Instituto Federal de Educação, Ciência e Tecnologia da Paraíba

Campus João Pessoa

Programa de Pós-Graduação em Tecnologia da Informação

ANÁLIA CRISTINA BEZERRA TIBURTINO MEIRA

LinkedID: UMA ABORDAGEM BASEADA EM UM MANIFESTO AUTOCONTIDO E VERIFICÁVEL PARA ASSOCIAÇÃO ENTRE IDENTIDADES DIGITAIS CENTRALIZADAS E DESCENTRALIZADAS

DISSERTAÇÃO DE MESTRADO

JOÃO PESSOA

2022

ANÁLIA CRISTINA BEZERRA TIBURTINO MEIRA

LinkedID: UMA ABORDAGEM BASEADA EM UM MANIFESTO AUTOCONTIDO E VERIFICÁVEL PARA ASSOCIAÇÃO ENTRE IDENTIDADES DIGITAIS CENTRALIZADAS E DESCENTRALIZADAS

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Tecnologia da Informação, pelo Programa de Pós- Graduação em Tecnologia da Informação do Instituto Federal de Educação, Ciência e Tecnologia da Paraíba – IFPB.

Orientador: Prof. Dr. Rostand Edson Oliveira Costa

Coorientador: Prof. Dr. Dênio Mariz Timóteo de Sousa

João Pessoa

2022

Dados Internacionais de Catalogação na Publicação (CIP)
Biblioteca Nilo Peçanha do IFPB, *campus* João Pessoa.

M514l Meira, Anália Cristina Bezerra Tiburtino.

LinkedID: Uma abordagem baseada em um manifesto autocontido e verificável para associação entre identidades digitais centralizadas e descentralizadas / Anália Cristina Bezerra Tiburtino Meira. – 2022.

89 f. : il.

Dissertação (Mestrado – Tecnologia da Informação) – Instituto Federal de Educação da Paraíba / Programa de Pós-Graduação em Tecnologia da Informação, 2022.

Orientador: Profº. Dr. Rostand Edson Oliveira Costa;
Coorientador: Profº. Dr. Dênio Mariz Timóteo de Sousa.

1. Sistemas de gerenciamento de identidades. 2. Manifesto autocontido e verificável. 3. Identidade centralizada. 4. Identidade descentralizada. 5. Mapeamento de identidades. I. Título.

CDU 004.65

Lucrecia Camilo de Lima
Bibliotecária – CRB 15/132

ANÁLIA CRISTINA BEZERRA TIBURTINO MEIRA

LinkedID: UMA ABORDAGEM BASEADA EM UM MANIFESTO AUTOCONTIDO E VERIFICÁVEL PARA ASSOCIAÇÃO ENTRE IDENTIDADES DIGITAIS CENTRALIZADAS E DESCENTRALIZADAS

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Tecnologia da Informação, pelo Programa de Pós-Graduação em Tecnologia da Informação do Instituto Federal de Educação, Ciência e Tecnologia da Paraíba – IFPB.

Aprovado em 08 de Março de 2022.

BANCA EXAMINADORA:

Prof. Dr. Paulo Ditarso Maciel Júnior – IFPB
Avaliador

Prof. Dr. Guido Lemos de Souza Filho – UFPB
Avaliador Externo

Prof. Dr. Rostand Edson Oliveira Costa
Orientador

Prof. Dr. Dênio Mariz Timóteo de Souza
Coorientador

Visto e permitida a impressão João Pessoa

Prof. Dr. Petrônio Alencar de Medeiros
Coordenador PPPGTI

Dedico este trabalho aos meus familiares em especial ao meu marido Thiago, às minhas filhas Júlia e Thainá e aos meus pais, Marleide e Ubinho, por todo amor, estímulo, apoio e compreensão.

AGRADECIMENTOS

Agradeço a Deus, por possibilitar a realização de tantos sonhos, por me ajudar em cada momento, permitindo aprender e crescer, e por tudo que me proporciona, obrigada.

A minha família, por me apoiar e compreender, em especial ao meu marido Thiago e nossas filhas Thainá e Júlia. Obrigada por cada gesto de amor, carinho e compreensão, por cada sorriso tão importante para me estimular a continuar sempre por vocês.

Aos meus pais, Euilb e Marleide, faço um agradecimento especial, pelas lições que me dão todos os dias de amor, companheirismo, dedicação, abnegação e perdão. Amo muito vocês e sou privilegiada por ter pais tão especiais. E aos meus irmãos que tanto amo, Adriana e Alex, sempre prontos a me apoiar e ajudar em tudo, obrigada.

Aos professores Dr. Rostand Costa e Dr. Dênio Mariz, obrigada por cada orientação, pela enorme competência, profissionalismo e dedicação tão determinantes. Pelas reuniões que tanto me estimularam a manter a mesma determinação do primeiro dia de aula. Obrigada por acreditarem em mim e por todos os incentivos.

Aos membros da banca examinadora, professor Dr. Guido Lemos e o professor Dr. Paulo Ditarso, que tão gentilmente aceitaram participar e colaborar com esta dissertação.

Agradeço ao professor Francisco Petrônio pela atenção, paciência, dedicação, entusiasmo, pelo compartilhamento do conhecimento, enfim pela excelente coordenação frente ao mestrado Profissional de Tecnologia da Informação.

Ao meu amigo Francisco Batista, da Superintendência de Tecnologia da Informação/UFPB, por toda dedicação e comprometimento com os projetos que iniciamos juntos, pelas palavras de ânimo e incentivo que eu precisava e por todo conhecimento compartilhado, sua amizade é muito importante.

A todos os professores e amigos do PPGTI/IFPB, obrigado pelo conhecimento compartilhado, convívio, amizade e apoio demonstrado. Em especial, ao meu amigo Anderson Boa Morte, pelas colaborações, incentivos e parceria durante todo o mestrado e todas as nossas reuniões.

A Rede Nacional de Ensino e Pesquisa (RNP), em especial, a todos os integrantes do Programa de Gestão de Identidades (PGID), por apoiar e financiar o desenvolvimento do protótipo para a Prova de Conceito deste projeto.

Por fim, os meus sinceros agradecimentos a todos aqueles que contribuíram, direta ou indiretamente, para a realização desta dissertação.

RESUMO

Dentro do consenso do enorme potencial que o modelo de identidades descentralizadas pode trazer para a construção de serviços e aplicações com maior robustez e privacidade, há ainda desafios a serem vencidos para a sua adoção em larga escala. Entre eles, está a promoção da sua aceitação tácita e inequívoca em todos os cenários da sociedade, incluindo os contextos fiscais e jurídicos. Neste sentido, abordagens mais tradicionais baseadas no modelo de identidades digitais centralizadas já possuem um amplo reconhecimento jurídico, amparado por um vasto arcabouço de normas e regulamentações disponíveis, com algum grau de adaptação à realidade local, em praticamente todos os países através das suas infraestruturas de chaves públicas nacionais. A hipótese base deste trabalho é que a adoção e o uso de identidades descentralizadas pode ser alavancada, em alguns cenários, a partir do uso de identidades centralizadas associadas como uma espécie de lastro, beneficiando-se assim do reconhecimento fiscal e jurídico já estabelecido para as centralizadas. Neste contexto, foi idealizado um mecanismo que possibilita unir os dois modelos, criando um modo de identificar uma entidade que tanto possa atuar unicamente de forma descentralizada, mas que também possa receber como associação uma identidade centralizada, que seja verificável e autocontida. Esta é uma alternativa que pode subsidiar fases de transição ou, até mesmo, viabilizar a possibilidade de cenários híbridos de coexistência entre identidades de natureza distintas. Obtendo-se um lastro da identidade centralizada na identidade descentralizada, que passa a fornecer uma referência adicional sobre a entidade representada, tornando o processo de gestão de identidades ainda mais confiável e interoperável. Nesta direção, este trabalho propõe o uso de tecnologias e compromissos criptográficos como base para o desenvolvimento de um manifesto autocontido e verificável de associação entre identidades digitais descentralizadas e identidades centralizadas para permitir a sua convivência em diversos contextos de aplicação. Para aferir a viabilidade da proposta, foi implementada e avaliada uma prova de conceito de associação entre duas identidades reais: e-CPF (centralizada) e DID (descentralizada).

Palavras-chaves: Sistemas de Gerenciamento de Identidades; Manifesto Autocontido e Verificável; Identidade Centralizada; Identidade Descentralizada; Mapeamento de Identidades; DID; Credenciais Verificáveis.

ABSTRACT

Within the consensus of the enormous potential that the decentralized identity model can bring to the construction of services and applications with greater robustness and privacy, there are still challenges to be overcome for its large-scale adoption. Among them is the promotion of its tacit and unequivocal acceptance in all societal scenarios, including fiscal and legal contexts. In this sense, more traditional approaches based on the model of centralized digital identities already have a large legal recognition, supported by a vast set of norms and regulations available, with some degree of adaptation to the local reality, in practically all countries through their infrastructures of national public keys. The base hypothesis of this work is that the adoption and use of decentralized identities can be leveraged, in some scenarios, from the use of associated centralized identities as a kind of coverage, thus benefiting from the fiscal and legal recognition already established for the centralized. In this context, a mechanism was devised that makes it possible to unite the two models, creating a way to identify an entity that can both act solely in a decentralized way, but that can also receive as an association a centralized identity, which is verifiable and self-contained. This is an alternative that can support transition phases or even enable the possibility of hybrid scenarios of coexistence between identities of different natures. Obtaining a coverage of the centralized identity in the decentralized identity, which provides an additional reference about the represented entity, making the identity management process even more reliable and interoperable. In this direction, this work proposes the use of technologies and cryptographic commitments as a basis for the development of a self-contained and verifiable manifest of association between decentralized digital identities and centralized identities to allow their coexistence in different application contexts. To assess the feasibility of the proposal, a proof of concept of association between two real identities was implemented and evaluated: e-CPF (centralized) and DID (decentralized).

Key-words: Identity Management Systems; Self-Contained and Verifiable Manifest; Centralized Identity; Decentralized Identity; Identity Mapping; DID; Verifiable Credential.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACID	Atomicidade, Consistência, Isolamento e Durabilidade
API	*Application Programming Interface*
CA	*Certificate Authority*
Covid-19	*Coronavirus Disease* 2019
DID	*Decentralized Identifiers*
DIM	*Digital Identity Management*
DLT	*Distributed Ledger Technology*
DNI	Documento Nacional de Identidade
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IAM	*Identity and Access Management*
IBM	*International Business Machines Corporation*
IdP	Provedor de Identidade
IdM	*Identity Management*
IEEE	*Institute of Electrical and Electronics Engineers*
INPI	Instituto Nacional da Propriedade Industrial
IPFS	*InterPlanetary File System*
JSON	*JavaScript Object Notation*
JSON-LD	*JavaScript Object Notation for Linked Data*
LGPD	Lei Geral de Proteção de Dados Pessoais
OIDC	*OpenID Connect*
P2P	Peer-to-Peer Practical
PKI	*Public Key Infrastructure*
RNP	Rede Nacional de Ensino e Pesquisa
SAML	*Security Assertions Markup Language*

SBRC	Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos
SIOP DID	*Self-Issued OpenID Connect Provider DID*
SP	Provedor de Serviço
SSI	*Self-Sovereign Identity*
SSO	*Single Sign-On*
TIC	Tecnologias da Informação e Comunicação
UML	*Unified Modeling Language*
URI	*Uniform Resource Identifiers*
URL	*Uniform Resource Locator*
VC	*Verifiable Credential*
VON	*Verifiable Organization Network*
VP	*Verifiable Presentation*
XML	*Extensible Markup Language*
W3C	*World Wide Web Consortium*

SUMÁRIO

1. INTRODUÇÃO

Com os avanços tecnológicos e a conscientização da sociedade da importância e utilidade de aplicações computacionais no dia a dia, cresce a busca pela eficiência no modo como o usuário utiliza as Tecnologias da Informação e Comunicação (TIC) e como as pessoas podem se conectar e utilizar serviços *online*. Em muitos casos, esses serviços requerem mecanismos de identificação de entidades do mundo real, normalmente através da associação com uma identidade digital. Em tal contexto, uma identidade digital é um conjunto de informações sobre uma entidade do mundo real (indivíduo, aplicativo ou organização), que permite representá-la e identificá-la em sistemas de informação, viabilizando transações, facilitando o trato com assuntos governamentais ou privados e habilitando serviços em geral de forma personalizada.

Os sistemas de gerenciamento de identidades digitais (DIM, do inglês *Digital Identity Management*) fornecem identidades digitais para os usuários e gerenciam autenticação, autorização e compartilhamento de dados. O Gerenciamento de Identidade e Acesso (ou IAM, do inglês *Identity and Access Management*) é o processo pelo qual se organiza e administra as relações entre pessoas e ativos de informação de uma organização. Engloba funcionalidades de governança e administração de identidades; autenticação; provisionamento automático; portal de autosserviço; auditoria automatizada entre outros.

Quando esse gerenciamento é **centralizado**, significa que há um único provedor de identidades responsável por armazenar os dados e autenticar os usuários. Os modelos **federados**, por sua vez, se baseiam em um modelo de cooperação para armazenar e gerenciar essas informações e otimizar a troca de dados através de relações de confiança entre federações (WANGHAM; MELLO, 2010). Nos modelos **descentralizados**, por sua vez, o processamento de dados é dividido entre vários servidores conectados entre si, possibilitando o compartilhamento dos recursos.

Uma das estratégias relacionadas com identidades descentralizadas é a aplicação da tecnologia de livro razão distribuído (DLT, do inglês *Distributed Ledger Technology*). Uma DLT, normalmente baseada em *blockchain*, é um sistema descentralizado de registro de transações que opera de forma segura, estável e sem intermediários, na qual todas as transações são registradas criptograficamente em uma rede distribuída *peer-to-peer* e seus eventos averbados em um livro público de forma inalterável, rastreável e transparente. No

contexto de identidades descentralizadas, DLT é utilizado para registrar transações e para se manter completamente replicado em todos os nós da rede *peer-to-peer* (P2P). Por isso, é tido como distribuído, replicado e imutável.

Com a adoção do uso da *blockchain* em diversos contextos, em especial nos sistemas de identidades digitais, surgiu um novo conceito denominado ***identidade autossoberana*** (SSI, do inglês *Self-Sovereign Identity*), que defende uma forma de identificação dependente apenas do próprio usuário, enraizada em identificadores não controlados por uma terceira parte que o ateste, mas que são verdadeiramente controladas pelo indivíduo (ALLEN, 2016).

Quando foi iniciada a pandemia de Covid-19, ficou evidente que uma parcela imensa da população brasileira não estava incluída nas mais de 15 bases de dados com informações pessoais do governo federal, impossibilitando o acesso aos auxílios que foram fornecidos para compensar os danos econômicos causados pela pandemia (Lemos, 2020). Além da impossibilidade de acesso por ausência de cadastro de alguns, o pagamento do auxílio emergencial expôs também os problemas do país com relação ao cruzamento dos dados distribuídos nos mais diversos cadastros existentes. Tais problemas no cadastro do programa de auxílio emergencial permitiram, conforme amplamente divulgado na imprensa, inúmeros casos de fraudes para recebimento do referido auxílio, sobretudo por parte de pessoas que na realidade não deveriam recebê-lo.

Uma reflexão emerge dessa situação: a necessidade de distanciamento social causada pela pandemia colocou em xeque as estratégias comumente utilizadas para cadastramento de usuários de sistemas governamentais no Brasil, uma vez que aqui, assim como em boa parte do mundo, são utilizados, primordialmente, os tradicionais sistemas de identidade centralizados. No caso específico do auxílio emergencial, pôde-se verificar também que uma parcela significativa da população brasileira elegível não estava digitalmente identificada para poder receber o benefício, seja por não estarem incluídas digitalmente, seja por falta de informação ou, até mesmo, por nem sequer ter conhecimento de que sua situação estava inadequada. Com este problema em foco, percebe-se a importância de se buscar uma forma de identificação mais inclusiva e que possa, com maior facilidade, permitir a integração dos diversos cadastros e serviços públicos.

Apesar da abordagem centralizada ser a mais tradicional, os sistemas descentralizados vêm ganhando espaço. Começaram a ser utilizados e a apresentar uma série de vantagens que podem torná-los mais adequados para determinados contextos. Este trabalho investiga uma

abordagem de mapeamento que permite que identidades centralizadas existentes (legadas) sejam compatíveis e possam ser utilizadas em contextos que demandem identidades descentralizadas. Como benefício direto desta associação, serviços que se apoiam em identidades descentralizadas poderão atender um público maior, pois as identidades centralizadas vinculadas auxiliarão no aumento da popularização e confiança em identidades descentralizadas, sem prejuízo para serviços que se apoiam unicamente em identidades centralizadas.

Em tal cenário, este trabalho foca na investigação da utilização de tecnologias e padrões emergentes, além de algumas estratégias já consolidadas, para auxiliar no desenvolvimento de um modelo que garanta a identificação dos indivíduos seguindo uma abordagem descentralizada, mas que possa ser integrada e conviver com a abordagem centralizada legada, mais adotada atualmente pelos serviços públicos. O ponto chave da proposta é a utilização de um manifesto de associação autocontido e verificável entre identidades centralizadas e identidades descentralizadas.

1.1. Motivação

Atualmente, os cadastros relacionados aos dados pessoais dos cidadãos brasileiros são separados em vários serviços. A depender da finalidade, a guarda dos dados fica sob a responsabilidade de um órgão diferente da administração pública, dificultando a interoperabilidade e colaboração centrada no usuário. Tal problema não ocorre apenas no Brasil, pois diversos países possuem cadastros dos cidadãos centralizados em determinadas organizações.

