e VCs para garantir um ecossistema de compartilhamento de dados mais descentralizado, que respeite a privacidade e que seja baseado em consentimento. O trabalho de padronização para tais tecnologias será realizado no recém-criado Grupo de Trabalho de Credenciais Verificáveis 2.0, que concentra suas atividades com base nos feedbacks do mercado. Em julho de 2022, o W3C anunciou que os Identificadores Descentralizados (DIDs) v1.0 são um padrão oficial da Web.

3.4 Trust-over-IP Foudation - ToIP

A Fundação Trust over IP (ToIP) foi lançada em maio de 2020 com 27 organizações membros. Foi gestado no ano anterior como uma confluência de vários esforços relacionados com identidade digital, credencial verificável e tecnologia blockchain. Um grupo de especialistas viu a necessidade de convergir e criar uma arquitetura interoperável para confiança digital descentralizada. Isso culminou em um artigo da Linux Foundation chamado The ToIP Stack publicado em agosto de 2019 e posteriormente se transformou em um artigo de dezembro de 2019 em uma edição especial da IEEE Communications Standards Magazine sobre identidade digital descentralizada[11].

3.5 EBSI e eSSIF LAb

No final de 2019, a União Européia lançou a European Blockchain Service Infrastructure - EBSI, que tinha como objetivo construir duas infraestruturas de rede blockchain para que os países membros pudessem, num primeiro momento, desenvolver e testar as suas aplicações. EBSI é a primeira infraestrutura de blockchain em toda a UE e foi projetada como um ecossistema voltado para o mercado, com base em padrões abertos e um modelo de governança transparente. Inicialmente, foram escolhidas as plataformas de blockchain permissionadas Hyperledger Fabric e Besu para o projeto.

Cada nó da rede EBSI é composto por três camadas:[12]

[10] Sobre o W3C. Disponível em: <https://www.w3c.br/Sobre/>. Acesso em: 05/10/2022.
[11] About ToIP. Disponível em: <https://trustoverip.org/about/about/>. Acesso em: 06/10/2022.
[12] Introducing EBSI. Disponível em: <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home>. Acesso em: 07/10/2022.

1. Infraestrutura: fornece recursos genéricos e conectividade para redes Blockchain;
2. Core de serviços: conjunto de interfaces padronizadas (APIs) que fornecem recursos para que terceiros desenvolvam aplicativos e garantam a conformidade com princípios orientadores definidos e aprovados pelo European Blockchain Partnership (EBP);
3. Armazenamento: engloba, tanto a blockchain quanto os protocolos de armazenamento off-chain atualmente suportados pela EBSI.

Um dos grupos de aplicação escolhidos para desenvolvimentos de soluções na EBSI foi o de identidade digital descentralizada. Nesse contexto, outra iniciativa relevante da Comissão Europeia é o European Blockchain Partnership, lançou o European Self-sovereing Identity Framework (eSSIF). Trata-se de uma iniciativa financiada pela UE que visa promover a ampla aceitação de SSI como uma solução de identidade digital de próxima geração, aberta e confiável para transações eletrônicas mais rápidas e seguras via Internet e na vida real.[13] Desafios do eSSIF:

- Facilitar a interação transfronteiriça com a SSI.
- Fomentar projetos SSI nacionais interoperáveis.
- Integrar soluções existentes, como o eIDAS e e-delivery com SSI;
- Conceituar e desenvolver uma camada de identidade na nova Infraestrutura de Serviços Blockchain Europeia.
- Preservar os valores democráticos europeus na implementação da identidade autossoberana.

O European Self-Sovereign Identity Framework Lab (eSSIF-Lab) pode ser considerado um ecossistema de partes que especificam, desenvolvem, experimentam e validam meios tecnológicos e não tecnológicos (por exemplo, governança) que apoiam pessoas, empresas e governos (partes) a pensar, projetar, adaptar e operar seus processos (de informação) de forma que possam negociar e realizar transações comerciais uns com os outros usando o suporte eletrônico fornecido pelas várias tecnologias de SSI[14].

Um dos projetos mais relevantes em andamento no eSSIF-Lab é o eIDAS Bridge, que busca a integração entre os sistemas de identidade centralizados e sistemas SSI. O eIDAS, cujo significado é identificação eletrônica e serviços de confiança para transações eletrônicas, é um sistema de identidade centralizado que garante a validade legal de documentos eletrônicos e serviços de confiança transfronteiriços, como assinaturas e selos eletrônicos. Para disponibilizar o eIDAS como uma estrutura de confiança no ecossistema SSI, a Comissão Europeia está desenvolvendo este projeto[15].

[13] NGI eSSIF-LAB - EUROPEAN SELF-SOVEREIGN IDENTITY FRAMEWORK LAB. Disponível em: <https://essif-lab.eu/#:~:text=EUROPEAN%20SELF%2DSOVEREIGN%20IDENTITY%20FRAMEWORK,Internet%20>. Acesso em: 06/10/2022.
[14] eSSIF Lab Vision. Disponível em: <https://essif-lab.github.io/framework/docs/essifLab-vision>. Acesso em: 06/10/2022.
[15] About SSI eIDAS Bridge. Disponível em: <https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about>. Acesso em: 06/10/2022. and%20in%20real%20life>. Acesso em: 06/10/2022.