Mesmo iniciativas recentes como as apontadas por Renato Mota (Mota, 2020) voltadas para a modernização das diversas identidades existentes, a exemplo da criação do e-Título de eleitor[1], da e-Carteira de Trabalho[2], da Carteira Nacional de Habilitação Digital[3] e do e-CPF[4], mantêm o mesmo modelo centralizado e com baixa integração. Tal necessidade de consolidação e interoperabilidade das identidades digitais nacionais é reconhecida nas esferas governamentais brasileiras e buscada através de iniciativas como a propositura de um

[1] e-titulo - http://www.tse.jus.br/eleitor/servicos/aplicativo-e-titulo
[2] CTPS digital - https://www.gov.br/pt-br/temas/carteira-de-trabalho-digital
[3] CNH Digital - https://servicos.serpro.gov.br/cnh-digital/
[4] e-cpf - https://loja.certisign.com.br/Certificados/E-CPF

Documento Nacional de Identidade (DNI)[5], cujo objetivo é que os cidadãos tenham um documento único, com informações de título de eleitor, CPF, carteira de identidade e biometria, diminuindo a quantidade de documentos a serem apresentados e facilitando a prestação de serviços, conforme (Guedes, 2018).

Visando alcançar toda população e unificar os identificadores, países como a Estônia, Índia, Canadá e Estados Unidos desenvolveram sistemas de identidade digital para seus cidadãos, possibilitando-os realizar seus atos junto ao Estado de forma digital e certificada, protegendo a privacidade e tomando por base uma arquitetura descentralizada.

Os cidadãos da Estônia, por exemplo, utilizam um documento único, que unifica as vidas *online* da população através de uma plataforma chamada *X-Road*. Cada habitante possui um cartão com um chip, que funciona como uma identidade única e que integra: RG, carteira de motorista, passaporte, vale-transporte, entre outros, possibilitando acesso a quase todos os serviços públicos, como declaração e pagamento de impostos, abertura de empresas, votação nas eleições, assinatura de contratos, transações bancárias, visualização de histórico médico e obtenção de receitas médicas (CryptoID, 2019).

Na Índia, foi criado o sistema de identidades digitais únicas chamado *Aadhaar*, como um processo que busca inclusão social e financeira. Esse sistema tornou-se o passaporte único das relações entre cidadãos e governo. O sistema permite abrir uma conta bancária, bem como receber benefícios sociais e realizar todas as operações pelo celular, dispensando a presença física do usuário. Antes do sistema, em 2008, apenas 17% dos adultos do país tinham conta em banco; em 2011, a Índia alcançou a média global de “bancarização”, e, em 2018, 80% da população adulta já possuía uma conta bancária, ultrapassando a média global (Matsuura, 2020).

Similarmente, vale destacar que o setor bancário canadense lançou oficialmente, em 2019, uma rede de identidade digital baseada em *blockchain*, denominada *Verified.me*. Nos EUA, a maioria das empresas de tecnologia que residem no Vale do Silício investem em DLT em diversos setores. Os projetos governamentais baseados em *blockchain* baseados em *blockchain* mais ativos estão em colaboração com a Secretaria da Saúde e com a IBM, pois esta é uma grande provedora BaaS (*Blockchain as a Service*) que oferece soluções baseadas em DLT para muitos setores.

[5] DNI - http://www.dni.gov.br/

No Brasil, foi estabelecida a Estratégia de Governo Digital[6] que busca a digitalização de todos os serviços públicos no âmbito federal, podendo alcançar também os estados e municípios (Amado, 2020). O decreto que estabelece esta Estratégia prevê em seus objetivos a identidade digital para o cidadão, criando condições para expandir a quantidade de brasileiros identificados digitalmente e para reduzir os custos dos certificados digitais. Disponibilizará, ainda, novos mecanismos de assinatura digital, incentivando seu uso com alto nível de segurança. Para isso, as medidas adotadas devem promover a divulgação ampla de sistemas e a verificação das políticas de assinatura com códigos abertos e interoperáveis. A Estratégia objetiva também implementar recursos para criação de uma rede *blockchain* do Governo federal interoperável, com uso de identificação confiável e de algoritmos seguros.

A W3C, principal entidade de padronização da *World Wide Web*, está trabalhando na especificação de um modelo de dados, um formato de URL (*Uniform Resource Locator*) e um conjunto de operações para identificadores descentralizados. Esses identificadores são capazes de fornecer autenticação segura e confiável. Eles foram projetados para permitir que o controlador de um DID (do inglês, *Decentralized Identifiers*)[7] prove ter o controle dele e que seja implementado independentemente de qualquer registro centralizado.

Os principais objetivos a serem alcançados pelo DID e elencados na especificação do W3C são: descentralização, controle, privacidade, segurança, interoperabilidade, portabilidade, extensibilidade, que sejam baseados em provas criptográficas, que engloba um conjunto de recursos simples para facilitar a compreensão, implementação e implantação da tecnologia, além da existência de um processo de descoberta de DID.

No Brasil, os diversos serviços e sistemas de identidade dos cidadãos são centralizados. No entanto, observa-se que nem sempre a grande parcela da sociedade é alcançada por tais cadastrados e nota-se, ainda, que aqueles cidadãos englobados neste meio acabam se deparando com o número crescente de sistemas aos quais devem se cadastrar pela ausência de uma maior integração entre as bases de dados. Por razões como estas, sistemas descentralizados vêm se tornando uma tendência, ganhando notoriedade e espaço nos sistemas de identidade e em diversas áreas, uma vez que para sua emissão não exigem a presença física da pessoa em um local de registro. Além disso, os dados ficam de posse do

[6] Estratégia estabelecida por meio do Decreto nº 10.332, de 28 de abril de 2020.

[7] DID - Identificador Descentralizado é o novo tipo de identificador que permite identidade digital verificável e descentralizada.

proprietário, normalmente, em uma carteira digital, e não sobre a posse de terceiros e seus custos são consideravelmente menores.

Ao pensar em adotar sistemas descentralizados é importante encontrar uma alternativa que possibilite a comunicação ou coexistência entre as duas modalidades, pelo menos em uma fase de transição ou aceitação. Este trabalho busca investigar como os sistemas de gerenciamento de identidades descentralizados poderiam ser integrados aos sistemas centralizados existentes, utilizando tecnologias bem estabelecidas como certificação e assinatura digital para obter uma forma segura de associação autoverificável para as entidades, a qual pode contribuir para lastrear as identidades descentralizadas emergentes com identidades centralizadas já consolidadas e reconhecidas.

1.2. Objetivos

Este trabalho tem como objetivo geral a investigação do uso de compromissos criptográficos e outras tecnologias correlatas como base para o desenvolvimento de um modelo autoverificável de associação entre identidades descentralizadas e centralizadas para permitir a sua convivência em diversos contextos de aplicação.

O principal objetivo do mecanismo de transição proposto é lastrear a criação e uso de identidades descentralizadas, ainda emergentes, a partir de identidades centralizadas existentes, possuidoras de ampla aceitação e relevância jurídica. A base da abordagem é permitir uma forma verificável e flexível de relacionar entidades reconhecidas por identificadores centralizados a identificadores descentralizados.

Para alcançar o objetivo geral desta proposta, foram definidos os seguintes objetivos específicos:

1. Identificar as diversas variantes da gestão de identidades, comparando aspectos relevantes das modalidades centralizada e descentralizada;

2. Investigar o estado da arte sobre tecnologias emergentes aplicadas à gestão de identidades;

3. Prospectar estratégias aplicáveis para a associação entre identidades descentralizadas e centralizadas;

4. Propor um modelo de mapeamento de identidades centralizadas para identidades descentralizadas com uso de associações verificáveis;

5. Implementar um protótipo capaz de associar identidades descentralizadas a uma ou mais identidades centralizadas utilizando o modelo proposto;

6. Avaliar os resultados dos testes para validar a proposta considerando um ou mais casos de uso potenciais.

1.3. Metodologia

Nesta seção, é apresentada a metodologia de realização deste trabalho que seguiu as seguintes atividades: análise bibliográfica, estudo de estratégias aplicáveis ao mapeamento de identidade centralizada para descentralizada, especificação e implementação de um protótipo capaz de mapear uma identidade descentralizada para uma centralizada e validação da proposta.

Inicialmente, foi elaborado um protocolo de revisão sistemática da literatura, com o propósito de investigar o estado da arte no contexto de identidades digitais, buscando os principais desafios, melhores práticas, modelos e ferramentas apresentados na literatura, bem como identificar os trabalhos relacionados potencialmente relevantes ao mapeamento entre identidades centralizadas e descentralizadas. Nesta fase da pesquisa, foi realizado também um estudo específico com o objetivo de identificar as principais contribuições relacionadas ao tema deste trabalho e assim atender ao segundo objetivo específico. A revisão sistemática da literatura foi conduzida para elucidar os conceitos acerca dos sistemas de gerenciamento de identidade digital centralizada e descentralizada, tendo em vista mapear os principais estudos relacionados à associação de identidades descentralizadas a identidades centralizadas.

O principal critério de busca adotado foi a possibilidade de mapear identidades descentralizadas para centralizadas e conciliar a convivência de sistemas de gerenciamento de identidades descentralizadas emergentes com modelos centralizados consolidados, utilizando a credibilidade dos últimos para lastrear a consolidação dos primeiros, visando identificar

trabalhos relacionados ao tema desta pesquisa por abordarem o mesmo problema e auxiliar na definição da delimitação do problema da pesquisa.

Em seguida, sentiu-se a necessidade de um aprofundamento no estudo sobre as estratégias e tecnologias disponíveis capazes de auxiliar na realização deste tipo de mapeamento entre identidades. Através deste levantamento, pôde-se compreender os componentes de um identificador descentralizado, entender quais abordagens ou soluções poderiam ser utilizadas com o intuito de apoiar a associação, incluindo abordagens com e sem o uso de tecnologias como *blockchain* e credenciais verificáveis. Também foram elencados e estabelecidos os critérios de sucesso para nortear a validação do manifesto de associação. Após este estudo, formalizou-se a proposta da pesquisa, ou seja, a proposta do manifesto de associação.

Para demonstrar a aplicabilidade da proposta, foi definida uma prova de conceito que apresenta como desenvolver um manifesto de associação, utilizando um par real de identidades centralizadas e descentralizadas, eCPF e DID, respectivamente. Após esta definição, foi iniciada a especificação do protótipo a ser implementado para verificar a exequibilidade da prova de conceito, bem como a prospecção das tecnologias aplicáveis a ele.

Passou-se, então, ao desenvolvimento do protótipo capaz de auxiliar na associação efetiva de uma identidade descentralizada existente (DID) em uma identidade centralizada existente (eCPF), aplicando o padrão de manifesto autocontido e verificável proposto.

Após a construção do protótipo, foram apresentados os resultados dos experimentos realizados e foi descrito como foram feitas as integrações com outras aplicações para validação do artefato construído de forma a atender as premissas estabelecidas.

1.4. Organização da Dissertação

Os capítulos subsequentes estão organizados da seguinte maneira.

O **Capítulo 2** contém a fundamentação teórica básica para o entendimento deste trabalho, na qual os conceitos relacionados a tecnologias de registros distribuídos, *blockchain* e identidades digitais são apresentados em detalhes, incluindo uma descrição dos conceitos de identificadores descentralizados (DID) e de credenciais verificáveis (VC).

O **Capítulo 3** apresenta os trabalhos relacionados ao tema em questão. Foram identificadas outras pesquisas ou iniciativas que se relacionam por tratarem da questão de criação de identidade descentralizada e também outros trabalhos que realizam associação de identidades de atores, porém apenas no âmbito centralizado.

O **Capítulo 4** apresenta a dinâmica proposta de associação entre identidades centralizadas e descentralizadas, a qual se baseia na criação de um artefato específico, autocontido e verificável, chamado *manifesto de associação.*

O **Capítulo 5** demonstra a aplicabilidade da proposta a partir da modelagem de uma prova de conceito para um cenário real, que ilustra como construir uma associação de forma concreta, utilizando um par real de identidades centralizada (eCPF) e descentralizada (DID).

O **Capítulo 6** apresenta a construção de um protótipo funcional da prova de conceito, chamado *LinkedID*, incluindo a discussão dos detalhes da implementação e a avaliação dos resultados obtidos.

O **Capítulo 7** traz as considerações finais e algumas propostas de continuação do trabalho.

2. FUNDAMENTAÇÃO TEÓRICA

Para uma melhor compreensão da estratégia adotada, faz-se necessário apresentar e discutir os elementos conceituais importantes utilizados na proposta de solução e que formam o referencial teórico para esta pesquisa. Neste Capítulo, será realizada uma revisão sobre os conceitos relacionados às identidades digitais, em seguida serão detalhadas as especificações dos identificadores descentralizados e credenciais verificáveis. Por fim, também serão explanados os conceitos sobre a tecnologia de livros-razão distribuídos (DLT).

2.1. Identidades Digitais

O conceito de identidade está relacionado ao ambiente onde ela será empregada, aos contextos semânticos e aos casos de uso (Cao, Yang, 2010). De forma geral, pode-se dizer que uma identidade é uma representação de uma entidade, que seja suficiente para identificá-la em um contexto particular. Uma entidade, por sua vez, é qualquer coisa existente no mundo real, como uma pessoa, uma máquina ou uma aplicação. Em geral, a relação de cardinalidade de uma entidade é que ela pode ter múltiplas identidades. De acordo com a norma ITU-T Y.2720 (ITU-T, 2009), uma identidade pode consistir de:

- *Identificador*: conjunto de dígitos, caracteres e símbolos ou qualquer outra forma de dados usada para identificar unicamente uma identidade. Podem ser delimitados pelo tempo e/ou espaço, tal como uma URL (*Uniform Resource Locator*) que é única ao longo do tempo. Como exemplo de identificadores temos CPF, RG, número de matrícula e número de passaporte.
- *Credenciais*: atestado de qualificação, competência ou autoridade, expedida por terceiros com autoridade relevante ou competência para tal ato e que atesta a veracidade da identidade. Na computação, exemplos de credenciais incluem certificados digitais X.509 assinados por uma autoridade certificadora (CA - *Certificate Authority*), senha, asserções SAML (*Security Assertions Markup Language*), dentre outros.

- *Atributos*: um conjunto de dados que descreve as características fundamentais de uma identidade. Como exemplo temos: nome, domicílio, data de nascimento e papéis (*roles*).

Por sua vez, o conceito de identidade digital pode ser visto como um conjunto de reivindicações feitas por uma entidade digital sobre ele próprio ou sobre outra entidade. Tais reivindicações correspondem a atributos cuja entidade reivindica em um ambiente digital (Cameron, 2005). Seu uso oferece várias vantagens quando comparado ao uso das identidades tradicionais:

- *economia*: elimina-se o custo de impressão da versão em papel;
- *replicação e distribuição ilimitada e gratuita*: a identidade digital poderá ser gerada e apresentada pelo portador quando for conveniente; e
- *auto-verificação*: viabiliza-se a utilização de técnicas automatizadas de verificação da autenticidade do documento pelo verificador.

Idealmente, uma identidade digital deve ser criada através de um conjunto de atributos que permitam diferenciar uma entidade da outra garantindo sua identificação única. O primeiro mecanismo utilizado para autenticar usuários foi através de um par login e senha.

Entretanto, para autenticar, autorizar e gerenciar dados pessoais e permitir o uso em transações críticas, faz-se necessário mecanismos de controle e de segurança adicionais, incluindo a gerência do ciclo de vida da utilização de identidades digitais em aplicações computacionais. Para lidar de forma padronizada com as demandas de controle de autenticação e autorização de operações para usuários, foi introduzido o conceito de Gerenciamento de Identidade e Acesso.

2.1.1. Evolução dos Modelos de Identidade Digital

Para atender ao objetivo específico descrito no item 1 da Seção 1.2, foi realizado um levantamento sobre as diversas variantes da gestão de identidade digital. Uma definição clássica de modelos de identidade digital prevê quatro tipos (El Haddouti, 2015):

a) **convencional**;

b) **centralizado**;

c) **federado**; e

d) **centrado no usuário**.

Cada modelo apresenta vantagens e desvantagens, porém todos enfrentam um problema em comum que é o grande controle exercido por autoridades centrais, que acabam privando os usuários da total propriedade dos seus dados pessoais e o fato de que, em determinados momentos de realização das identificações, podem ser compartilhadas mais informações que o necessário.

Na busca para diminuir a influência e/ou necessidade de uma autoridade central, outros modelos de identidade digital começaram a surgir e estão em construção. Dentre eles, as abordagens mais promissoras são as identidades autossoberanas descentralizadas e as identidades descentralizadas baseadas em *blockchain*. Os aspectos relevantes de cada um e suas vantagens e desvantagens serão descritos a seguir:

- **Modelo de Identidade Convencional**

  O Modelo de Identidade Convencional requer que cada usuário possua um identificador para acessar cada serviço isoladamente. Nele, um provedor de serviço (SP, do inglês *Service Provider*) também desempenha o papel de um provedor de identidade. Cada SP requer seus próprios atributos para formar a identidade do usuário, de modo que este fornecerá as informações tantas vezes quanto for o número de contas criadas no SP.

  Do ponto de vista da segurança, uma grande quantidade de contas e senhas para memorizar torna-se algo cada vez mais difícil de lembrar, bem como reutilizar senhas torna as contas vulneráveis, caso alguém as descubra, dando origem ao risco de segurança de fraude de identidade e outras formas de atividade criminal associadas.

- **Modelo de Identidade Centralizada**

  Para evitar redundâncias e inconsistências que surgiram nos modelos de login e senha convencionais, o modelo centralizado foi criado baseado na existência de um único Provedor de Identidade e vários Provedores de Serviços, os quais compartilham entre si as identidades dos usuários. Este modelo é considerado o modo mais simples de implementar a autenticação única (SSO, do inglês *Single Sign-On*), na qual o usuário se autentica uma vez obtendo credenciais para os Provedores de Serviços utilizados.