3.6 Rede Sovrin

A Sovrin Foundation foi fundada em setembro de 2016. Atualmente, é uma fundação global sem fins lucrativos com um conselho de doze curadores e um Conselho de Governança Técnica. A Sovrin é uma rede global de identidade digital descentralizada, sendo classificada como pública e permissionada.

Trata-se de uma infraestrutura pública para suportar aplicações de SSI, porém permissionada no que diz respeito aos nós validadores da rede. Tais nós, que garantem o consenso das transações no livro-razão, se submetem à governança da Sovrin Foundation. A Sovrin utiliza a blockchain Hyperledger Indy e possui três tipos de rede: BuilderNet, StagingNet e MainNet[16]. Atualmente, a MainnNet, usada para suportar soluções em operação, possui 17 nós sendo um deles localizado no Brasil e é operado pelo CPQD.

Trata-se de uma alternativa interessante para aqueles que querem ofertar uma solução de SSI para o mercado, porém não possuem interesse e/ou recursos para criar o seu próprio consórcio. Os modelos de negócio para utilização da rede são simples e podem ser encontrados no próprio site da Sovrin Foundation.

3.7 Rede LacChain

Latin America and Caribean Chain (LACChain) é uma iniciativa do Laboratório de Inovação do Banco Interamericano de Desenvolvimento (BID LAB) que tem por objetivo acelerar a habilitação e adoção da tecnologia blockchain, incluindo SSI na região para promover a inovação, bem como para uma série de objetivos social e economicamente orientados. Oferecendo uma plataforma aberta com o mínimo de restrições, a LACChain está organizada como um consórcio para a gestão e administração de uma infraestrutura categorizada como pública-permissionada.

A LACChain possui um grupo de trabalho de identidade digital responsável pelo detalhamento dos conceitos relacionados a SSI (DIDs, VCs, carteiras digitais e blockchain, entre outros) abordando questões tecnológicas, regulatórias e de framework[17]. O LACChain também habilitou um conjunto completo de ferramentas de código aberto para permitir a compatibilidade entre serviços de identidade sobre as redes LACChain.

3.8 Testbed IDD da RNP

No primeiro semestre de 2020, a Rede Nacional de Pesquisa (RNP) lançou o Comitê Técnico de Blockchain (CT-Blockchain) é um comitê técnico de caráter consultivo para fomentar o ecossistema e acompanhar os principais avanços técnico-científicos em Blockchain e propor uma visão de futuro no tema à RNP[18].

O CT-Blockchain é assim um espaço de reflexão de pesquisadores e diversos

[16] Sovrin has three networks for self-sovereign identity. Disponível em: <https://sovrin.org/overview/>. Acesso em: 07/10/2022.
[17] DIGITAL IDENTITY - Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust. Enisa. Disponível em: <https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust>. Acesso em: 10/10/2022.
[18] CT-Blockchain. Disponível em: <https://wiki.rnp.br/display/blockchain/CT-Blockchain>. Acesso em 07/10/2022.

profissionais no tema, posicionados de maneira estratégica para fazer evoluir a tecnologia no Brasil nos seus variados escopos. O comitê é composto por seis grupos de trabalho, sendo um deles de identidade digital descentralizada e outro de infraestrutura de redes blockchain. Esses dois grupos estão envolvidos pela implantação de um testbed de rede para suporte à experimentações e desenvolvimento de aplicações IDD.

Atualmente, a rede possui 4 nós, sendo dois localizados na RNP, organizados pela gerência do GidLab, e dois no CPQD. Espera-se, para o curto prazo, a implantação de novos nós nas universidades, órgãos de governo e empresas participantes do CT-Blockchain.

3.9 Credit Union - Member Pass

Um dos primeiros projetos de SSI foi desenvolvido a partir de 2016 pela empresa americana Evernym e por uma cooperativa de crédito americana denominada Credit Union National Association (CUNA). Uma primeira versão da solução foi apresentada no Hyperledger Global Forum de 2018 na Basileia, Suíça.

A partir de 2021, algumas cooperativas de crédito iniciaram a operação de sistemas de identificação baseados em credenciais para seus clientes. Durante este ano, sete cooperativas de crédito emitiram credenciais para mais os seus clientes. O principal objetivo da CUNA é mitigar as fraudes aplicando o uso de credenciais digitais para controle de acesso lógico sem senha, acesso à call center, ATM a agências.

As cooperativas de crédito são muitas vezes pequenas e se uniram para formar organizações de serviços de cooperativas de crédito (CUSOs) que lhes fornecem os serviços que não podem construir por conta própria. Eles formaram um CUSO chamado CULedger, mais tarde renomeado Bonifii, para tornar essa visão uma realidade. Atualmente, a Bonifii oferece uma solução baseada em SSI para cooperativas de crédito chamada MemberPass[19].

3.10 British Columbia - Canadá

A Colúmbia Britânica foi pioneira no uso de SSI para simplificar os processos governamentais. Lançado em 2019, o OrgBook é a primeira iniciativa voltada para a identidade das empresas e utiliza componentes da Hyperledger Foundation (Indy, Aries e Ursa). A principal motivação da iniciativa é reduzir a burocracia associada à administração de pequenas empresas.

O OrgBook é um repositório de credenciais verificáveis, instâncias de agentes emissores/verificadores de Verifiable Organizations Network (VON), o equivalente a documentos “Permit to Operate” postados nos murais das empresas. Atua como um mercado digital, combinando

[19] Building an SSI Ecosystem: MemberPass and Credit Unions. Disponível em: <https://www.windley.com/archives/2021/06/building_an_ssi_ecosystem_memberpass_and_credit_unions.shtml>. Acesso em: 06/10/2022.

organizações que solicitam licenças a quem as emite, verificando a integridade desse processo por meio de métodos de identidade autossoberana[20]. As assinaturas permitem que qualquer pessoa receba atualizações automáticas sobre alterações no OrgBook BC, como novos registros e licenças renovadas. Uma API também suporta o uso de dados do OrgBook BC em outros sites, sistemas e processos. Recentemente, o governo lançou o "Verifiable Credentials for People" como projeto exploratório que utiliza a rede Sovrin para registro.

3.11 ID Union

No primeiro semestre de 2021, a Alemanha, com o apoio do Ministério Federal de Economia, lançou o consórcio IDunion (LEDGER INSIDE, 2021). Os parceiros incluem DB Systel, Deutsche Telekom, GS1 Germany, Robert Bosch, Siemens e outros 26 parceiros associados. O objetivo da IDunion é usar SSI para lançar uma rede de produção e implementar mais de quarenta aplicativos de identidade.
Os casos de uso variam de educação, mobilidade, e-saúde a finanças e soluções de IoT. As soluções são projetadas para cumprir os padrões internacionais de credenciais verificáveis e identificadores descentralizados (DID). Portanto, a rede utiliza os padrões estabelecidos pelo W3C, Decentralized Identity Foundation (DIF) e Trust over IP Foundation (ToIP). No médio prazo, será gerida por uma cooperativa europeia, constituída por diversos atores, compostos por empresas privadas, associações, cooperativas, instituições governamentais, instituições de ensino e outras pessoas jurídicas (IDunion, 2022).

3.12 Open Wallet Security Foundation

Em 13 de setembro de 2022, a Linux Foundation, o consórcio de tecnologia sem fins lucrativos que hospeda e promove o desenvolvimento de projetos de código aberto que inclui entre eles o núcleo do Linux e Kubernetes, anunciou a criação da Open Wallet Foundation, uma organização ligada a sua estrutura de projetos de código aberto voltada para a proposição de uma carteira digital utilizando os padrões emergentes de identificação descentraliza (https://openwallet.foundation).
O esforço colaborativo visa desenvolver software para suportar a interoperabilidade de uma ampla gama de casos de uso que incluem identidade e pagamentos. A missão da Open Wallet Foundation (OWF) será "desenvolver um engenho em código aberto de multiplos propósitos que qualquer organização possa utilizar para construir sua carteira interoperável".

Alguns dos atores de mercado que aderiram: Accenture, Avast, CVS HEalth, JCB, Open IDentity Exchange, OpenID Foundation, Okta, Ping Identity, Procivis, Trust over IP Foundation.

A OWF não pretende desenvolver uma carteira digital, oferecer credenciais ou

[20] British Columbia OrgBook – 'Tell Us Once' via Blockchain and Self-Sovereign Identity. Disponível em: <https://digitalcanada.io/bc-orgbook-tell-us-once/>. Acesso em: 06/10/2022.

definir padrões, mas "focará em construir um componente de software aberto que outras organizações e companhias poderão utilizar para desenvolver sua carteira". Outra preocupação da OWF é "definir as melhores práticas para a criação da tecnologia de carteiras digitais através da colaboração com código aberto para ser usado como ponto de partida para qualquer agente que queira construir carteiras digitais interoperáveis, seguras e que protejam a privacidade de seus usuários".

Até o final de 2022 a OWF pretende divulgar sua estrutura de governança e seus planos para atingir seus objetivos.

Iniciativas nacionais

3.13 Iniciativas Relevantes do Governo Brasileiro

No Brasil, recentemente, vem sendo desenvolvido o projeto **Real Digital, liderado pelo Banco Central do Brasil**. Inserido no contexto dos projetos de emissão de moedas digitais pelos bancos centrais (em inglês, *Central Bank Digital Currencies - CBDC*) que têm se espalhado no mundo, como apontado no site do Banco Central do Brasil[21], a Autarquia "*vem acompanhando o tema há alguns anos e em agosto de 2020 organizou um grupo de trabalho, constituído pela Portaria nº 108.092/20, para a realização de estudos sobre a emissão de uma moeda digital pela instituição. (...) Resultados preliminares foram apresentados à Diretoria Colegiada, que determinou o estabelecimento de um fórum regular para a discussão do tema com o corpo técnico do BC. As discussões conduzidas nesse fórum motivaram: a publicação das diretrizes do Real Digital em maio de 2021; realização de uma série de webinars; e o Lift Challenge Real Digital.*" Entre as considerações técnicas já divulgadas, com relação ao tema de identidade digital, destaca-se que o BCB responde, em sua página de perguntas sobre o tema[22]: "*Como o usuário tem acesso ao real digital na prática? O usuário final terá uma carteira virtual em custódia de um agente autorizado pelo BC – como um banco ou uma instituição de pagamento.*" Há, assim, uma expectativa, debatida pelo grupo que elaborou o presente documento, de que tal projeto possa ensejar uma discussão sobre identidade de alguma natureza, podendo, inclusive, envolver discussões sobre o uso de identidades descentralizadas.