O provedor de identidades é implementado como um *software* e é executado em um ambiente de servidor sob controle da parte hospedeira, que adquire grande domínio sobre as informações registradas. Algumas vantagens deste modelo são as formas eficazes de gerenciar de maneira automatizada a acessibilidade dos usuários, unificar perfis, diminuir a redundância dos dados, facilitar a geração de relatórios sobre usuários favorecendo as atividades de auditorias e implantação rápida em resposta a ameaças.

- **Modelo de Identidade Descentralizada**

  A abordagem de identidade descentralizada busca colocar o usuário no centro da estrutura e remover a necessidade de terceiros emitirem e administrarem as identidades. Neste modelo, identidades digitais são criadas pelo próprio usuário, entidade ou organização e permanecem sob seus cuidados, fornecendo total propriedade e controle dos dados, cabendo somente a ele escolher quais informações compartilhar, sem depender de um repositório central de dados de identidade.

  Os dados sob a posse da entidade podem tornar as informações mais interoperáveis e aumentar o controle individual e a privacidade, pois permitem selecionar o que será divulgado, possibilitam atualizar informações quando necessário e promovem independência de um servidor central. O proprietário é quem detém as informações e seleciona o que será divulgado.

  O modelo é iniciado com a criação do identificador ou identificadores exclusivos pelo usuário e, em seguida, adicionam-se informações e técnicas criptográficas, como assinatura digital, que corroboram para provar a autenticidade. O modelo de identidade descentralizado apresenta outras vantagens como alta escalabilidade e resiliência diante de sobrecarga, confere à entidade mais controle sobre sua identidade, facilita a utilização da identidade *online*, podendo ser facilmente empregada para vários usos. Identidades descentralizadas se apresentam como uma abordagem mais vantajosa que as centralizadas, pelo simples motivo de o proprietário manter a identidade e a responsabilidade pelos dados consigo. Também se apresenta como uma opção atrativa para as empresas, que não seriam mais as únicas responsáveis pela infraestrutura de identidade, reduzindo custos e riscos.

  Em sistemas centralizados, o provedor que fornece a identidade é responsável pela segurança dos dados. Em uma estrutura descentralizada, a responsabilidade pela segurança passa a ser da entidade detentora da identidade, a qual poderá implementar suas próprias medidas ou agenciar algum serviço. Entretanto, como a descentralização não exige uma autoridade central de confiança, pode haver problemas para chegar a um consenso global sobre o estado da informação de identidade entre os pares. Este problema tem sido abordado recentemente pelo uso da tecnologia DLT (*blockchain*).

- **Modelo de Identidade Descentralizada baseado em DLT**

  A tecnologia de DLT fornece às identidades digitais uma plataforma transparente de auditoria de dados, principalmente devido à imutabilidade dos dados por ela registrados. Os sistemas de identidade baseados em *blockchain* podem fornecer uma solução poderosa para diferentes aspectos da estrutura de identificação descentralizada, apresentando soluções com criptografia rígida e *ledgers* distribuídos, permitindo que todos armazenem chaves criptográficas de uma maneira inviolável e cronologicamente ordenada. Posteriormente, as chaves serão utilizadas para permitir que outras pessoas verifiquem assinaturas digitais ou criptografem dados para o detentor da identidade.

  Alguns exemplos de potenciais usos da *blockchain* em contextos de identidade descentralizada são:

  - criar identificadores descentralizados (DID);
  - atuar como carimbo de tempo e selo eletrônico - podendo ser utilizado com credenciais para fornecer prova de quando a credencial foi criada
  - registrar direitos de acesso e consentimento - as cadeias de bloco podem ser usadas para registrar tais direitos às informações -, entre outros.

  O uso desses modelos baseados em DLT acrescenta como característica diferencial a natureza imutável das *blockchains*, as quais, para ser violada com sucesso, demandam um ataque sobre cada bloco individual da cadeia de blocos, o que pode ser computacionalmente inviável. No entanto, tal característica tem levantado algumas dificuldades, como o direito ao esquecimento ou o direito à retificação, ambos previstos na Lei Geral de Proteção de Dados (LGPD). Esta discussão deve ser aprofundada caso o projetista de *software* precise lidar com tais requisitos.

2.2. IDENTIFICADORES DESCENTRALIZADOS (DID)

Como parte do estudo sobre tecnologias emergentes aplicadas à gestão de identidade, analisamos dois novos padrões em desenvolvimento que constroem a base para identidade digital descentralizada: o DID e as credenciais verificáveis. Um DID é um identificador descentralizado que identifica de forma única uma entidade (pessoa, organização, modelo de dados) permitindo-lhe o controle de sua identificação independentemente de um registro

centralizado. Segundo Clauß e Köhntopp (2001, 205-219), uma identidade digital pode ser construída com a participação da entidade interessada e possui natureza de multiplicidade, isto é, entidades podem ter diferentes *personas*[8] de acordo com o contexto em que estão interagindo. Os identificadores descentralizados abordam este conceito de multiplicidade possibilitando a cada entidade ter quantos DID desejar para respeitar os diferentes contextos no qual se identifique, mas também porque os DID de diferentes métodos podem não ser interoperáveis e a existência de vários deles podem dar suporte aos relacionamentos. Outro motivo para se adotar tal multiplicidade é para dar suporte aos diferentes esquemas criptográficos de diferentes métodos, pois nem todas as partes suportam os mesmos esquemas.

O padrão DID foi projetado para permitir que indivíduos e organizações gerem seus próprios identificadores usando sistemas nos quais confiam e para permitir que se autentiquem com esses identificadores usando provas criptográficas, como assinaturas digitais, protocolos biométricos de preservação da privacidade, entre outros. Como eles são criados, controlados e compartilhados pelos próprios indivíduos, então é possível gerar quantos identificadores forem necessários para respeitar a separação desejada de identidades, *personas* e contextos.

2.2.1. Componentes da arquitetura DI

Há vários elementos envolvidos na composição e obtenção de um DID. Os principais componentes de sua arquitetura são apresentados na Figura 1.

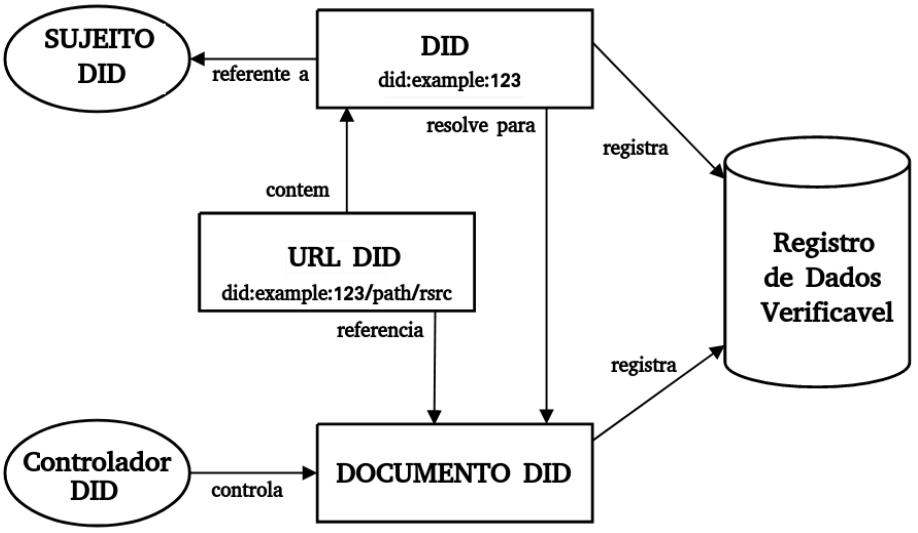

Figura 1. Principais componentes da arquitetura DID. Fonte: Reed et al, 2020.

[8] *Persona* - um dos arquétipos da personalidade humana, incluindo os papéis sociais e o estilo de expressão pessoal do indivíduo.

A função de cada elemento é resumidamente apresentada na Tabela 1.

Tabela 1. Descrição dos elementos que compõem um DID.

Elementos DID	Objetivo/função de cada elemento
Métodos DID	São utilizados para criar, resolver, atualizar e desativar um DID. Todos os métodos suportam a mesma funcionalidade básica, mas diferem na maneira como as implementam, na definição de como um DID é criado ou na forma onde e como o documento DID é armazenado e recuperado.
Sujeito DID	É a entidade identificada pelo DID, podendo ser uma pessoa, grupo, organização, algo físico ou lógico.
DID/DID URL	DID é a representação do identificador no formato - did:example:0x123456abcdefgfnsekjfnks e DID URL – estende a sintaxe do DID. É semelhante às URLs HTTP e HTTPS, podem receber componentes anexados ao nome do domínio, como um caminho opcional, uma sequência de consultas e um fragmento opcional.
Documento DID	Contém os metadados associados ao identificador, métodos de verificação e serviços relevantes para a interação. Para identificadores digitais, a utilidade não vem apenas do próprio identificador, mas de como ele pode ser usado por aplicativos projetados para consumir esse tipo específico de identificador, como carteiras, agentes ou armazenamento de dados pessoais que usam DID. Esses metadados podem ser usados para: ● Procurar uma chave pública para verificar uma assinatura digital do emissor; ● Para autenticar o controlador DID quando ele precisar "efetuar login"; ● Para descobrir e acessar um serviço conhecido associado ao controlador DID, como um site, rede social ou autoridade; ● Para solicitar uma conexão para o controlador DID.
Resolvedor DID	Trata-se de um *software* ou *hardware* que recebe um DID ou DID URL como entrada e produz um documento DID ou um recurso como saída. Para a maioria das DID URLs, existe uma etapa executada pelo algoritmo de desreferenciamento DID. Enquanto a resolução retorna o documento DID, no desreferenciamento, o documento DID é processado para acessar ou recuperar o recurso identificado pela DID URL.
Controlador DID	Entidade capaz de controlar um DID que necessita de um controlador. Por exemplo, quando o DID se refere a pessoas que não podem se responsabilizar por tal, como bebês, pessoas sem acesso à internet, coisas artificiais, digitais, coisas naturais, animais etc.
Registro de Dados Verificáveis	É a rede subjacente que armazena o DID e oferece suporte ao retorno de dados necessários para produzir um documento DID. Através dela o verificador pode validar uma credencial. Os registros nele armazenados são essenciais para que o ecossistema de DID opere de maneira eficaz e eficiente.

- **Formato DID**

Um DID é representado por uma URI (*Uniform Resource Identifier*) composta por 3 partes, como pode ser visto na Figura 2. Contém o Identificador de Esquema, o Método DID e o Identificador Específico do Método DID. O Identificador de Esquema é a sintaxe formal de um identificador descentralizado globalmente

exclusivo. O Identificador para o Método DID é uma definição de como um DID pode ser implementado em uma DLT específica. Toda especificação de método DID deverá definir o formato e como gerar o Identificador Específico do Método DID, que deverá ser único no *namespace* do seu Método DID.

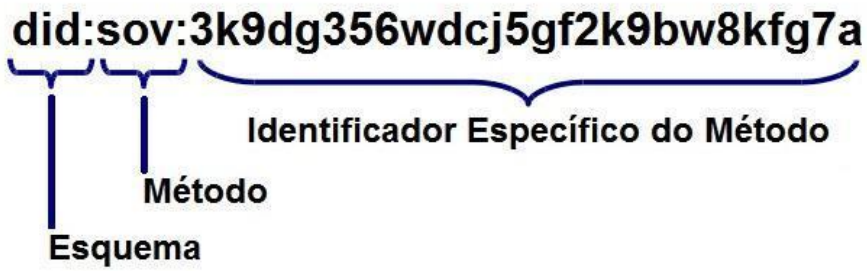

Figura 2: Exemplo da sintaxe de um DID. Fonte: Própria.

Uma DID URL estende a sintaxe de um DID básico para incorporar outros componentes padrão de URI, como uma consulta, um caminho ou um fragmento para localizar um recurso específico. Por exemplo, uma chave pública dentro de um documento DID ou um recurso disponível externo ao DID documento, conforme Figura 3.

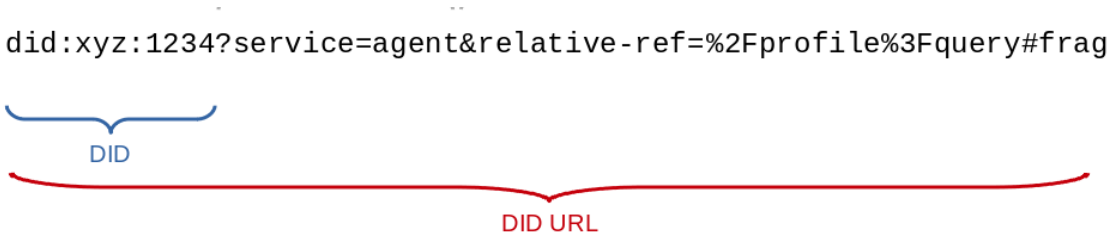

Figura 3: Exemplo da sintaxe de um DID URL. Fonte: Sabadello, 2021.

- **Documento DID**

O identificador digital por si só não é interessante. Sua utilidade reside em como ele pode ser utilizado por aplicativos desenvolvidos para consumir esse tipo específico de identificador. Ou seja, ao digitar o identificador em um navegador, será retornada uma página que apresenta o recurso por trás dele, por exemplo. Assim ocorre com o DID que pode ser resolvido para seu respectivo Documento DID, que é uma estrutura de dados feita para ser consumida por aplicativos ou serviços de identidade digital, como carteiras, agentes ou armazenamentos de dados pessoais, os quais usam DID como blocos de construção fundamentais. Um documento DID é um arquivo JSON-LD (*JavaScript Object Notation for Linked Data*) contendo metadados associados ao

identificador, expressando métodos de verificação e serviços relevantes para as interações.

O documento DID pode armazenar qualquer informação sobre o Sujeito DID, mas por questões de privacidade recomenda-se que contenha apenas a quantidade mínima de metadados necessária para permitir a interação confiável com o Sujeito DID, que é a entidade identificada. Nesse contexto, o objeto JSON-LD inclui as seguintes funcionalidades principais para interagir com o titular do DID:

1. O ID do próprio DID, a partir do qual se obtém o documento DID e se torna possível a vinculação a outros documentos.
2. Chaves públicas ou outras provas que podem ser usadas para autenticação durante uma interação com a entidade identificada.
3. Um conjunto de *services endpoint* que descreve onde e como interagir com a entidade identificada, o que pode incluir protocolos de mensagens instantâneas ou protocolos de identidade dedicados, como *OpenID Connect* (OIDC), DIDComm, entre outros.
4. Pode-se, ainda, decidir autorizar outras entidades a fazer alterações no documento DID, processo chamado de delegação, que pode se tornar importante e útil no caso de perda de chave privada.
5. Carimbos de data e hora podem ser adicionados durante a criação ou atualização de um DID específico, útil para processos de auditoria.
6. Uma assinatura JSON-LD também pode ser adicionada se houver necessidade de verificar a integridade do documento.

Para gerar o documento DID, é preciso acionar um *Resolver*, ou seja um sistema que recebe um DID como entrada e recupera um documento DID ou retorna um recurso como resultado da resolução. Ele é capaz de executar o algoritmo *DID Resolution* ou o algoritmo *DID URL Dereferencing* para este fim.

- **O Sujeito e o Controlador DID**

O sujeito é a entidade identificada pelo DID, podendo ser uma pessoa, grupo, organização, algo físico ou lógico. O sujeito DID também pode ser o controlador DID, que é a entidade (pessoa, organização ou software autônomo) capaz de fazer alterações

em um documento DID. Um DID pode ter mais de um controlador e o(s) controlador(es) pode(m) incluir o sujeito do DID.

Esse recurso geralmente é afirmado pelo controle de um conjunto de chaves criptográficas usadas pelo software que atua em nome do controlador, embora também possa ser afirmado por outros mecanismos.

Em muitos casos, o controlador DID é o mesmo que o sujeito DID, mas também podem ser diferentes. Por exemplo, quando um pai controla um DID que identifica seu filho. Nesse caso, o sujeito DID é o filho, mas o controlador DID é o pai.

- **Registro de Dados Verificáveis**

Os DID geralmente são gravados em um sistema ou rede subjacente de algum tipo. Independentemente da tecnologia específica usada, qualquer sistema que ofereça suporte à gravação de DID e ao retorno de dados necessários para produzir documentos DID é chamado de registro de dados verificável. Ele realiza a função de mediar a criação e a verificação de identificadores, chaves e outros dados relevantes, como esquemas de credenciais verificáveis, registros de revogação, chaves públicas do emissor e assim por diante. Os exemplos incluem DLT, sistemas de arquivos descentralizados, bancos de dados, redes ponto a ponto e outras formas de armazenamento de dados confiáveis.

Os dados que devem ser armazenados no registro são: o DID e o *endpoint* do seu controlador ou agente; os esquemas de estruturas de dados e definição de credenciais; e as revogações das credenciais. Por outro lado, não se deve armazenar: pseudônimo ou DID de relacionamento (que é um par único de ID gerados entre duas partes quando eles desejam compartilhar dados com cada pedido); as credenciais que cada usuário pode armazenar com segurança em sua carteira; chaves privadas; dados de credenciais emparelhados ou compartilhados entre duas partes; *service endpoint* para permitir a interação entre o emissor, o proprietário e os verificadores de identidade por meio de agentes associados.

- **Métodos DID**

Os DID não são criados e mantidos em um único tipo de banco de dados ou rede como a maioria dos outros tipos de URI. Não há um registro centralizado ou uma hierarquia de registros federados onde todos os DID são gravados e lidos. Existem, hoje, muitos tipos de DID na comunidade SSI, todos padronizados para atenderem a mesma funcionalidade básica. O que os distingue é a forma como essa funcionalidade é implementada, como cada um é criado, ou onde e como um documento DID associado a um DID é armazenado e recuperado.