Outra iniciativa relevante é a da **Rede Blockchain Brasil (RBB)**[23], lançada através de um Acordo de Cooperação Técnica estabelecido entre o BNDES e o TCU formalizado em maio de 2022[24]. De acordo com os órgãos envolvidos[25]: "*A rede pública, sem fins lucrativos, já funciona em caráter experimental e a previsão é de que a primeira aplicação descentralizada ocorra em 2023. A tecnologia busca trazer inova-*

[21] Disponível aqui:https://www.bcb.gov.br/estabilidadefinanceira/real_digital
[22] Disponível aqui: https://www.bcb.gov.br/estabilidadefinanceira/real_digital_faq
[23] Saiba mais aqui: https://github.com/RBBNet/rbb
[24] Disponível aqui: https://www.bndes.gov.br/wps/portal/site/home/imprensa/noticias/conteudo/aviso-de-pauta-lancamento-do-acordo-de-cooperacao-tecnica-entre-o-bndes-e-o-tcu-para-formacao-da-rede-blockchain-brasil
[25] Disponível aqui: https://portal.tcu.gov.br/imprensa/noticias/tcu-e-bndes-lancam-rede-blockchain-brasil-e-definem-proximos-passos.htm

ção, eficiência, transparência e integridade a atos e contratos da administração pública". De acordo com participante da RBB e um dos colaboradores deste texto, e conforme disponível em repositório público da iniciativa[26], na fase de estudos preliminares, os técnicos da RBB chegaram a iniciar um grupo de estudo sobre soluções de identidade para a própria rede, por entender que este serviço básico é um dos passos importantes para viabilizar a integração entre soluções, uma das motivações para a sua criação, inspirada no evento Blockchain.Gov, realizado no BNDES, no fim de 2019. Em fase de estruturação de sua governança, a discussão sobre o serviço básico de identidade a ser adotado é prevista para ser retomada ainda no ano de 2023.

A **Secretaria de Governo Digital** do Ministério da Economia (SGD/ME) é a responsável pela implementação do gov.br, um serviço de autenticação que é usado para dar acesso a inúmeros serviços do governo em várias esferas. Inclusive, em sua página, a SGD coloca como uma de suas prioridades "lançar da identidade digital"[27]. Neste contexto, em março de 2021, SGD e Enap[28] estruturaram uma oficina com representantes da área financeira, setor aéreo, turismo, transportes, saúde e educação sobre aprimoramentos na Identidade Digital para que possa ser utilizada pelo cidadão em transações não só com governo, mas também com o setor privado. Foram avaliadas as potencialidades do uso da identidade digital nas transações realizadas pelos cidadãos brasileiros com empresas de diversos segmentos.

Todos estes casos são de iniciativas ainda muito embrionárias, mas que indicam que identidades descentralizadas são um tema que vem crescendo em diversas instâncias do governo, o que precisa, no mínimo, ser monitorado, principalmente para evitar incompatibilidades entre soluções. Principalmente, no caso da iniciativa do Real Digital, este tem sido pensado para ser utilizado dentro de um contexto de DeFi. Logo, é preciso considerar a necessidade de convergência de iniciativas relacionadas à identidade digital, principalmente no que tange padronização e compatibilidade, uma vez que não é salutar que usuários precisem, por exemplo, usar padrões diferentes de identidades para utilizar o Real Digital para investir em valores mobiliários.

[26] Disponível aqui: https://github.com/RBBNet/rbb/blob/master/iniciativas.md
[27] Disponível aqui: https://www.gov.br/governodigital/pt-br/sisp/secretaria-de-governo-digital-sgd
[28] Disponível aqui: https://www.enap.gov.br/pt/acontece/noticias/identidade-digital-e-aprimorada-com-base-em-escuta-ao-setor-privado

4. Indicação de possíveis projetos para prototipação: desafios e oportunidades de Identidade Digital Autossoberana

Contexto das pessoas físicas

No cenário atual, pessoas físicas têm acesso a diferentes tipos de credenciais físicas ou até digitais, emitidas por diferentes organizações tais como agências governamentais, instituições de ensino, instituições financeiras, empregadores, provedores de serviço de água, luz, telefone, associações, entre outros. Os indivíduos precisam usar essas credenciais para provar sua identidade, residência, nacio-

nalidade, licenças profissionais, certificações, renda, patrimônio, entre outros tipos de informação, para poderem se relacionar com terceiros, como bancos, corretoras, empregadores e instituições de ensino, entre outros.

Da mesma forma que o indivíduo fornece essas informações manualmente, as instituições que as recebem também verificam manualmente as credenciais, algumas vezes até entrando em contato com o emissor original, ou usando ferramentas para validação de documentos, bases de antifraude. Nesse cenário, os indivíduos têm pouco controle sobre quais partes de seus dados são acessadas, com que rapidez ou quanto desses dados são retidos pelas entidades verificadoras mesmo após o término da necessidade.

Em web 2.0 as soluções ainda são construídas de forma fragmentada e em um modelo "centrado em organizações". Esse modelo, além de ter barreiras de escalabilidade, também apresenta diversos desafios de integração. Por outro lado, quando falamos em web 3.0, a ID Digital Autossoberana permite as chamadas "*verifiable claims*" - ou reivindicações verificáveis, e os "*self-contained pods*" que persistam aos dados da identidade, enquanto o controle permanece com o usuário. Ainda assim, teremos desafios a enfrentar, tais como a interoperabilidade entre diferentes "trust fabrics", principalmente para não exigir que o usuário precise de diferentes wallets para acessar diferentes serviços, além da necessidade de suportar a chamada "economia programável", por meio de digital ownership, tanto no mundo físico quanto virtual.

É nesse tocante que soluções de identidade digital autossoberana tem o potencial de impacto positivo em atividades econômicas, ao passo que permite, de forma verificável, a criação, o controle de titularidade e o consumo de ativos digitais. Adicionalmente, do ponto de vista dos indivíduos, essas soluções têm capacidade de elevar o nível de segurança, ao colocar os usuários no centro do controle de seus dados.

Sugestão de caso de uso para ser explorado pelo grupo no LAB:

Solução de Know Your Client (KYC), em inglês, ou "*conheça seu cliente*" e avaliação do perfil do investidor (*suitability*) simplificada e reutilizável para realizar cadastro de investidores em plataformas de investimento participativo (*equity crowdfunding*), oferecendo uma maneira mais simples, rápida e eficiente de verificação de identidade que possa ser compartilhada entre as plataformas.

Benefício para os investidores: experiência do usuário mais simples, maior segurança e controle no compartilhamento de dados pessoais.

Benefício para as entidades reguladas: menor custo com o processo de KYC e *suitability*, ao passo que é possível cumprir com requisitos regulatórios, com diligência, pelo uso de credenciais verificáveis.

Sobre essa sugestão de caso de uso, é interessante novamente mencionar o paper da McKinsey[29], no qual eles fazem uma distinção entre ID digital básico, que apenas permite verificação e autenticação, e ID digital com aplicações avançadas, por eles chamada de ID digital avançado ou ID avançado. Na definição da McKinzey, o ID avançado permite armazenar ou vincular informações adicionais sobre proprietários de IDs individuais e, portanto, pode facilitar o compartilhamento avançado de dados, com o consentimento informado do usuário. Programas avançados de identificação devem ser projetados com princípios de minimização de dados.

Os agregadores de dados públicos e privados precisam proteger a privacidade do usuário e ser responsáveis pelos dados que coletam e processam, enquanto os proprietários dos dados - neste caso os detentores de ID digital - precisam ser orientados e capacitados para fornecer consentimento consciente, e exercer controle sobre o uso de seus dados. Em muitos casos, as linhas entre a ID digital básica e a avançada podem se confundir porque ecossistemas digitais mais amplos podem ser construídos em cima de uma ID digital básica que permite uma capacidade subjacente de autenticação em canais digitais.

Contexto das pessoas jurídicas

A fundamentação é que a identidade digital corporativa (ID) tem o potencial de simplificar a identificação e verificação de empresas, com capacidade de redução dos riscos e custos para utilizar serviços financeiros e não financeiros. Pode, também, aumentar a capacidade de acesso à informação sobre a empresa para contrapartes, clientes, reguladores e prestadores de serviços.

No cenário atual, no Brasil existe o CNPJ para identificação de empresas. Em nível global, em 2012 o G20 introduziu o *Legal Entity Identifier* ("LEI") como um sistema universal de designação para entidades individuais, para permitir sua identificação e rastreamento em mercados globais. Essa determinação veio em linha com uma série de diretrizes após a crise financeira de 2008, e foi adotada especificamente em resposta às lacunas na identificação de pessoas jurídicas envolvidas em transações complexas. Para acessar serviços financeiros na Europa, por exemplo, é obrigatório que as empresas possuam o LEI - exigência introduzida pelo MiFIR em 2018.

Assim, o LEI serve como identificador de entidades jurídicas envolvidas em transações financeiras, com um conjunto de 20

[29] Mckinsey. Digital identification: A key to inclusive growth. Disponível em: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

caracteres alfanuméricos, cuja definição se dá pela ISO 17442. O LEI somente pode ser emitido por uma *Local Operating Unity* ("LOU") que seja certificada pela *Global Legal Entity Identifier Foundation* ("GLEIF[30]"). Por buscar fornecer sistema global de identificação corporativa, o LEI não é o mesmo que um número local de registro de empresa – que é jurisdicional por natureza.

Cabe destacar que esses números de registro locais são válidos apenas em uma determinada jurisdição, e não são padronizados e únicos entre as jurisdições. Portanto, é natural que, no contexto de transações transfronteiriças, tais como operações de investimento estrangeiro, financiamento comercial, entre outras, um identificador global seja preferível a um local.

Vale ressaltar que existem diferenças entre o LEI e o DID (Identificador Descentralizado), esse último fornece uma forma de verificação eletrônica da identidade de uma pessoa jurídica. Para ser "digital", os atributos associados a um ID digital corporativo devem ser capturados eletronicamente, armazenados e disponibilizados para potenciais usuários de dados.

Outro ponto é o fato de um DID poder conter diversas informações sobre uma entidade jurídica, por meio da emissão de diferentes credenciais verificáveis. Nesse contexto, o próprio LEI, o CNPJ, entre outros identificadores, poderiam ser emitidos na forma de credencial dentro de um DID.

No Brasil, existe a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, que foi instituída pela Medida Provisória nº 2.200-2/2001. A ICP-Brasil é uma cadeia hierárquica cuja principal função é regulamentar, gerenciar e viabilizar a emissão de certificados digitais, que servem como meio de identificação eletrônica, principalmente utilizada para formalizar e atestar a autoria de transações no ambiente virtual.