Tais funcionalidades de cada tipo de DID são definidas e especificadas nos Métodos DID, que é o mecanismo utilizado para criar, resolver, atualizar e desativar um DID e seu Documento DID, utilizando um Registro de Dados Verificável específico. Como citado anteriormente no formato do DID, a segunda parte identifica o método usado para criação do identificador e busca fornecer transparência e interoperabilidade. Devem ser especificados para que outras entidades entendam como os documentos DID e o DID são criados, resolvidos e gerenciados em um DLT específico. Cada método DID deve ter sua própria especificação técnica, os seguintes aspectos:

- A sintaxe da 3ª parte do formato do identificador DID - a parte após o segundo dois pontos - é o identificador específico do método (uma cadeia longa gerada usando números aleatórios e funções criptográficas);
- As quatro operações básicas que podem ser executadas são: **criação** (como um DID e seu documento DID são criados), **atualização** (como o conteúdo do documento DID pode ser alterado), **desativação** (como um DID pode ser desativado para que não possa mais ser usado) e **leitura** (como recuperar o documento DID de um DID);
- Considerações de segurança e privacidade específicas para o método DID.

- **Resolvedor DID**

O processo de obtenção do documento DID associado a um DID fornecido como entrada é realizado na Resolução DID, tomando-se por base a operação de leitura. Ele permite que aplicativos e serviços habilitados para DID obtenham os metadados disponíveis sobre o sujeito, expresso pelo documento DID. A partir de tais metadados é possível, por exemplo, pesquisar uma chave pública para verificar uma assinatura

digital, autenticar o controlador DID, solicitar uma conexão entre DIDs com o controlador DID, entre outros.

Os resolvedores DID podem ser construídos em várias formas de arquitetura. Podem ser implementados como uma biblioteca nativa, incluída em um aplicativo ou em um sistema operacional, ou mesmo ser fornecidos por terceiros como um serviço hospedado, respondendo a solicitações de resolução de DID via HTTP ou outros protocolos. Formas mistas também são possíveis, por exemplo, um resolvedor DID local pode delegar parte ou todo o processo de resolução DID a um resolvedor DID pré-configurado, hospedado remotamente.

Ao receber um DID como entrada, os resolvedores devem implementar as funções de resolução DID, que resolve um documento DID usando a operação *read/verify* do método DID. Ao receber um DID URL como entrada, deve-se executar um *DID URL dereferencing*, que é um componente de *software* ou *hardware* que usa uma DID URL como entrada e produz um recurso (e metadados associados) como saída.

2.3. Credenciais Verificáveis (VC)

Os identificadores descentralizados permitem que os usuários se autentiquem *online* de maneira descentralizada e preservem a sua privacidade. Porém, em muitos casos de uso, é necessário obter informações confiáveis sobre a identidade de alguém para realizar determinadas transações. Isso pode ser alcançado usando Credenciais Verificáveis (VC, do inglês *Verifiable Credentials*), que complementam os DID fornecendo um meio seguro e criptograficamente verificável para a troca de informações de identidade.

As credenciais verificáveis nos fornecem uma forma digital de credencial equivalente a que usamos em nossas vidas cotidiana, como carteira de motorista, passaporte ou diploma universitário, através da utilização de métodos seguros, os quais visam preservar a privacidade do detentor e permitir que a credencial seja verificável por máquina. As credenciais verificáveis geralmente contêm as informações necessárias sobre o seu titular e sobre a entidade que as emitiu.

As credenciais também suportam a divulgação seletiva, para que os usuários finais possam provar afirmações sobre sua identidade sem revelar mais informações do que o necessário para executar uma ação específica. As VC podem expressar qualquer informação

que contenha uma credencial física, mas o uso de assinaturas digitais do emissor e do titular as tornam invioláveis e mais confiáveis para o verificador.

2.3.1. Ambiente das Credenciais Verificáveis

O ambiente das credenciais verificáveis pode ser observado na Figura 4, na qual identificamos a presença dos seguintes elementos:

- Titular (*holder*).
- Emissor (*issuer*).
- Sujeito (*subject*).
- Verificador (*verifier*).
- Registro do Identificador (*identifier registry)*.

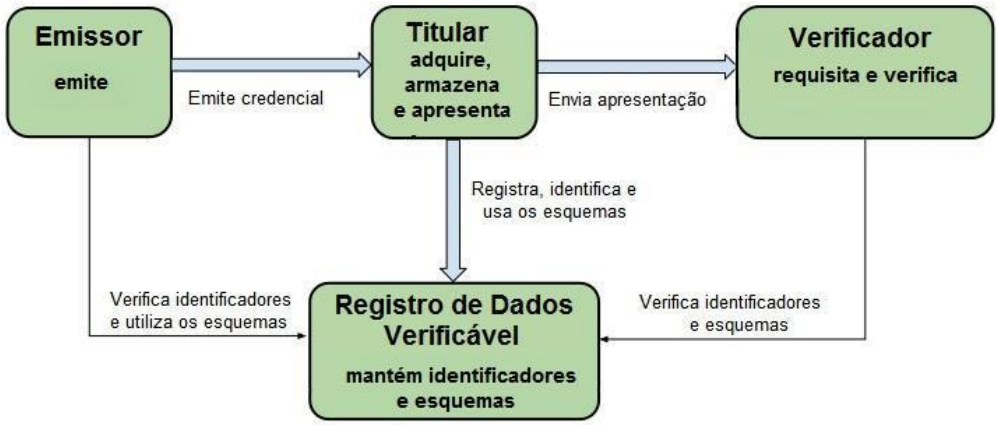

Figura 4. Papéis e fluxos de informações que formam a base para a especificação das Credenciais Verificáveis. Fonte: Sporny, 2020.

O titular adquire credenciais verificáveis dos emissores e as armazena para posteriormente apresentá-las a terceiros que as solicitem. O emissor é aquele que faz uma ou mais reivindicações de uma pessoa, criando credenciais a partir dessas reivindicações e transmitindo-as a um detentor. O sujeito é a entidade sobre a qual a reivindicação é feita. Em muitos casos, o titular de uma credencial verificável é o sujeito, mas em certos casos não. Por exemplo, um pai (o titular) pode possuir as credenciais verificáveis de uma criança (o sujeito), ou o dono do animal (o titular) pode possuir as credenciais verificáveis de seu animal de estimação (o sujeito).

A função do verificador é garantir que o titular cumpra alguns requisitos ao apresentar uma VC para que possam ser autenticadas. Registro do Identificador é um sistema no qual o titular pode registrar um identificador, possibilitando que ele interaja com emissores e verificadores, que poderão utilizar esse registro para verificar se o identificador é da pessoa que diz ser, antes de emitir ou solicitar uma credencial verificável.

As credenciais verificáveis (VC) facilitam as interações usando um padrão chamado triângulo de confiança, conforme pode ser visto na Figura 5. Os emissores criam credenciais, os titulares as armazenam e os verificadores solicitam provas com base nelas.

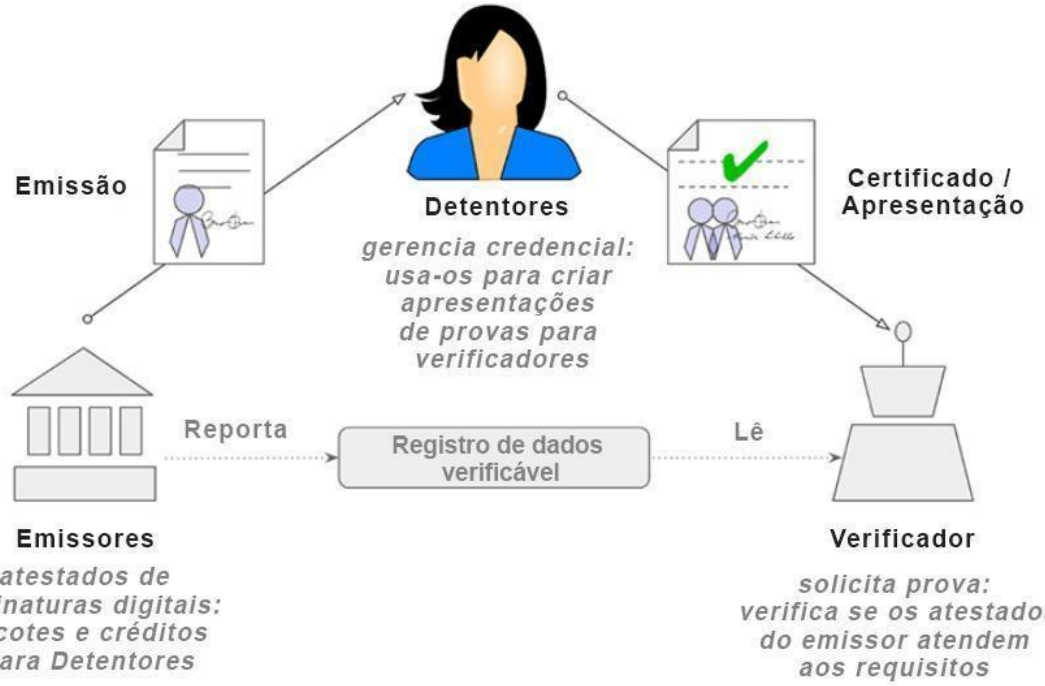

Figura 5. Triângulo de confiança das credenciais verificáveis. Fonte: própria. Adaptado da *wikipedia*.

As Apresentações Verificáveis (VP, do inglês *Verifiable Presentations*), por sua vez, são pacotes de evidências – credenciais ou dados derivados de uma ou mais credenciais. As VP são construídas pelos titulares para satisfazer os requisitos de um verificador. Os verificadores aprendem quais emissores atestaram algo verificando assinaturas digitais em um registro de dados verificável (normalmente, uma *blockchain*). Com reivindicações verificáveis, o verificador não precisa mais entrar em contato com o emissor para confirmar a credencial.

O titular mantém controle e propriedade sobre sua identidade e escolhe o que deseja divulgar e para quem divulgar. Por exemplo, ele pode provar que é eleitor registrado e ainda

não votou, sem revelar o nome ou o número de título. Essa estrutura fornece descentralização, flexibilidade e liberdade.

As VC buscam a interoperabilidade, segurança, controle e privacidade. Os atestados que eles fazem são apoiados por outra tecnologia de rastreamento de padrões, os Identificadores Descentralizados (DID). Ambos usam mecanismos de criptografia bem estabelecidos e as assinaturas digitais que as endossam possuem algoritmos documentados para verificação.

- **Modelo de dados das credenciais verificáveis a partir de um DID**

  Um modelo de VC pode ser visto na Figura 6. Como discutido, inclui um emissor, um titular da identidade e um verificador. Além disso, há um registro de dados verificável, o qual será mantido em um armazenamento descentralizado, como uma DLT. Estas credenciais incluem, ainda, uma camada intermediária referente aos identificadores descentralizados (DID).

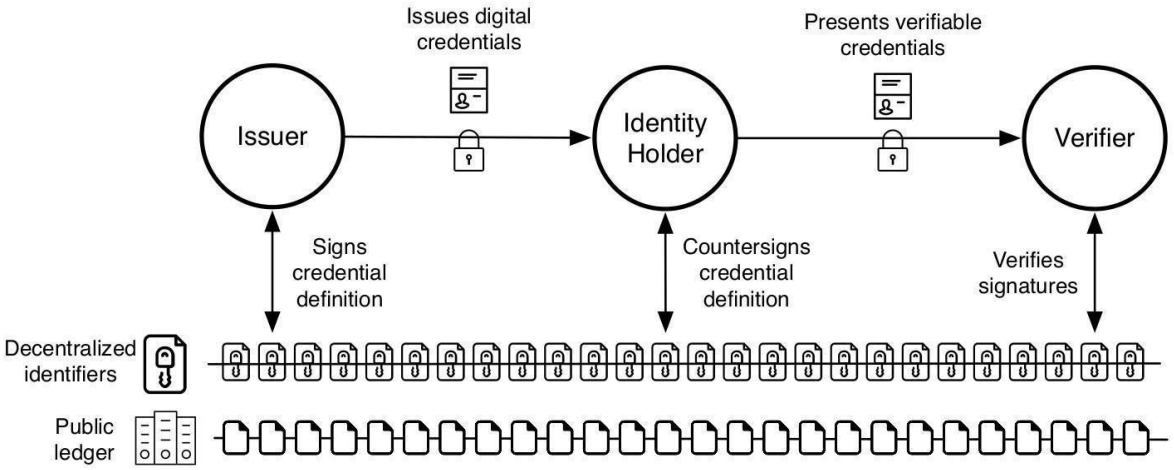

Figura 6. Modelo de Dados das Credenciais Verificáveis de um DID. Fonte: Lux, 2020.

- **Verificação das Credenciais Verificáveis**

  Um verificador define suas políticas para aceitar credenciais de detentores para seus serviços suportados. Uma característica notável das VC é que um verificador pode oferecer vários serviços e cada um deles pode ter uma política diferente. Isso ajuda a fornecer o recurso de privilégios mínimos, porque o verificador precisa solicitar apenas as propriedades do sujeito que são necessárias para o serviço solicitado. Cada

política definirá os emissores nos quais o verificador pode confiar para emitir VC para este serviço.

Os emissores emitirão credenciais verificáveis para os titulares finais, que irão armazená-las em suas carteiras digitais. O titular solicitará um serviço específico de um verificador e este retornará sua política ao Agente, que verifica se o Titular tem o conjunto necessário de VC em sua carteira, cumprindo, assim, a política. Esta credencial apresentada ao verificador pode vir, opcionalmente, dentro de uma apresentação verificável, que é um mecanismo de empacotamento para provar criptograficamente que o titular é quem está enviando os VC. O Verificador verifica:

a) se as VC e VP apresentadas possuem assinaturas digitais autênticas;

b) se as VC correspondem à sua política;

c) se o titular tem o direito de detê-los;

d) as condições postas na VP pelo titular para segui-las.

Se todas as condições forem satisfeitas, o verificador realizará o serviço solicitado para o titular; caso contrário, retornará uma mensagem de erro. No mundo *offline*, existem milhões de emissores de credenciais e milhões de verificadores, e todo o sistema é descentralizado. As relações de confiança são estabelecidas par-a-par diretamente entre detentores e verificadores. Essa orquestração é conhecida como modelo de rede de confiança.

2.4. Tecnologia de Livro Razão Distribuído - DLT

A Tecnologia de Livro Razão Distribuído (ou simplesmente DLT, do inglês *Distributed Ledger Technology*) ganhou notoriedade no ano de 2008, quando um indivíduo de pseudônimo Satoshi Nakamoto, criou e disseminou o conceito de criptomoedas através do seu artigo "*Bitcoin: A Peer-to-Peer Electronic Cash System*" (Nakamoto, 2008). A criptomoeda foi desenvolvida tomando por base uma DLT estruturada em uma cadeia de blocos ou *blockchain*. Posteriormente, a DLT passou a ser adotada em diversos contextos que não apenas o financeiro, tais como saúde, cadeias de suprimentos, internet das coisas, identidade digital.

Este avanço para outras áreas se deu devido às características intrínsecas da tecnologia como segurança, privacidade, imutabilidade dos dados, confiabilidade, entre outras. Uma rede *blockchain* permite a atuação de um grande número de nós no consenso das transações válidas, dificultando, assim, a ocorrência de fraudes e se apresentando como uma alternativa em potencial para o fornecimento de diversos serviços de confiança. Por sua vez, as transações devem obedecer as mesmas propriedades de banco de dados: Autenticidade, Consistência, Isolamento e Durabilidade (ACID). Nesse sentido, a criptografia e o consenso são os elementos chaves para manutenção da autenticidade, integridade, consistência e disponibilidade do livro-razão (NARAYANAN et al., 2016). Dependendo da proteção que se deseja - se quer confidencialidade, autenticação, integridade ou não-repúdio - é que se escolhe qual chave usar para codificar uma mensagem no processo de criptografia. Para se alcançar a integridade, consistência e a disponibilidade, cada um dos nós da rede *blockchain* possui todo o conteúdo do *ledger* armazenado localmente e, através de um processo de consenso, adicionam ou não um novo bloco na cadeia de blocos.

Uma rede *blockchain* pode ser entendida como um sistema distribuído, mantido e gerido de forma compartilhada e descentralizada por uma rede P2P, na qual todos os participantes são responsáveis por armazenar e manter a base de dados. O conceito tem como base quatro características arquiteturais:

(i) segurança das operações;

(ii) descentralização de armazenamento e computação;

(iii) integridade de dados; e

(iv) imutabilidade de transações.

- ***Blockchain* e Identidade Digital**

As aplicações relacionadas a identidade digital utilizando tecnologia *blockchain* permitem a verificação, autorização e gerenciamento de identidades inalteradas, o que reduz significativamente casos de fraudes. A tecnologia fornece o mecanismo ideal para identidades digitais, podendo fornecer uma solução para a forma como protegemos nossas informações *online,* utilizando criptografia e *ledgers* distribuídos.

Para se ter uma identidade descentralizada, que defende uma forma de identificação dependente e verdadeiramente controlada apenas pelo próprio usuário, alguns princípios devem ser buscados, como:

1. *Existência*: Os usuários devem ter uma existência independente. Ele nunca pode existir totalmente em formato digital;
2. *Controle*: Os usuários devem controlar suas identidades. Sujeito a algoritmos bem conhecidos e seguros que garantem a validade continuada de uma identidade e suas reivindicações, o proprietário é a autoridade máxima em sua identidade. Ele sempre deve ser capaz de fazer referência a ela, atualizá-la ou ocultá-la;
3. *Acesso*: Os usuários devem ter acesso aos seus próprios dados onde e quando desejarem, sendo capazes de recuperar facilmente as reivindicações e outros dados dentro de sua identidade, não devendo haver dados ocultos;
4. *Transparência*: Os sistemas usados para administrar e operar uma rede de identidades devem ser abertos, tanto na forma como funcionam, quanto na forma como são gerenciados e atualizados;
5. *Persistência*: As identidades devem ter vida longa ou pelo menos enquanto o usuário desejar. Mesmo que as chaves precisem ser trocadas ou os dados precisem ser alterados, a identidade permanece;
6. *Portabilidade*: Informações e serviços sobre identidade devem ser transportáveis, em vez de serem mantidas por uma única entidade terceirizada, mesmo se for uma entidade confiável, pois entidades podem desaparecer. Identidades transportáveis garantem que o usuário permaneça no controle de sua identidade, não importa o que aconteça;
7. *Interoperabilidade*: As identidades devem ser o mais amplamente utilizáveis possível, pois têm pouco valor se funcionarem apenas em nichos limitados;
8. *Proteção*: Os direitos dos usuários devem ser protegidos de conflitos entre as necessidades da rede de identidade e os direitos dos usuários individuais;

9. *Consentimento*: O titular deve concordar com o uso de sua identidade. Qualquer sistema de identidade é construído em torno do compartilhamento dessa identidade e de suas reivindicações. No entanto, o compartilhamento dos dados só deve ocorrer com o consentimento do usuário.
10. *Minimalização*: Quando os dados são divulgados, essa divulgação deve envolver a quantidade mínima de dados necessária para realizar a tarefa em mãos.