A emissão do certificado digital somente pode ser feita por meio de uma entidade certificadora, que precisa ser integrante da ICP, e ter uma classificação quanto ao seu nível de segurança. Entidades Certificadoras são entidades públicas ou privadas, cuja responsabilidade é a emissão, distribuição, renovação, revogação e o gerenciamento de todos os certificados vinculados à elas. Outra atribuição é a checagem se o titular do certificado possui a chave privada correspondente à chave pública. Existem também as Autoridades de Registro, que são vinculadas às Autoridades Certificadoras ("AC") e tem como função a criação da interface e a facilitação do contato entre usuários e ACs.

É dessa forma que a validade jurídica dos documentos eletrônicos, autenticidade e integridade, são garantidos nesse modelo. Para que haja a validação dos documen-

[30] GLEIF: https://www.gleif.org/pt/

tos, é preciso ter um par de chaves, onde uma delas é de conhecimento geral, a chave pública, e a outra é privada, ou seja, apenas o proprietário tem acesso. Esse método é chamado de criptografia assimétrica.

Conforme já demonstrado ao longo do texto, a inovação tecnológica tem o poder de dar forma à identidade digital. Isso vale, inclusive, para a ID Corporativa, ajudando a melhorar a eficiência, a integridade do mercado (maior efetividade na identificação e prevenção a fraudes), a estabilidade financeira (facilidade para identificar interconexões entre contrapartes), e a inclusão financeira - principalmente no caso dos processos de KYC e prevenção à lavagem de dinheiro e de capitais/combate ao financiamento do terrorismo (PLD/FT) das pequenas e médias empresas (SME). Entretanto, nenhum stakeholder será capaz, sozinho, de entregar todos esses benefícios e conduzir todas as mudanças necessárias. É preciso um trabalho em conjunto de diferentes stakeholders para entregar diferentes tipos de credencial verificáveis, cada qual contendo um conjunto de informações específicas e relevantes.

Nesse sentido, a publicação feita pelo *Bank for International Settlements* (BIS) "*Corporate Digital Identity, no silver bullet but silver lining*[31]" faz uma reflexão sobre os stakeholders que podem contribuir, em conjunto, para abordar os pontos problemáticos de uma ID Digital corporativa. São eles:

a. Registros corporativos: os registros são indispensáveis em qualquer solução de identificação digital corporativa. Para melhorar o seu papel, as empresas precisam de uma melhor forma para "abertura" e disponibilidade de dados (nomeadamente dados de beneficiários efetivos), além de qualidade, digitalização e conectividade de dados. Os dados devem ser verificados quanto à precisão, atualizados regularmente e serem de fácil acesso.
b. Bancos e outras instituições financeiras: essas instituições coletam e verificam grandes quantidades de dados para suas próprias operações e para atender a requisitos regulatórios, e podem usar esses dados para serviços de identificação corporativa. Mas o compartilhamento de tais dados, por exemplo, no contexto de KYC, pode ser um desafio. Em muitos casos, isso requer ação legislativa ou regulatória, como tem sido o caso em sistemas de compartilhamento de informações de crédito e sistemas de divulgação de mercados de capitais em todo o mundo.
c. Fornecedores/prestadores de serviços estabelecidos e empresas de regtech emergentes: grandes empresas atualmente sustentam a maioria dos processos de KYC e integração de bancos e empresas, e estão desenvol-

[31] BIS - Corporate digital identity: no silver bullet, but a silver lining. Disponível em: https://www.bis.org/publ/bppdf/bispap126.pdf

vendo recursos novos. Enquanto isso, as empresas de regtech mais recentes usam tecnologia inovadora para resolver pontos problemáticos em identificação e verificação ("ID&V") corporativo. Por exemplo, eles fornecem conectividade automatizada entre várias fontes de dados e ferramentas para extrair informações de documentos corporativos ou dados não estruturados.

d. Reguladores e formuladores de políticas: nos últimos anos, um número crescente de jurisdições está construindo sistemas públicos de identificação digital individual, conforme destacado pela iniciativa Identificação para o Desenvolvimento (ID4D) do Banco Mundial e refletido nos Objetivos de Desenvolvimento Sustentável (ODS) da ONU. Embora esses sistemas se relacionem com os sistemas corporativos, eles são invariavelmente separados, com oportunidades e desafios na construção de vínculos. Reguladores e formuladores de políticas têm um papel fundamental na coordenação, inclusive transfronteiriço. Isto é visto particularmente no contexto dos processos existentes relativos ao compartilhamento de informações fiscais e divulgação de beneficiários efetivos (coordenados pela OCDE), PLD/FT (coordenados pelo GAFI), derivativos de balcão (OTC) e infraestrutura financeira (coordenado pelo FSB, CPMI e IOSCO), e outros como dados de mercado de capitais (coordenado pelo IOSCO e ISSB), relatórios de crédito (ICCR) e sustentabilidade (ISSB).

O referido paper reforça que as entidades citadas acima podem contribuir sobremaneira para o progresso da identificação digital corporativa, contando com o uso inovador de tecnologia e políticas apropriadas. Ao passo que cada um desses players tem sua própria força em termos de recursos, sofisticação tecnológica e confiança do público, mas também seus próprios desafios a serem superados, vale ressaltar que não parece viável alcançar todo o potencial que o ID Digital Corporativo pode trazer apenas com ações unilaterais.