Observa-se que muitas dessas propriedades levantadas são intrínsecas à tecnologia *blockchain.* Por esta razão, ela representa um modelo eletivo para o uso de identidades descentralizadas, primando pela eliminação de uma autoridade centralizadora para verificar sua autenticidade.

- **Estrutura de uma *Blockchain***

Uma *blockchain* é uma cadeia de blocos que são ordenados de forma temporal e validados por meio de um algoritmo para resolver um problema matemático que envolve funções *hash* unidirecionais. O tamanho dessa cadeia cresce de acordo com o aumento do número de transações adicionadas. Cada bloco possui um *hash* exclusivo atribuído, que é formado pelo conjunto das transações que estão sendo incluídas neste bloco e o *hash* do bloco anterior.

Um bloco é criado no momento em que ele é validado pelo consenso da rede. Manter o *hash* do bloco anterior é o que garante a estrutura em cadeia dos blocos e previne a alteração de qualquer bloco ou que outro seja inserido entre dois blocos existentes. A alteração em qualquer uma das operações de um bloco invalida todo o restante da cadeia. Assim, cada bloco subsequente fortalece a checagem do bloco anterior e, consequentemente, de toda a *blockchain*.

Todos os dados em uma *blockchain*, após serem selados criptograficamente, são armazenados cronologicamente com um carimbo de data/hora permanente. Ela é formada por blocos encadeados por apontadores *hashes* em uma lista, na qual o primeiro bloco é designado bloco gênesis. Cada bloco contém um conjunto de transações, que são orquestradas numa estrutura de árvore binária de apontadores *hash*.

Uma transação estabelece uma sequência de operações sobre estados. Ela incorpora uma transferência de ativo ou um contrato inteligente. No geral, a transação envolve uma assinatura digital do emissor e o endereço do receptor, além de entradas (*inputs*) e saídas (*outputs*) das transações. Se a transação se refere a contratos inteligentes, pode envolver a invocação de um método com suas entradas; ou, se a intenção é a publicação (*deploy*) do contrato, deve conter o código de inicialização.

3. TRABALHOS RELACIONADOS

No melhor do nosso conhecimento não encontramos pesquisas com o mesmo foco específico deste trabalho: promover o lastreamento de identidades descentralizadas, ainda emergentes, a partir de associações verificáveis com identidades centralizadas já reconhecidas. Entretanto, alguns trabalhos possuem uma relação complementar com o que está sendo proposto no escopo desta pesquisa e serão apresentados a seguir.

Para a contextualização e desenvolvimento desta pesquisa, foram identificados e selecionados os trabalhos que se referem às identidades digitais descentralizadas, sobretudo os que consideravam a utilização de tecnologias distribuídas, a exemplo de DLTs, para a construção de novos modelos bem como trabalhos que realizam associação entre identidades digitais em outros contextos além do descentralizado.

O portal **gov.br**[9], por exemplo, foi projetado para unificar contas digitais e canais do governo federal. A conta gov.br identifica cada cidadão que acessa os serviços digitais no portal. Foi criado visando simplificar o acesso público aos vários serviços oferecidos *online*, viabilizar maior integração entre as entidades governamentais e garantir mais eficiência na prestação de serviços ao cidadão.

As autenticações na conta gov.br e assinaturas realizadas também associam outras autenticações para confirmar a identidade das entidades, podendo utilizar um código de confirmação por e-mail ou SMS, a combinação de dados biográficos e biométricos. Seus mecanismos utilizados para autenticação de acesso e assinaturas de documentos eletrônicos associam identidades digitais centralizadas para facilitar a vida do usuário. O Portal Gov.br é um impulsionador da tecnologia de identificação digital e de assinatura de documentos eletrônicos no Brasil, porém, apesar de associar várias formas de autenticação, até o momento da escrita desta dissertação, este portal ainda não possibilita realizar autenticação e assinatura digital utilizando identidades descentralizadas.

Atualmente, para fazer associação entre as identidades, deve-se fazer acordos proprietários entre as empresas. Ou seja, tem-se uma junta comercial que reconhece o gov.br e que faz acordos com terceiros, como por exemplo, um banco. Uma vez firmado este acordo, o

[9] gov.br - https://www.gov.br/governodigital/pt-br/conta-gov-br/

banco implementa a API do gov.br. A pessoa que está se autenticando decide entre utilizar o gov.br ou o banco e assim é direcionada para a interface escolhida onde realizará assinatura.

Uma possibilidade de uso deste trabalho seria assinar com o DID diretamente na junta comercial que reconhecesse o manifesto, por exemplo. Assim, se fosse utilizado o manifesto, seriam eliminadas essas indireções com um único certificado composto por uma assinatura qualificada (que agrega valor jurídico), como um certificado digital, e uma assinatura avançada (que usa criptografia), como um DID.

Em nossa pesquisa, analisamos também o *OpenID Connect* (OIDC), que atua como uma camada de autenticação e permite aos clientes verificarem a identidade do usuário final com base na autenticação realizada por um servidor de autorização, conforme definido no site oficial do OIDC[10]. Em Lux *et al.*, os autores implementaram como prova de conceito um provedor OIDC descentralizado, compatível com os conceitos da identidade autossoberana, abordando as credenciais verificáveis. O trabalho propôs uma infraestrutura de chave pública descentralizada com credencial verificável, utilizando DLT, que cria uma maneira direta e verificável de recuperar certificados digitais. O objetivo da proposta é pedir ao usuário as informações pessoais sem realmente ter uma conta de usuário no Provedor SSI OIDC. Assim, não existe uma base de dados central com dados pessoais em que o utilizador tenha de confiar e que esteja sujeita a ataques de *hackers*.

Os autores fizeram uma revisão dos métodos de autenticação de identidade autossoberana, implementaram e avaliaram a autenticação autossoberana para OIDC, e analisaram os benefícios de uma PKI com SSI. Apresentaram como proposta uma infraestrutura de chave pública descentralizada, sua abordagem consegue autenticar uma identidade centralizada como uma descentralizada.

Em nosso trabalho, para possibilitar essa integração entre sistemas centralizados e descentralizados, em vez de utilizar OIDC, propomos o uso da abordagem de identificadores descentralizados (DID) definidos pelo W3C, e associamos a um certificado digital obtendo maior confiabilidade ao utilizar a reputação existente de uma autoridade certificadora centralizada, armazenando tais dados em uma DLT. Assim podem servir como um registro publicamente verificável que incluem metadados de certificado X.509 necessários para verificar credenciais verificáveis.

[10] OIDC - https://openid.net/connect/

O *ShoCard*[11] é uma outra abordagem analisada, que propõe um sistema de gerenciamento de identidade federada seguindo o modelo autossoberano baseado em *blockchains*. Ele busca mapear credenciais tradicionais, normalmente físicas, digitalizando e publicando um hash em um livro-razão público distribuído.

Os usuários escaneiam suas credenciais, por exemplo seu passaporte, utilizando a câmera do dispositivo e os atributos são armazenados nos dispositivos móveis dos usuários. Um *hash* assinado desses dados, chamado *ShoCardID*, é armazenado em transações da *blockchain Bitcoin*. Em uma segunda etapa, esses dados devem ser certificados por um provedor de identidade (IdP) e o *hash* do certificado é publicado no livro razão do *Bitcoin*. Como o *ShoCard* utiliza em suas transações essa *blockchain* que demora em média 10 minutos para minerar as transações e realiza a espera por seis blocos adicionais para liquidação de uma transação, implica dizer que esta é uma restrição que limita o uso do *ShoCard* a cenários que exigem apenas identidades predefinidas (onde os atributos são conhecidos com antecedência), uma vez que não é possível criar identidades em tempo real.

Diferentemente do que ocorre com o *ShoCard*, este trabalho adota a *Blockchain Hyperledger* em detrimento da *Bitcoin*, pois não necessita de uma prova de trabalho dispendiosa para alcançar o consenso, que reduz o custo com energia e melhora o rendimento da transação. A confiança reside no consenso de um conjunto de nós validadores e do código, tornando-se mais econômica e rápida em seu processamento. Outro fator é que, neste trabalho, associamos a identidade descentralizada a uma centralizada reconhecida pela infraestrutura de chaves públicas brasileira, como não há necessidade de escanear documentos, o objeto gerado é então armazenado em uma carteira digital, enquanto que o *ShoCard* escaneia documentos para serem validados por um IdP, para gerar um *hash* desse conteúdo e armazenar em um bloco na *blockchain*.

O *uPort*[12] é um sistema de identidade autossoberana baseado no *Ethereum*. Seus desenvolvedores implementaram uma autenticação baseada nos perfis do *OpenID* utilizando DID compatível com *OpenID Connect*, que busca realizar *login* em um aplicativo *web* com autenticação DID. A equipe criou a especificação que define o *SIOP DID Profile*[13] (Terbu et al, 2020) para utilizar OIDC junto com a forte descentralização, privacidade e garantias de segurança de identificadores descentralizados. Uma forma genérica de integrar carteiras de identidade em seus aplicativos da *web*, em vez de ter um servidor centralizado que armazena

[11] ShoCard - https://shocard.com/
[12] uPort - https://www.uport.me/
[13] Também denominado apenas SIOP DID

os dados pessoais dos usuários. Apesar de desenvolverem produtos para a área de gerenciamento de identidades utilizando DLT, não tratam a possibilidade de mapeamento de uma identidade centralizada para uma identidade descentralizada.

Aqui no Brasil, algumas iniciativas também têm trabalhado com identificadores descentralizados para identidade dos cidadãos. No Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD), foram desenvolvidas algumas aplicações para identidades digitais descentralizadas que utilizam *blockchain*. Por exemplo, a solução *FinID* (CPqD, 2021) é um sistema de identidade digital descentralizada desenvolvido com o Banco Central (BC), no qual foi levantada uma rede para rodar a solução de identidade autossoberana para o setor financeiro nacional, conectando instituições e consumidores, fornecendo ao próprio dono (*holder*) da identidade digital a responsabilidade pelo controle e gestão dos seus dados.

Os autores afirmam que nos sistemas atuais o usuário tem uma identidade digital para cada instituição financeira com a qual tem relacionamento. Com a identidade digital descentralizada, essa credencial fica de posse do usuário, que pode apresentá-la a outras instituições com as quais não se relaciona, mas que têm uma oferta do seu interesse sem precisar de um terceiro intermediando. Nesta solução, adota-se a autenticação utilizando-se direta e unicamente identificadores descentralizados. Através da nossa solução a autenticidade de uma entidade pode ser atestada tanto com sua identidade centralizada quanto com sua descentralizada.

O CPqD produziu também a solução Simples Receita com a startup *WConnect*[14] e o apoio da EMBRAPII (CPqD, 2021). Também utilizou tecnologia *blockchain* para dar mais segurança e confiabilidade à prescrição digital de receituário médico, tendo o médico como emissor e o paciente como receptor. A intenção é permitir que o paciente atendido via telemedicina receba a receita em formato digital e possa utilizar a mesma plataforma para comprar medicamentos na farmácia sem sair de casa. Para isso, a rede *blockchain* desenvolvida reúne médicos, farmácias e pacientes.

Esta implementação faz interoperabilidade com um certificado digital X.509 para assinar a prescrição eletrônica, através de um PDF assinado e um JSON que é verificável na *blockchain*, permitindo uma verificação máquina a máquina sem intervenção de humanos. Acredita-se que, com a utilização de um manifesto de associação como o proposto neste trabalho, seria possível criar um identificador descentralizado para um médico que permitisse

[14] WConnect- https://wconnect.com.br/

verificar que o certificado X.509 é realmente de um médico, através da ligação dele com o seu CRM e gerar uma credencial única associando a identidade descentralizada e o certificado.

Foi feito um comparativo entre alguns desses trabalhos encontrados e a solução feita nesta pesquisa, denominada *LinkedID*, comparando-os quanto a algumas das características consideradas importantes. Uma delas diz respeito ao *multitenancy*, que é a capacidade de uma única instância atender a vários usuários. Quanto à premissa da descentralização, o *LinkedID* poderia ser considerado parcialmente descentralizado por conter em sua solução uma identidade centralizada, porém parte-se do princípio que o usuário já possui uma e a utiliza para associar a uma descentralizada, após a associação o artefato gerado ficar em ambiente descentralizado, o que justifica sua classificação como descentralizado.

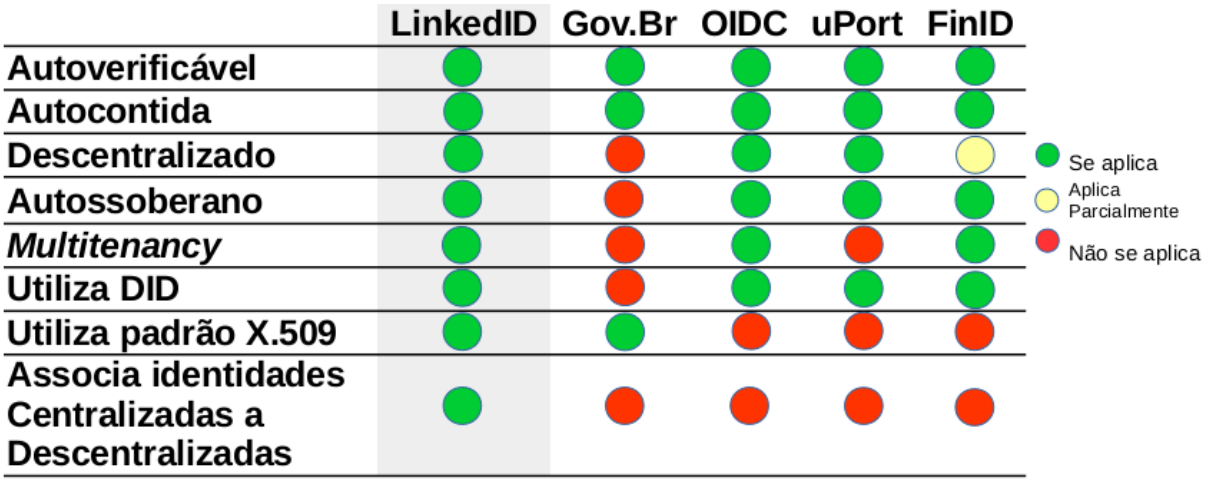

Figura 7. Comparativo entre soluções.

Fonte: Própria.

Considerando que a proposta gera um único artefato (Manifesto) que se refere a duas identidades de forma autocontida, tem-se que tal simplicidade também facilita sua manutenção, possibilitando que o artefato seja gerado em arquivos de texto puro, que demandam pouco espaço de armazenamento nos sistemas e são facilmente gerenciáveis. A partir disso do artefato autocontido, é possível verificar seu conteúdo, o que o torna auto verificável. Pode-se prever a exigência de baixo investimento na implementação desta proposta e a possibilidade de utilizar serviços intermediadores para realização de registro de forma descentralizada. Como dito, utiliza DID e certificado digital X.509 na associação das identidades e, conforme definido na Seção 2.4, atende às características elencadas como pré-requisito para ser considerado autossoberano.

4. PROPOSTA DA SOLUÇÃO

As identidades descentralizadas podem ser usadas por suas entidades detentoras para interagirem com outras entidades, de forma confidencial e segura. O uso de pares de chaves assimétricas permite validar mensagens assinadas, confirmar pedidos de autenticação ou verificar afirmações apresentadas, como nas identidades centralizadas, mas sem a necessidade de entidades confiáveis intermediárias, garantindo que a propriedade da informação fique sob a posse do seu titular.

Tomando por base uma iniciativa como o portal gov.br, por exemplo, que unificou em uma só plataforma diversos canais digitais, buscando melhorar a experiência do usuário, podemos verificar que através dele o cidadão pode buscar por serviços oferecidos pelo governo, todos em um só lugar. Para ter acesso, o usuário deve informar seu CPF e realizar um cadastro. Já para obter maior confiabilidade na conta, o proprietário dela pode mudar de nível de autenticação, que é um recurso de segurança da informação da identidade e que permite flexibilidade para realização dos próximos acessos. Os níveis são divididos em: bronze, prata ou ouro e consistem em orientar para qualificação das contas ao obter os atributos autoritativos do cidadão a partir de outras bases oficiais do governo, unindo essas credenciais de acesso.

Assim, cada vez o governo detém em suas bases de dados mais informações pessoais dos cidadãos, através de dados sensíveis que muitas vezes têm seu uso autorizado através dos termos de contrato que são assinados eletronicamente. Se fossem utilizadas as identidades descentralizadas para autenticação nesse tipo de sistema, fazendo uso de carteiras digitais, o usuário conseguiria provar que é quem diz ser sem precisar se expor, nem ter seus dados armazenados em servidores centralizados, tornando o processo menos burocrático e preservando o direito à privacidade.

A parte do consenso de enorme potencial que o modelo de identidades descentralizadas pode trazer para a construção de serviços e aplicações com maior robustez e privacidade, há ainda desafios a serem vencidos para a sua adoção em larga escala. Dentre eles está a promoção da sua aceitação tácita e inequívoca em todos os cenários da sociedade, incluindo os contextos fiscais e jurídicos.