De forma análoga ao que as soluções de identidade digital autossoberanas devem oferecer aos usuários finais que são pessoas físicas, quando utilizadas por empresas, também implica no fato de essas terem maior controle sobre sua identidade. Assim, as empresas podem conceder direitos de acesso a determinados dados (credenciais verificáveis) a partes específicas. O direito de acesso a esses atributos pode ser gerenciado de forma descentralizada, de forma que os titulares da ID Digital não dependam de provedores terceiros para armazenar e gerenciar seus dados de forma centralizada. Ou seja, o consentimento e o controle são duas funções que estão no cerne da solução.

Avançando para soluções propostas para

os desafios da identidade digital corporativa, cabe destacar as baseadas no padrão de identificadores descentralizados (DIDs) proposto pelo consórcio World Wide Web (W3C).

Concebidos como um protocolo técnico, a proposta com base nos DIDs enfatiza os princípios básicos de interoperabilidade, propriedade e controle, e verificação digital. O W3C formulou os requisitos específicos para este novo tipo de identificador, sendo:

a. Descentralização: não deve haver um agente emissor central;
b. Persistência: os identificadores devem ser inerentemente persistentes, não exigindo a continuidade da operação de uma organização subjacente;
c. Verificabilidade criptográfica: deve ser possível comprovar o controle do identificador criptograficamente; e
d. "Resolvable": deve ser possível descobrir metadados sobre o identificador.

O DID também se aplica a soluções de Identidade Digital voltadas para pessoas físicas. De fato, sob vários aspectos técnicos a ID digital corporativa é bastante semelhante a ID digital individual. No entanto, diferentemente de um indivíduo, os atributos de uma empresa podem mudar com frequência, e isso traz a necessidade de atualização. Além disso, algumas empresas podem fazer parte de uma estrutura corporativa complexa, com presença em diferentes jurisdições, sendo um desafio identificar seu beneficiário final.

Nesse sentido, mesmo que o ID digital corporativo não seja uma simples extensão do ID corporativo individual, pode-se imaginar que o ID digital individual atua como um complemento para o ID digital corporativo, ao passo que permite identificar e verificar as identidades dos indivíduos que afirmam representar a corporação.

5. Conclusão e próximos passos

A presente conclusão sintetiza os principais tópicos analisados e discutidos neste relatório e aponta os próximos passos do grupo de trabalho.

Ao longo do presente relatório, foram demonstrados os limites conceituais e a metodologia de funcionamento da identidade autossoberana, uma iniciativa que, para além do fato de aumentar o acesso à informação de forma ampla (v.g.: entre clientes, contrapartes, reguladores, prestadores de serviços etc.), também tem o potencial de simplificação da identificação e verificação de indivíduos e empresas, acompanhada da mitigação de riscos e custos, sejam eles financeiros ou não.

A criação, o controle e a utilização da identidade digital são permitidas pelo SSI, sem a dependência de entidades centralizadas.

A despeito de estar fortemente relacionada à identidade dos indivíduos, enquanto pessoas naturais, a SSI também é aplicável às organizações e "coisas", ou seja, é aplicável a qualquer entidade, personificada ou não, que necessite de uma identidade segura na internet.

Vale ressaltar, conforme anteriormente demonstrado, que os estudos referentes à ideia de identidade autossoberana pressupõe a neutralidade dessa identidade, de modo a proporcionar uma economia verdadeiramente programável, daí por que a identidade digital autossoberana é uma solução por meio da qual o próprio usuário assume foros de relevância e toma o protagonismo central na administração de sua identidade mediante total controle sobre a mesma, viabilizando, repita-se, que os usuários criem, controlem e usem sua própria identidade digital, incluindo identificação, autenticação e outros tipos de informações relacionadas à identidade, sem precisar depender de uma única autoridade centralizada.

São elementos componentes da ideia de identidade autossoberana: (i) ausência de uma autoridade central; (ii) infraestrutura baseada em blockchain; (iii) uso de tecnologias baseadas em padrões; (iv) foco no usuário, uma vez que ele define quais, como e onde os seus dados serão utilizados; (v) elevados níveis de segurança e privacidade; (vi) mecanismos de governança para garantir a confiança entre os membros da rede; e (vii) conformidade às legislações de proteção de dados.

É premissa deste conceito a ideia de que o usuário é real e verdadeiro proprietário da identidade digital criada por credenciais verificáveis, por meio da utilização de uma carteira digital. Para que esta realidade seja possível, é indispensável a existência da figura do emissor de credenciais, as quais serão regularmente atestadas, conforme seu uso, pelos verificadores de credenciais.

A utilização da identidade autossoberana vem acompanhada da padronização dessa solução, associada a uma implementação pautada em princípios de security-by--design, privacy-by-design e privacy-by--default, assegurando a observância dos ditames de legislações de proteção de dados.

O presente relatório aponta, ainda, que o avanço econômico que será proporcionado pela utilização de identidades autossoberanas advém de diversos elementos, tais como, exemplificativamente: (i) redução de fraudes; (ii) criação de modelos inovadores de negócios; (iii) ganhos de eficiência; (iv) confiabilidade na transmissão de informações com maior qualidade em suas credenciais.

Importante assinalar, consoante demonstrado ao longo do relatório, que, dentre os materiais analisados, em especial o estudo da McKinsey, os próprios indivíduos poderiam acumular mais da metade do valor

econômico potencial da ID digital, sendo que tais benefícios não seriam meramente quantitativos, mas também qualitativos, o que desaguaria em maior inclusão social e política, incremento da proteção de direitos e elevação dos níveis de maturidade em termos de transparência.