Neste sentido, abordagens mais tradicionais baseadas no modelo de identidades digitais centralizadas já possuem um amplo reconhecimento jurídico, amparado por um vasto arcabouço de normas e regulamentações disponíveis, com algum grau de adaptação à realidade local, em praticamente todos os países através das suas infraestruturas de chaves públicas nacionais.

A hipótese complementar deste trabalho é que a adoção e o uso de identidades descentralizadas pode ser alavancada, em alguns cenários, a partir do uso de identidades centralizadas associadas como uma espécie de lastro, beneficiando-se assim do reconhecimento fiscal e jurídico já estabelecido para as centralizadas.

Neste contexto, foi idealizado um mecanismo que possibilita unir os dois modelos, criando um modo de identificar uma entidade que tanto possa atuar unicamente de forma descentralizada, mas que também possa receber como associação uma identidade centralizada, que seja verificável e autocontida. Esta é uma alternativa que pode subsidiar fases de transição ou, até mesmo, viabilizar a possibilidade de cenários híbridos de coexistência entre identidades de natureza distintas. Obtendo-se um lastro da identidade centralizada na identidade descentralizada, que passa a fornecer uma referência adicional sobre a entidade representada, torna o processo de gestão de identidades ainda mais confiável e interoperável.

Propõe-se, portanto, o uso de tecnologias e compromissos criptográficos como base para o desenvolvimento de um modelo autocontido e verificável de associação entre identidades digitais descentralizadas e identidades centralizadas para permitir a sua coexistência em diversos contextos de aplicação.

4.1. Dinâmica da Associação

Esta seção apresenta a dinâmica da associação entre identidades centralizadas e descentralizadas, apresentando o compromisso criptográfico, a prova de posse e a prova de associação.

O estabelecimento da associação deve ocorrer de uma forma que seja possível comprovar que uma entidade é o detentor de ambas as identidades apresentadas e permitir validar atos criptográficos feitos por qualquer uma das duas identidades.

As condições básicas para realizar a associação em pauta são as seguintes:

i) a entidade de interesse deve possuir uma identidade centralizada válida e validável;

ii) a mesma entidade de interesse deve possuir um identificador descentralizado válido e validável.

O processo de associação será concretizado através da criação de um artefato verificável específico para a associação, que será emitido pelo próprio titular das duas identidades envolvidas e obedecerá uma estrutura própria.

4.1.1. Compromisso Criptográfico

Um compromisso criptográfico é um esquema que permite que uma entidade se comprometa com um valor escolhido enquanto o mantém oculto, com a capacidade de revelar o valor posteriormente. Similar a um contrato firmado entre interessados, no qual a mensagem trocada seria mantida segura em um envelope e lacrada, para ser mantida em segredo (oculta) até que seja necessário torná-la conhecida.

Um esquema de compromisso criptográfico tem duas propriedades principais: *oculta* e *vinculativa*. A primeira protege os interesses do emissor para, ao final do compromisso, o receptor não obter nenhuma informação adicional sobre a declaração que passou pelo processo. A propriedade vinculativa, por sua vez, protege os interesses do destinatário, pois os esquemas de compromissos são concebidos de forma que uma parte não possa alterar o valor ou a declaração depois de se comprometer com ele.

O processo de associação aqui proposto utiliza compromissos criptográficos em duas camadas, que se combinam para permitir a produção de um artefato autossoberano para uma entidade. Nessas camadas, utiliza-se a combinação de assinaturas digitais, *hashes* e encriptação de dados para prover a associação segura entre as identidades.

O processo de associação usa alguns dados referentes às identidades envolvidas (descentralizada e centralizada) para montar um bloco de declarações. Em seguida, tal bloco será assinado com a chave privada da identidade descentralizada do titular, gerando um *hash* do conteúdo. Ao final desse bloco, adicionam-se dados para verificação do que foi assinado, como o método de verificação, o tipo de assinatura realizada, a chave pública correspondente à chave privada da assinatura e o conteúdo assinado.

Por fim, esse conteúdo (bloco contendo as declarações e a assinatura descentralizada) passará por uma nova assinatura realizada com a chave privada da identidade centralizada. Ao final, também será acrescentado conteúdo para verificação desta assinatura, compondo assim o bloco de controle.

Dessa forma, gera-se uma ligação entre as identidades e monta-se um artefato de associação verificável de forma autônoma por qualquer interessado.

4.1.2. Prova de Posse e de Identidade

O artefato de associação proposto permite a realização de **duas provas criptográficas** usando as chaves públicas das identidades associadas, às quais chamamos de **prova de posse e prova de identidade**.

A **prova de posse** é utilizada pelo interessado para legitimar o vínculo da entidade detentora do artefato com a identidade descentralizada em pauta, indicando se a entidade possui acesso à chave privada da identidade descentralizada associada. Só quem possui essa chave poderia realizar a assinatura digital com a chave pública correspondente da identidade descentralizada.

A **prova de identidade**, por sua vez, tem como finalidade atestar que a entidade que está declarando a associação é quem diz ser. Tal validação é feita a partir do certificado digital da entidade, que é emitido por uma autoridade certificadora reconhecida e, ao ser usado para assinar o bloco de declarações, agrega validade jurídica à associação entre as identidades. A prova propriamente dita se resume a verificar se a assinatura foi feita com a chave privada equivalente à chave pública do certificado digital usado na associação.

As duas provas funcionam de forma consolidada, cooperativa e entrelaçada, para criar uma ligação verificável entre as identidades centralizadas e descentralizadas envolvidas na associação, permitindo validar atos criptográficos envolvendo as respectivas chaves privadas de forma intercambiável.

4.2. Manifesto de Associação

A seguir, a geração do artefato autodeclarado pela entidade para associar as suas identidades será descrita de forma detalhada. O artefato foi denominado de **Manifesto de Associação**.

4.2.1. Modelo Proposto

Em conformidade com o objetivo específico 4 da Seção 1.2, foi desenvolvido um modelo para geração do manifesto de associação que é composto de dois blocos: **Bloco de Declarações** e **Bloco de Controle**. No Bloco de Declarações são informados os dados da identidade descentralizada (identificador único, identificador do local onde está registrada) e dados da identidade centralizada (número de série e nome da entidade). É calculado o *hash* do conteúdo do bloco de declarações, que é então duplamente assinado digitalmente utilizando as chaves privadas das identidades descentralizada e centralizada. A assinatura final e informações sobre como o *hash* e as assinaturas foram obtidas formam o Bloco de Controle, para permitir que o manifesto seja auto verificado posteriormente por qualquer interessado. O modelo proposto está ilustrado na Figura 8.

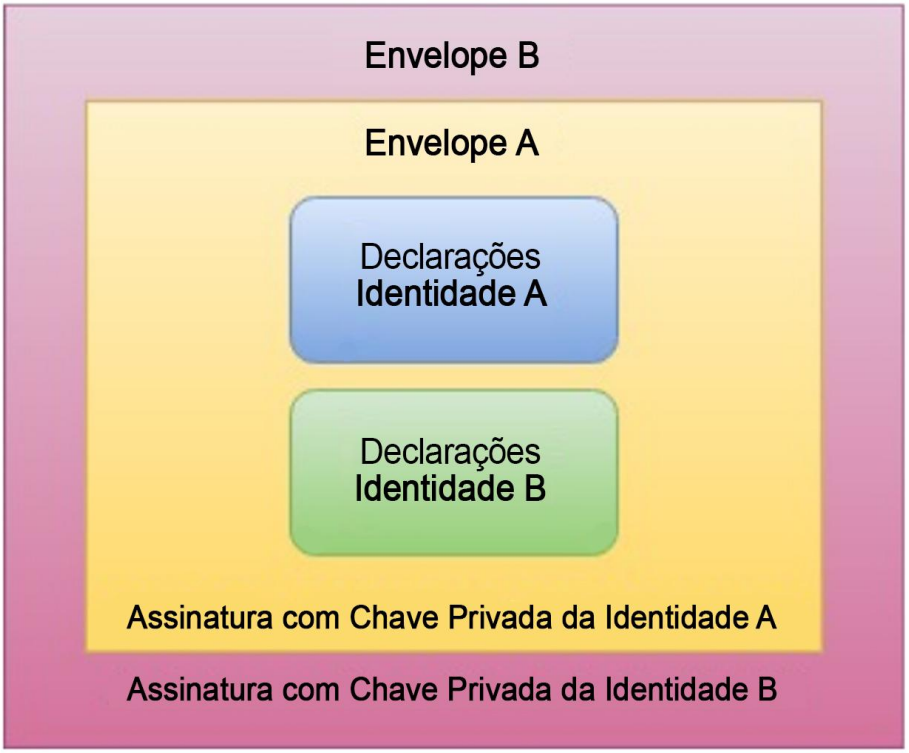

Figura 8. Modelo de assinatura de um Manifesto de Associação.

Fonte: Própria.

De maneira formal, o manifesto de associação da identidade centralizada *IDC* com a identidade descentralizada *IDD*, ambas pertencentes à entidade *E*, é representado pela seguinte tupla ${}^{E}A^{IDC/IDD} \rightarrow \{\boldsymbol{BD}, \boldsymbol{BC}\}$, onde ***BD*** é o bloco de declarações e ***BC*** é o bloco de controle.

O bloco de declarações ***BD*** é composto pelo conjunto de dados ***dc*** necessários da identidade centralizada *IDC*, pelo conjunto de dados necessários da identidade descentralizada *IDD*, pela data de emissão ***e*** e pela data de validade ***v*** do manifesto (opcional), é representado pela tupla $\boldsymbol{BD} \rightarrow \{\boldsymbol{dc}, \boldsymbol{dd}, \boldsymbol{e}, \boldsymbol{v}\}$.

O bloco de controle ***BC***, por sua vez, é representado pela tupla $\boldsymbol{BC} \rightarrow \{\boldsymbol{a}^{IDD}, \boldsymbol{a}^{IDC}\}$, onde $\boldsymbol{a}^{IDD}$ é a assinatura realizada com a identidade descentralizada *IDD* e $\boldsymbol{a}^{IDC}$ é a assinatura realizada com a identidade centralizada *IDC*.

A primeira assinatura do bloco de controle é representada pela seguinte tupla $\boldsymbol{a}^{IDD} = \{\boldsymbol{c}^{IDD}, \boldsymbol{vm}, \boldsymbol{t}, \boldsymbol{va}^{1}\}$, onde $\boldsymbol{c}^{IDD}$ é o certificado de *IDD*, ***vm*** é o método de verificação a ser utilizado, ***t*** é o tipo da assinatura realizada e $\boldsymbol{va}^{1}$ é o valor assinado, que é obtido pela seguinte operação:

$$va^1 = sign(\ hash(\ \mathbf{BD}\ ),\ c^{IDD}.prvkey,\ vm,\ t),$$

onde $c^{IDD}.prvkey$ *é* a chave privada da identidade descentralizada *IDD* e *sign* e *hash* são funções para assinatura e cálculo de resumos matemáticos, respectivamente.

A segunda assinatura do bloco de controle também é representada pela tupla $a^{IDC} = \{c^{IDC}, vm, t, va^2\}$, onde c^{IDC} é o certificado de *IDC*, ***vm*** é o método de verificação a ser utilizado, ***t*** é o tipo da assinatura realizada e va^2 é o valor assinado que, neste caso, é obtido pela seguinte operação:

$$vb^2 = sign(\ va^2,\ c^{IDC}.prvkey,\ vm,\ t),$$

onde $c^{IDC}.prvkey$ *é* a chave privada da identidade centralizada *IDC*.

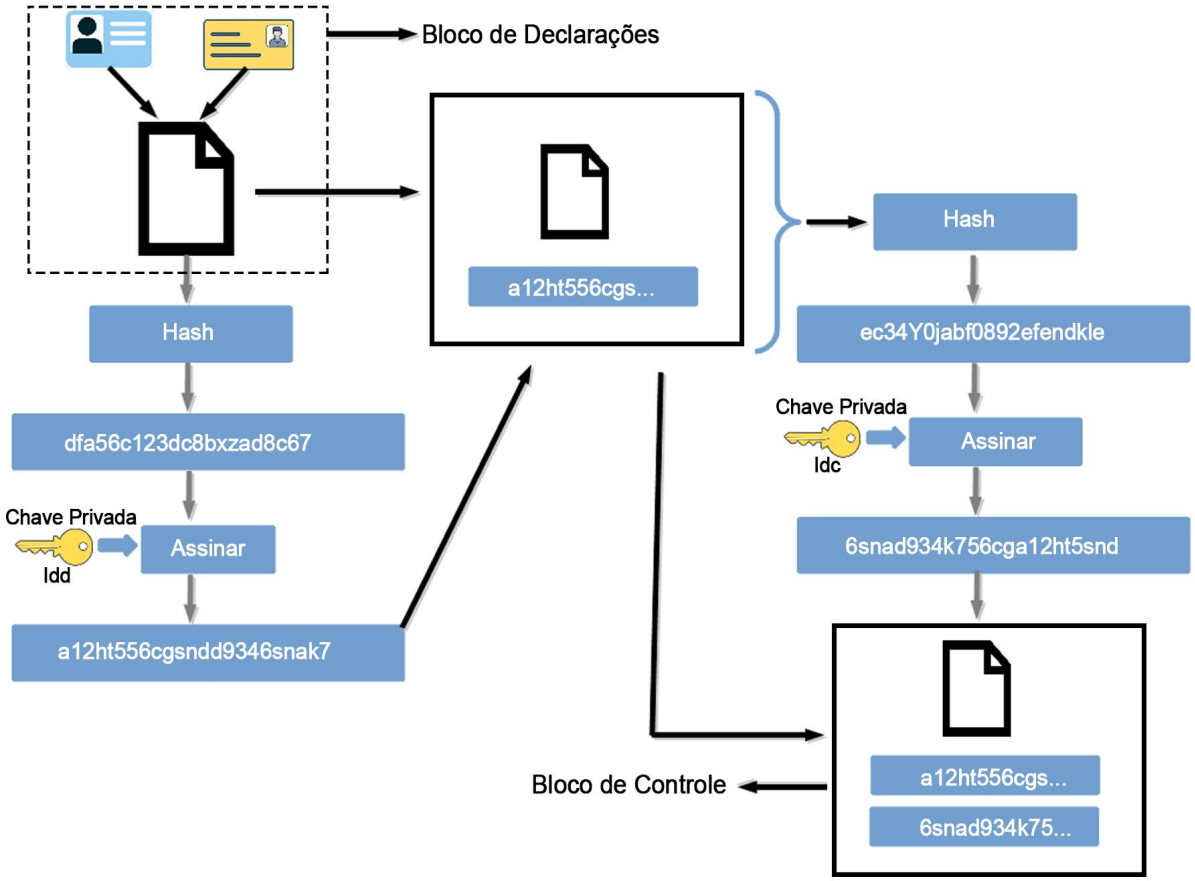

Figura 9. Fluxo de geração de um Manifesto de Associação. Fonte: Própria.

4.2.2. Protocolo de Verificação

Para a verificação do manifesto de associação entre as identidades centralizadas e descentralizadas é feito um processo inverso ao de geração, utilizando as chaves públicas. A verificação é feita de forma autônoma, uma vez que o manifesto armazena as informações necessárias para o processo de verificação da autenticidade das identidades e utiliza procedimentos padronizados, como algoritmos públicos.

Na medida em que cada assinatura vai sendo decriptada, será encontrado um *hash* de um artefato da associação. A partir disso, basta tomar por base o conteúdo original e executar a mesma função de *hash* para encontrar um resumo resultante.

Retomando as operações va^1 e va^2 feitas no processo de geração descritas na subseção 4.2.1 e realizando o processo inverso iremos, a partir de va^2, obter va^1. Na sequência, obter o *hash* de ***BD*** valida o seu conteúdo e, consequentemente, a associação entre *IDC* e *IDD*. O fluxo para verificação do manifesto pode ser observado através da Figura 10 e descrito nas seguintes etapas:

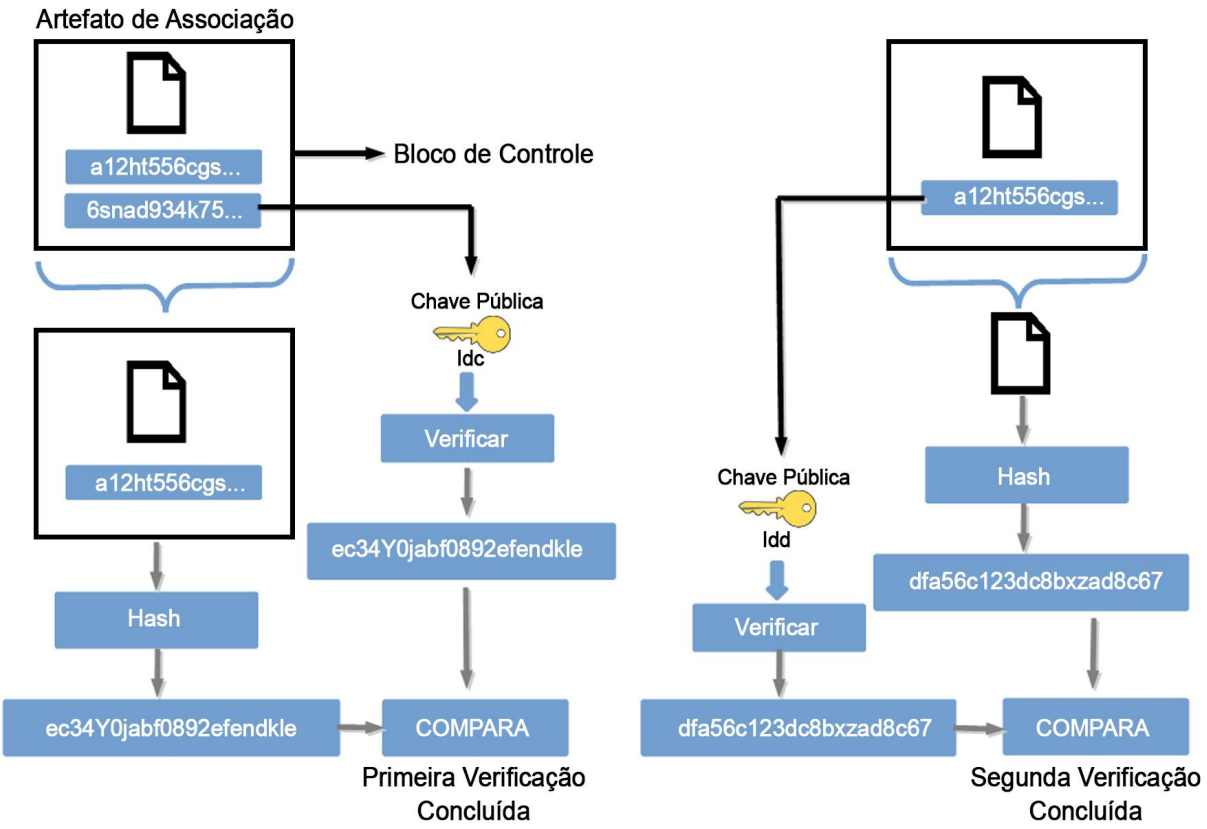

Figura 10. Fluxo de verificação das assinaturas de um Manifesto de Associação. Fonte: Própria.