O presente relatório também se preocupou em arrolar os desafios e oportunidades da identidade autossoberana envolvendo pessoas físicas e jurídicas, com foco em possíveis casos de uso para testes e pilotos.

No que tange às pessoas físicas, foi possível verificar que a ID Digital Autossoberana poderia ser utilizada para questões afetadas às diligências de Know your Cliente (KYC) ou "conheça o seu cliente"; para avaliação do perfil do investidor (*suitability*); para cadastro de investidores em plataformas de investimento participativo (*equity crowdfunding*), o que proporciona uma experiência melhor e mais simples para o usuário, com incremento da segurança e controle no compartilhamento de dados pessoais, sendo certo, ainda, que na perspectiva das entidades reguladas, ter-se-á menor custo com o processo de KYC e *suitability*, com maior velocidade e diligência no cumprimento de requisitos regulatórios.

Isso é possível graças ao fato de que as identidades digitais autossoberanas permitem que as "verifiable claims" e os "self-contained pods" persistam aos dados da identidade, e, ao mesmo tempo, mantenham o controle com o usuário.

A interoperabilidade entre diferentes "trust fabrics", por sua vez, coloca-se como um desafio a ser superado, pois não há que se demandar do usuário a utilização de várias e diferentes wallets para acesso a serviços distintos. Dessa forma, o relatório já identifica a necessidade de premente de interoperabilidade entre as diferentes wallets.

No que se refere às pessoas jurídicas, foi destacada no relatório a existência da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, que se traduz em uma cadeia hierárquica cuja principal função é regulamentar, gerenciar e viabilizar a emissão de certificados digitais, os quais são emitidos por entidades certificadoras específicas e integrantes do IPC, e são utilizados como um instrumento de identificação eletrônica. Este caso de uso poderia ser tomado como ponto de partida para uma identidade autossoberana a nível corporativo.

No presente relatório, e com referência ao documento (BIS) "*Corporate Digital Identity, no silver bullet but silver lining*", foram identificados diversos stakeholders que podem contribuir para abordar os pontos sensíveis envolvendo o conceito de ID Digital corporativa, dentre os quais foram destacados: (i) registros corporativos; (ii) bancos e outras instituições financeiras; (iii) fornecedores e/ou prestadores de

serviços estabelecidos e empresas de regtech emergentes; (iv) reguladores e formuladores de políticas públicas.
De tudo quanto exposto, o principal pilar que merece destaque refere-se à questão da interoperabilidade, ou seja, há de se pensar e estruturar frameworks e padrões de funcionamento relativamente às ID Wallets, de forma a não gerar barreiras de entrada para novos entrantes e, ao mesmo tempo, garantir que não sejam gerados ônus aos usuários com a criação de diferentes wallets desnecessariamente.

No que tange à questão da interoperabilidade é necessário um olhar para ela além da conveniência do usuário. A interoperabilidade entre diversas implementações de identidades descentralizadas não é garantida. Em especial, é preciso atentar para que se evite a criação de silos de solução dentro do próprio país, o que poderia reduzir sobremaneira o valor agregado dessas soluções que, no fim e ao cabo, só se pagam pelo efeito de rede que é gerado exatamente pela sua adoção horizontal, em diversos contextos, não apenas num silo de negócios. Nesse sentido, faz-se necessário buscar o alinhamento entre diferentes iniciativas, como as já citadas: o Real Digital, do Bacen; o gov.br, da SGD; e a RBB, do BNDES, TCU e outros.

Tal questão também deveria ser considerada em nível internacional. Sair na frente e criar um padrão brasileiro que só funciona no Brasil, mesmo que seja uma grande realização, pode rapidamente deixar de ser uma vantagem competitiva para tornar-se um problema para o país, caso o tema avance nos fóruns mundiais. Seria essencial a presença de representantes do Brasil nos fóruns de discussão do tema, com o objetivo de manter-se sempre em linha com as melhores práticas internacionais e, ainda mais importante, com capacidade mínima de influência nas escolhas adotadas, principalmente no contexto da governança e outros mecanismos mais discricionários.

Como **próximo passo**, o grupo focará em discutir e desenhar casos de uso, com objetivo de fornecer insumos para a prototipação de solução de identidade digital, buscando adequação à regulamentação e estrutura dos mercados financeiro e de capitais brasileiro. Para tanto, serão definidos os elementos, tipos necessários de credenciais e condicionantes para o desenho de um possível modelo de aplicação para identidade digital. Ou seja, o trabalho de prototipagem tem como objetivo principal apresentar à sociedade um caso de uso real, explorando soluções que facilitem a adoção tecnológica de protocolos (preferencialmente autossoberanos) e podendo, inclusive, serem identificados gargalos regulatórios.

Para embasar as discussões sobre aplicação de casos de uso, a frente fará a análise de pressupostos e incentivos para adoção de protocolos e padrões de iden-

tidade digital no Brasil. Especificamente, a frente buscará entender os fatores que poderão contribuir para o desenvolvimento, investimento e adoção, por agentes do mercado brasileiro, de tecnologias e soluções relacionadas à identidade digital. O estudo de tais fatores será aqui chamado de "economia da adoção" ("*economics of adoption*"), a ser debatido pelos membros, podendo inclusive gerar um documento complementar a este texto.


labo
Laboratório
de Inovação
Financeira