Em resumo, para *prova de posse* da identidade descentralizada deve-se realizar as seguintes verificações:

- *hash*(***BD***) = Decrypt(va^1, c^{IDD}***.pubkey***, ***vm***, ***t***)
- ***BD.dd.id*** = a^{IDD}. c^{IDD}***.id***

Para *prova de identidade* da identidade centralizada deve-se realizar as seguintes verificações:

- va^1 = Decrypt(va^2, c^{IDD}***.pubkey***, ***vm, t***)
- ***BD.dc.id*** = a^{IDC}. c^{IDC}***.id***

4.3. Premissas

O manifesto de associação proposto deve, idealmente, ser autocontido, autoverificável, transparente, descentralizado, autossoberano, voluntário e opcional.

Autocontido

O manifesto gerado armazena em seu bloco de controle todo o conjunto de provas das identidades associadas (prova de posse e prova de identidade). Ou seja, a comprovação de que o usuário possui uma das identidades está contida no manifesto, o que significa que ele não depende de acordos com Autoridades Certificadoras, não depende de sistemas complexos para validar sua identidade e que o artefato é independente de sistema específico.

Autoverificável

Para atendimento dessa premissa as provas de posse e identidade contém informações para serem verificadas de forma autônoma por algum terceiro interessado usando apenas o conteúdo do próprio manifesto. As provas são baseadas em padrões abertos e o manifesto possui todas informações necessárias para que um interessado consiga verificar a autenticidade e a integridade dos dados. Ao verificar a integridade do conteúdo, um destinatário do manifesto pode constatar se o item recebido não foi modificado durante a transmissão. Enquanto verifica a autenticidade, pode constatar se o manifesto recebido é realmente da entidade que o apresenta. Para isto, ele inclui chaves públicas que são usadas como método de verificação. Essas chaves podem ser usadas para autenticar o proprietário das identidades, mas também para verificar assinaturas digitais geradas por ele e outras informações relacionadas.

Transparente

A emissão do manifesto ocorre de forma transparente ao usuário, que não precisa ter conhecimento sobre assinatura digital, geração de hash ou uso específico de determinadas tecnologias para emitir, gerenciar e compartilhar um manifesto de associação. A decisão de usá-lo cabe ao proprietário, mas caso opte por não utilizar o manifesto, suas identidades descentralizada e centralizada continuarão a funcionar normalmente em seus ambientes. A associação é uma possibilidade de embuti-la em um objeto típico desse ambiente descentralizado que estamos representando.

Descentralizada

Mesmo realizando a associação com uma identidade centralizada, a natureza desse manifesto é descentralizada e, após ser gerado, será armazenado em uma carteira digital criada para o dono das identidades. A posse dele permanece nesse ambiente descentralizado enquanto existir e não será gerenciada por uma entidade centralizada.

Autossoberana

De acordo com este critério, somente o titular das identidades digitais envolvidas pode ser capaz de emitir o manifesto de associação e deve ter autonomia de decidir quando e com quem compartilhá-lo. Algumas características intrínsecas dessa premissa definem que este objeto gerado deve ser descentralizado, interoperável, acessível, controlado por seu titular, transparente e persistente.

Voluntária

Após criar sua identidade digital descentralizada, o detentor pode voluntariamente associá-la a uma identidade centralizada válida que possua, realizando a associação verificável de forma autônoma, conforme descrito nesta proposta. Caso não realize a associação, poderá utilizar normalmente o identificador descentralizado em seu ambiente específico.

Opcional

Caso não deseje realizar a associação entre suas identidades, o usuário poderá utilizar apenas para criar uma carteira digital, bem como para criar e registrar identidade descentralizada para o titular da carteira.

5. PROVA DE CONCEITO

Para validar a aplicabilidade da proposta apresentada no Capítulo 4 e atingir o objetivo específico 5 da Seção 1.2, foi definida uma prova de conceito que demonstra como construir um manifesto de associação de forma concreta, utilizando um par real de identidades centralizadas e descentralizadas para ilustrar como a proposta poderia ser adotada considerando as características específicas de cada uma das identidades associadas.

5.1. Identidades a serem Associadas

Esta prova de conceito da proposta de associação de identidades usará como base a especificação da W3C de **Identificadores Descentralizados (DID),** para representar a identidade descentralizada. Para representar as identidades digitais centralizadas, serão usados certificados digitais **e-CPF/e-CNPJ, representações digitais de pessoas físicas e jurídicas da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)**, cujo protocolo será aplicado na verificação da viabilidade de associação entre identidades.

5.1.1. Identidade Centralizada: eCPF/eCNPJ

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma implementação de uma PKI baseada em terceiros confiáveis, como Autoridades Certificadoras, para a emissão de chaves de forma segura que utiliza o padrão de certificado X.509 de acordo com a padronização internacional para uso na internet.

As Autoridades Certificadoras (AC) emitem Certificados Digitais, que possuem mecanismos para possibilitar a confirmação da autenticidade de uma entidade. Uma AC coleta evidências que associam uma entidade (por exemplo: pessoa, organização, máquina, empresa etc) a uma chave criptográfica. Estas evidências são materializadas na forma de certificados digitais, que são documentos eletrônicos usados para identificar um indivíduo, uma empresa ou uma entidade e associá-lo a uma chave pública (Stallings, 2013).

A credibilidade sobre um certificado digital está associada às entidades e à organização da ICP que o produziu. A ICP-Brasil utiliza as assinaturas digitais em documentos eletrônicos assinados por chaves emitidas por uma Autoridade Certificadora da cadeia que são juridicamente reconhecidas. Por esta razão, para esta prova de conceito, foram escolhidos o **Certificado Digital e-CPF**, que é a identidade digital da pessoa física, e o **Certificado Digital e-CNPJ**, que é direcionado para empresas, ambos bastante adotados no Brasil e que conferem autenticidade, confidencialidade, integridade e não repúdio aos documentos por eles assinados.

5.1.2. Identidade Descentralizada: DID

Em uma **Infraestrutura de Chaves Públicas Descentralizadas**, a confiança nos dados não é garantida por um terceiro de confiança como ocorre nas PKI, mas sim na rede descentralizada, permitindo que qualquer entidade na rede consiga criar e gerenciar seus identificadores. Neste contexto, se encaixa a especificação de identificador descentralizado (DID) da W3C, já definido e detalhado na Seção 2.2, na qual pode-se verificar seu conceito, componentes, formatos e objetivos. Este foi escolhido para representar a identidade descentralizada nesta prova de conceito.

De forma sucinta, DID são URIs que associam uma entidade a um *Documento DID*, permitindo uma interação confiável com essa entidade. Um DID é resolvido por um elemento chamado "*resolver*", que aponta para uma estrutura de dados intitulada *DID Document*, o qual fornece chaves-públicas para a verificação de provas criptográficas e expõe serviços com os quais o titular pode interagir.

Os DIDs possuem propriedades intrínsecas que se adequam àquelas propriedades definidas para se obter uma identidade autossoberana, que concede aos titulares dos dados mais controle sobre suas informações, inclusive acesso a elas quando desejar, definindo também quem poderá acessá-las e quando. Outrossim, os DIDs se adequam, ainda, ao decreto nº 10.332, de 28 de abril de 2020, que institui a Estratégia de Governo Digital para o período de 2020 a 2022, como citado na Seção 1.1.

5.1.3. Estrutura do Manifesto de Associação DID e eCPF/eCNPJ

A organização do manifesto de associação utilizado para gerar um elo entre um **DID e um e-CPF/e-CNPJ** segue o modelo geral descrito no Capítulo 4 e pode ser visualizada através da Figura 11. O manifesto engloba as declarações sobre o titular e o conteúdo para verificação de autenticidade das assinaturas é acrescentado ao final do documento, conforme o modelo de assinatura envelopada. O conteúdo da assinatura é o próprio documento e o valor da assinatura é adicionado juntamente com o certificado digital do titular. Com isso, obtém-se um artefato autocontido que possui os componentes essenciais para a verificação de autenticidade da informação criptografada.

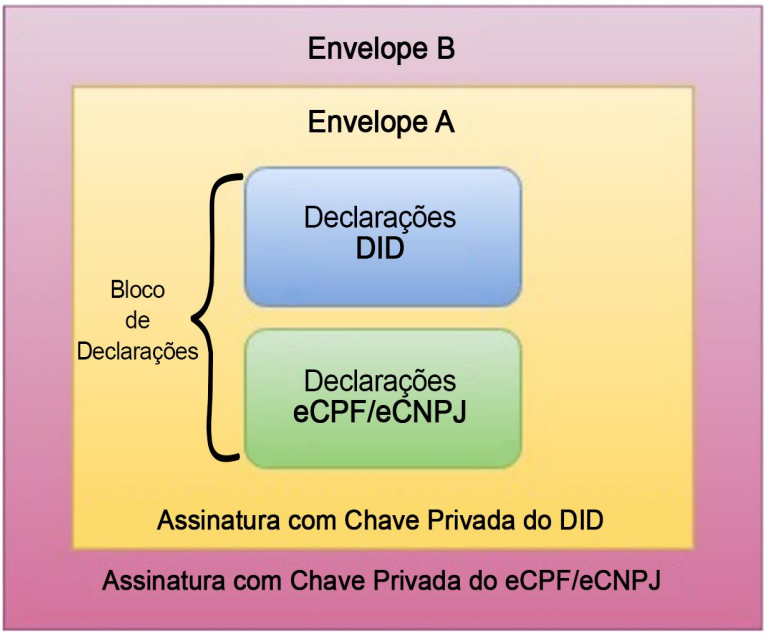

Figura 11. Modelo de assinatura de um Manifesto de Associação entre DID e e-CPF/e-CNPJ.
Fonte: Própria.

Ao final do Manifesto de Associação duplamente assinado, adiciona-se a ***verkey*** (chave pública) associada ao DID para a verificação da prova de posse e o certificado digital com a respectiva chave pública para a verificação da prova de identidade. O fluxo seguido para composição do artefato completo é exibido na Figura 12.

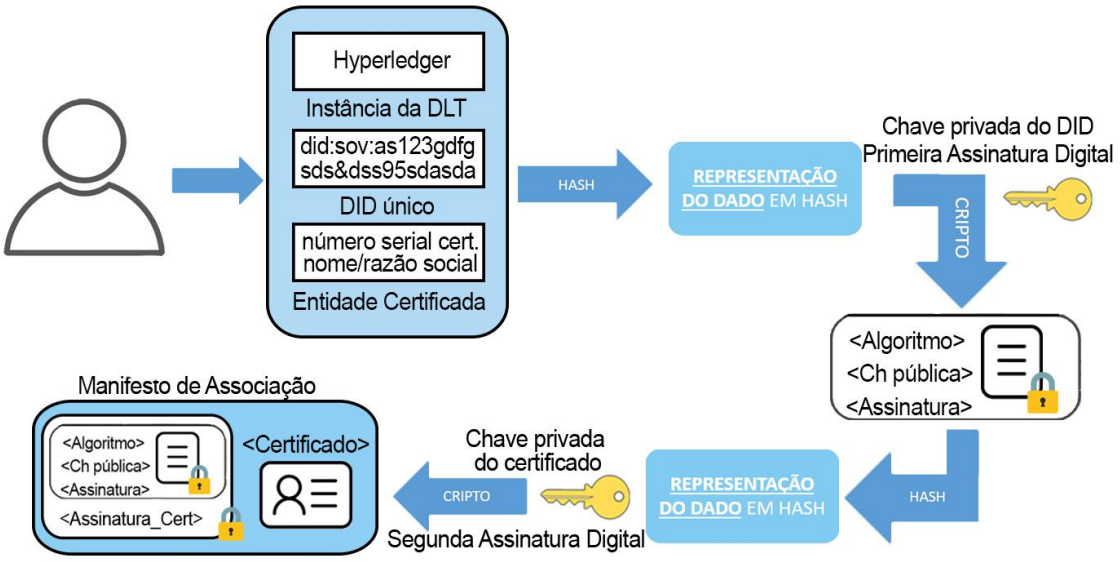

Figura 12. Fluxo de assinatura do Manifesto de Associação entre DID e eCPF/eCNPJ

Fonte: Própria.

5.1.4. Geração do Manifesto de Associação DID e e-CPF/e-CNPJ

Para esta prova de conceito, definiu-se um esquema específico de uma credencial que determina a estrutura de dados adotada no manifesto, ou seja, a semântica adotada, e será referenciado através do contexto do bloco no momento do compromisso criptográfico. A utilização desses esquemas representa uma boa prática por permitir uma ontologia comum entre as aplicações, a interoperabilidade e por seguir padrões.

Iniciamos a montagem do bloco informando o esquema adotado, incluindo em seguida as declarações sobre o DID e o e-CPF/e-CNPJ. As informações a serem incluídas são: identificador DID, o registro onde foi publicado, o número serial do e-CPF/e-CNPJ, o nome/razão social e informações que não são tidas como sensíveis. Esses dados compõem o bloco de declarações a ser assinado com a chave privada do DID (primeiro envelope - Envelope A).

Essa assinatura será realizada utilizando o formato JWS (*JSON Web Signature*), após ser assinado, temos o conteúdo original das declarações mais um bloco de controle denominado *proof*. Este possui, entre outras informações, o método de verificação, o algoritmo utilizado (Ed25519), a data da assinatura e o JWS gerado, conforme pode ser verificado na Figura 13.

Figura 13. Exemplo de um bloco do Manifesto de Associação assinado pelo DID (JWS).
Fonte: Própria.

Esse bloco assinado com o DID do titular gera um fluxo de *bytes* referente ao documento assinado contendo declarações das duas identidades mais o bloco de controle da primeira assinatura. Em seguida, gera-se um hash utilizando o algoritmo SHA-256, que será cifrado (assinado) com a chave privada correspondente ao e-CPF/e-CNPJ de posse do mesmo titular.

Após a assinatura, será acrescentado ao final do documento, um novo bloco de controle, usado para armazenar a assinatura digital, o algoritmo utilizado no processo de assinatura, o certificado digital e o valor assinado. Após a inclusão deste segundo bloco de controle, obtém-se um manifesto de associação entre um DID e um eCPF/eCNPJ específicos.

5.2. Algoritmo de Verificação

A verificação do manifesto de associação DID e eCPF/eCNPJ ocorre seguindo o processo inverso ao apresentado na seção anterior. A validação utilizará as chaves públicas do certificado digital e do DID (chamada *verkey*) para realizar a verificação, que é baseada em

algoritmos públicos e pode ser feita de forma soberana a partir do bloco de controle contido no próprio manifesto.

Assim, utiliza-se a chave pública do certificado digital do eCPF/eCNPJ para verificar a autenticidade da *prova de identidade*, associando o manifesto ao titular do eCPF/eCNPJ utilizado. Igualmente, utiliza-se a chave pública do DID para verificação da *prova de posse* e associar o manifesto ao detentor do identificador descentralizado (DID).

O fluxo de verificação das provas para a validação do manifesto de associação DID-eCPF/eCNPJ pode ser verificado na Figura 14. Através da imagem pode-se constatar que, ao decriptar a assinatura com a chave pública correspondente, encontra-se um resumo (*hash*) do bloco assinado. Para a verificação da autenticidade, ao aplicar a mesma função no artefato original (não-assinado), obtém-se também um resumo (*hash*). De posse dos dois conteúdos é possível compará-los e, se o resultado da comparação for verdadeiro, o manifesto é válido.

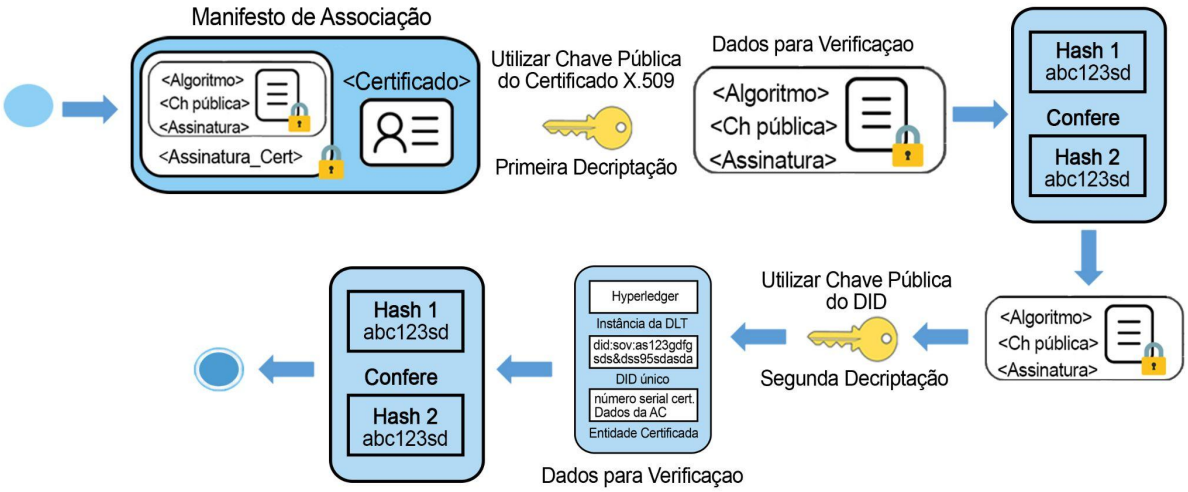

Figura 14. Fluxo de validação do Manifesto de Associação duplamente assinado.

Fonte: Própria.

5.3. Validação das Premissas Básicas

Conforme vimos nos fluxos apresentados anteriormente e tomando por base as premissas listadas na Seção 4.3, a saber: i) autocontida; ii) autoverificável; iii) descentralizada; iv) transparente; v) autossoberana; vi) voluntária e vii) opcional, é possível concluir que as premissas básicas são cumpridas.

Na Figura 15, pode-se verificar o bloco de controle que é adicionado ao Manifesto de Associação após ser duplamente assinado com as identidades digitais descentralizadas e centralizadas do titular. Com essas informações é possível checar o algoritmo utilizado na assinatura feita com o certificado digital, além do método de verificação do identificador descentralizado e o tipo do algoritmo adotado na assinatura. Assim, é possível analisar se o arquivo em questão está com assinaturas aderentes às normas do W3C de identificadores descentralizados e às normas da ICP-Brasil, além de verificar sua validade. Com esse conteúdo incluído no manifesto constatamos que ele é **autocontido.**


```
"verkey": "2LkqAdG9vWh9pJmbvVzBgpUQhLJnvcFFCJZsCfQyxnZq",
"dataCriacao": "2022-02-07T22:48:48.493164394",
"proof": {
    "proofPurpose": "assertionMethod",
    "verificationMethod": "3TfQL3J3hdgwvSoMijGtKg",
    "type": "Ed25519Signature2018",
    "created": "2022-02-08T01:49:05Z",
    "jws": "eyJhbGciOiAiRWREU0EiLCAiYjY0IjogZmFsc2UsICJjcml0IjogWyJiNjQiXX0..p2egvv0XaGZXsB0CS2me4avn13C6yRbgvrdtwY
},
"Assinatura": {
    "x509Certificate": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUgxekNDQmIrZ0F3SUJBZ0lJWStHN1BLeHJtbHN3RFFZSktvWkl
    "signatureValue": "s/FWdoVFlz6+9gQ5VpK6k1mDtE3lo9PSVO2xANzsaaogsCKwaRUAba8UbIJ+QsbeCe2zU4Mss8J2kpNqvoBvfPt9E3g4
    "digestValue": "57FF2D0A01890758E25124D3326CA1FCE61D3FE5",
    "x509SubjectName": "CN=AC ONLINE RFB v5, OU=Secretaria da Receita Federal do Brasil - RFB, O=ICP-Brasil, C=BR",
    "algoritmo": "SHA256withRSA"
}
```


Figura 15. Bloco de controle após ter sido duplamente assinado.

Fonte: Própria.

Observa-se ainda que os valores assinados por ambos os identificadores estão contidos no bloco. A primeira validação a ser realizada no processo de verificação do manifesto é com relação a prova de identidade, conforme pode ser visto na propriedade Assinatura da Figura 15. Percebe-se também o certificado digital utilizado para assinar este artefato, o valor do conteúdo assinado e o algoritmo adotado (SHA-256). O hash do conteúdo também aparece no bloco, para a verificação.

Na propriedade *proof*, encontra-se a prova de posse, que utiliza uma chave pública (propriedade *verkey*) para verificar os metadados. Aparece também o conteúdo assinado, do qual é possível pegar o conteúdo original e aplicar a função de hash para obter um novo resumo e compará-los. Desta forma, com todos os dados necessários à verificação presentes, pode-se concluir que o Manifesto de Associação é **autoverificável.**

O artefato também atende à premissa de **descentralização**, pois fica sob a posse do titular em sua carteira digital criada no processo de geração do DID e não em um servidor central. Logo, aumenta o controle e independência por parte do proprietário das identidades. Quando ele apresenta o manifesto, a verificação pode ocorrer tanto ao se conferir o

certificado digital, como também ao constatar a veracidade das provas associadas ao DID. Isso ocorre de forma transparente para o usuário, atendendo a premissa da **transparência**.

Quanto a ser **autossoberano**, após ampla pesquisa sobre o que define uma identidade autossoberana, consideramos válido e verificamos que é amplamente aceito o posicionamento de (ALLEN, 2016). Este expõe que a identidade autossoberana é o próximo passo além da identidade centrada no usuário e isso significa que ela começa neste ponto: o usuário deve estar no centro da administração da identidade.

Isso requer não apenas a interoperabilidade consentida da identidade de um usuário em vários locais, mas também o verdadeiro controle dessa identidade digital, criando autonomia do usuário. O Manifesto foi desenvolvido visando todo esse controle por parte do titular da identidade, buscando atender aos dez princípios da identidade autossoberana elencados na Seção 2.4 como necessários para garanti-lo.

Além disso, a criação da associação é decisão do usuário. Caso não deseje associar, pode utilizar o protótipo apenas para criação da carteira digital e da identidade descentralizada, podendo assinar documentos a serem validados nesses ambientes. Isto demonstra que a geração do Manifesto de Associação neste protótipo é **opcional e voluntária**.

6. EXPERIMENTOS

Neste Capítulo será descrito o protótipo LinkedID que implementa a associação de um DID a um eCPF/eCNPJ para verificar a viabilidade da prova de conceito proposta no Capítulo 5. Também serão discutidos alguns cenários experimentais que foram montados e executados para avaliar o comportamento da solução desenvolvida.

6.1. Construção do Protótipo

- **Objetivo e Escopo**

Para o desenvolvimento do protótipo e realização dos experimentos localmente, foi necessário integrá-lo com outras aplicações e tecnologias, como *Aries-Cloud-Agent Python*, *blockchain* da *Hyperledger Indy* e *Hyperledger Aries, PostgreSQL*, um *ledger browser*, entre outras, que auxiliaram na geração de DID e credenciais verificáveis. Como apresentado no Capítulo 5, foi utilizado, ainda, um certificado digital ICP-Brasil com o valor de *Subject Name*: *Anália Cristina Bezerra Tiburtino Meira:052.XXX.XXX-50*[15].

O principal objetivo em se construir um protótipo para a geração do Manifesto de Associação entre um DID e um e-CPF é possibilitar a verificação da exequibilidade da prova de conceito descrita no Capítulo 4. O escopo do projeto foi definido em termos das funcionalidades necessárias para cumprir o objetivo do projeto, ou seja utilizar compromissos criptográficos e tecnologias correlatas para o desenvolvimento de um manifesto auto verificável de associação entre identidades descentralizadas e centralizadas.

6.1.1. Especificação

[15] Por segurança, os caracteres "X" estão substituindo os números do CPF.

O protótipo desenvolvido será especificado nesta seção. Seus requisitos serão classificados em requisitos funcionais e requisitos não funcionais e descritos nos próximos itens.

- **Requisitos Funcionais**

Tabela 2: Tabela de Requisitos Funcionais

Código	Nome	Prioridade
RF01	Criação de *subwallets* para o armazenamento dos DID	Alta
RF02	Criação de um identificador descentralizado (DID)	Alta
RF03	Estabelecimento de conexões entre agentes	Alta
RF04	Criação do manifesto associação	Alta
RF05	Pesquisar manifesto de associação	Baixa
RF06	Validar manifesto de associação	Alta
RF07	Criação de credencial verificável do manifesto de associação.	Alta
RF08	Emitir apresentações verificáveis do manifesto	Média
RF09	Verificar provas da apresentação verificável	Alta

RF01

Prioridade: Alta

Funcionalidade inicial para que se realizem operações neste ambiente descentralizado, consiste na criação de uma *subwallet*, que são carteiras para os usuários, nas quais serão armazenados os DIDs e as credenciais verificáveis. Como forma de simular um dispositivo do usuário no qual seus dados seriam guardados e também possibilitar que outras medidas adicionais relacionadas à segurança e à disponibilidade possam ser adotadas, as carteiras dos usuários devem ser armazenadas em um banco de dados relacional neste protótipo.

RF02

Prioridade: Alta

O usuário deve ter a possibilidade de criar, caso não possua em sua carteira digital, um DID para interagir com a aplicação. No processo de obtenção de uma *subwallet*, adquire-se um token para gerar DID local com seu par de chaves. Em seguida, registra-se o DID na *ledger* selecionada para torná-lo público.

RF03

Prioridade: Alta

Para interagir com um agente na rede é necessário estabelecer uma conexão prévia, por exemplo, para emitir uma credencial verificável. As credenciais são emitidas por agentes emissores na rede, para que um detentor solicite uma credencial, deve estabelecer uma conexão com o emissor que pode ser um entre vários nós na rede, o nó participante aceita o convite e está estabelecida a conexão para esta ação específica.

RF04

Prioridade: Alta

Para a criação do manifesto associando o identificador descentralizado a um identificador centralizado pré-existente, não é necessário o RF03 (estabelecer conexão entre agentes). O titular das identidades, de forma voluntária, pode criar seu manifesto pela aplicação. Ao solicitar a associação, utiliza-se os pares de chaves públicas dos identificadores para a realização do compromisso criptográfico que irá gerar o manifesto.

RF05

Prioridade: Alta

Para realizar a pesquisa pelo manifesto deve-se informar alguns dados como entrada, como a carteira onde ele está armazenado para, então, obtê-lo como resposta.

RF06

Prioridade: Alta

Para validação do manifesto, realiza-se o processo inverso ao da criação e utiliza-se o conteúdo do próprio manifesto para certificação das assinaturas ali contidas.

RF07

Prioridade: Alta

Funcionalidade adicional para aprimorar o protótipo e que é totalmente condizente com o ambiente descentralizado. Para criação de credenciais verificáveis, deve-se indicar um contexto em uma estrutura de dados denominada *schema*, que indique o tipo de conteúdo a ser inserido na credencial. Além disso, alguns nós de confiança na rede descentralizada devem aderir a essa estrutura de dados, tornando-se emissores desta credencial. O titular então pode solicitar uma credencial verificável do manifesto, para posteriormente apresentar a um verificador que a solicite.

RF08

Prioridade: Alta

A credencial do titular fica disponível para que ele a apresente quando e a quem desejar. Para apresentar credencial verificável, inicialmente, deve-se estabelecer uma conexão entre os agentes envolvidos. Após o estabelecimento, ele poderá enviar a apresentação verificável.

RF09

Prioridade: Alta

A verificação das provas ocorre de forma autocontida. O verificador recebe a credencial apresentada e verifica a autenticidade de forma autônoma.

- **Requisitos Não Funcionais**

Tabela 3: Tabela de Requisitos Não Funcionais

Código	Nome	Prioridade
RNF01	Usabilidade	Média
RNF02	Tempo de resposta de 5 segundos para as operações básicas	Alta
RNF03	O software deverá apresentar mensagens claras e palavras simples.	Alta
RNF04	Interoperabilidade	Alta

RNF01

Prioridade: Média

A interface deve ser projetada de forma que utilizar o protótipo seja algo amigável, fácil e intuitivo. Deve possuir apenas informações necessárias de forma a cumprir o objetivo proposto deste trabalho. Por exemplo, poucos menus e itens a serem preenchidos para obtenção das funcionalidades.

RNF02

Prioridade: Alta

O sistema deve possuir baixo tempo de espera de resposta para as operações mais básicas. No caso das operações mais complexas, o tempo de resposta não será limitado devido à complexidade computacional esperada como as que envolvem interação com a *ledger* e as chamadas API REST.

RNF03

Prioridade: Alta

O sistema deve possuir mensagens claras e com uso de vocabulário simples, pois o objetivo da aplicação é ser utilizada por qualquer usuário que decida ter o controle dos seus dados. Não é objetivo deste projeto exibir diversas mensagens, mas apenas as necessárias para conduzir/informar o usuário sobre o fluxo das operações.

RNF04

Prioridade: Alta

A criação de serviços (REST) para serem consumidos por outras aplicações permite a interoperabilidade. Possibilita o uso do protótipo, por exemplo, por outra identidade centralizada ou por outro registro descentralizado (*blockchain*).

6.2. Detalhes de Implementação

Esta solução foi desenvolvida para fornecer três serviços principais: um de criação de DID, outro de registro de manifesto - ambos utilizados de maneira voluntária por uma entidade que seja titular de uma carteira e de um certificado digital para registrar a associação entre essas identidades - e um terceiro serviço de consulta que, de forma geral, recebe parâmetros de entrada como um identificador de um endereço de carteira e retorna ao usuário o manifesto associado.

Para implementar as funcionalidades elencadas, foi feito um levantamento das tecnologias existentes que poderiam ser aplicadas de forma colaborativa com o desenvolvimento do protótipo. Elaborou-se um ambiente que inclui uma aplicação cliente na qual se cria, controla e gerencia DID, o manifesto de associação e credenciais verificáveis que porventura venham a ser geradas. Utilizou-se também uma interface para interagir com o componente responsável por criar automaticamente agentes em uma instância de servidor, orquestrar os eventos que ocorrem com o agente monitorado, para fazer os registros em uma rede descentralizada, entre outras tarefas.

Para a prova de conceito, esta versão foi desenvolvida adotando instâncias de *DLT Hyperledger*. A escolha por utilizar uma *blockchain* como registro descentralizado se deve ao fato de ser uma tecnologia de livro-razão com registros imutáveis, descentralizada, mantido em uma rede distribuída por múltiplos nós pares. Além disso, suas demais características são compatíveis com as premissas preconizadas neste trabalho e desejáveis em um sistema de gerenciamento de identidades descentralizadas.

Já a escolha pela *Hyperledger* ocorreu por ser uma *blockchain* permissionada, onde, diferente de uma rede pública, os participantes são conhecidos em vez de anônimos. Embora não confiem plenamente uns nos outros, uma rede pode ser operada sob um modelo de governança baseada na confiança existente entre os participantes, como um contrato ou modelo para reger divergências. Este modelo foi considerado ideal para o projeto que inicia com o intuito de possibilitar uma transição entre ambientes centralizados e descentralizados. Como nos ambientes centralizados a maioria dos aplicativos corporativos dependem de

relações de confiança nesta *blockchain*, operar sob um modelo de governança que promove um certo grau de confiança pode proporcionar essa segurança.

Outros fatores que foram levados em consideração nesta escolha pela *Hyperledger* foram sua finalidade, a maturidade, a adesão a padrões interoperáveis, configuração que garante que os limites são flexíveis o suficiente para trazer mais participantes no futuro e por não ter a necessidade de executar mecanismos de prova de trabalho. Estes são mecanismos mais demorados no processamento das transações e podem resolver problemas mais imediatos do que em uma *blockchain* pública de criptomoeda.

Para simular este ambiente que inclui uma rede digital confiável de dados verificáveis, que seja globalmente conectada, interoperável e segura, foi utilizado o projeto da *blockchain* do Governo da Colúmbia Britânica - *VON Network*, que é uma Rede de Organizações Verificáveis, com código *open source* e disponibilizado no GitHub. É construída sobre a base da tecnologia *blockchain* e, mais especificamente, focada nas bases criptográficas de identificadores descentralizados (DID) e credenciais verificáveis (VCs).

Como foi preciso criar DID para em seguida proceder à geração do manifesto, optou-se por utilizar dois arcabouços: *Hyperledger Indy*[16] (HLI) e *Hyperledger Aries*[17] (HLA), ambos oferecidos pelo *Hyperledger Greenhouse*[18], um consórcio de código aberto hospedado pela *Linux Foundation,* para o desenvolvimento de tecnologias em *blockchain*. O HLI [Bhattacharya et al. 2020] fornece ferramentas, bibliotecas e componentes reutilizáveis para criar e usar identidades descentralizadas que sejam interoperáveis entre domínios administrativos, aplicativos e redes organizacionais distintas. O HLA é uma infraestrutura para interações entre pares confiáveis e troca de mensagens, servindo como um cliente da *blockchain* e utilizado em ambientes de emissão de credenciais verificáveis.

A aplicação atua como controlador de negócios, ou seja, é cliente da API fornecida pelos agentes no *Hyperledger Aries-Cloud-Agent Python (aca-py)*. O cliente realiza chamadas ao componente *Aries Cloud Agent* (enviando requisições HTTP e recebendo notificações via *webhook*), que faz chamadas à DLT para registrar ou buscar informações importantes no processamento das transações. No final, o agente de borda responde por eventos ao controlador de negócios.

[16] https://www.hyperledger.org/use/hyperledger-indy
[17] hyperledger.org/use/arie
[18] https://www.hyperledger.org/

Neste trabalho, está implementado a multilocação (*multitenancy*), que é a capacidade de a aplicação suportar a execução de uma instância (escalonável) de software para atender a vários grupos de usuários diferentes. Ou seja, ao adotar este conceito para o registro de DID, pode-se operar vários agentes de vários proprietários utilizando apenas uma *wallet* (carteira), que comporta o conceito de *subwallets* para representar cada proprietário. Através da Figura 16, verifica-se a funcionalidade *multitenancy* habilitada no aca-py. Há um único agente em execução, porém, os recursos passam a ser compartilhados entre os inquilinos do agente em suas *subwallets*. Portanto, uma carteira própria para cada proprietário, que armazenará seus próprios DIDs, suas conexões e credenciais.

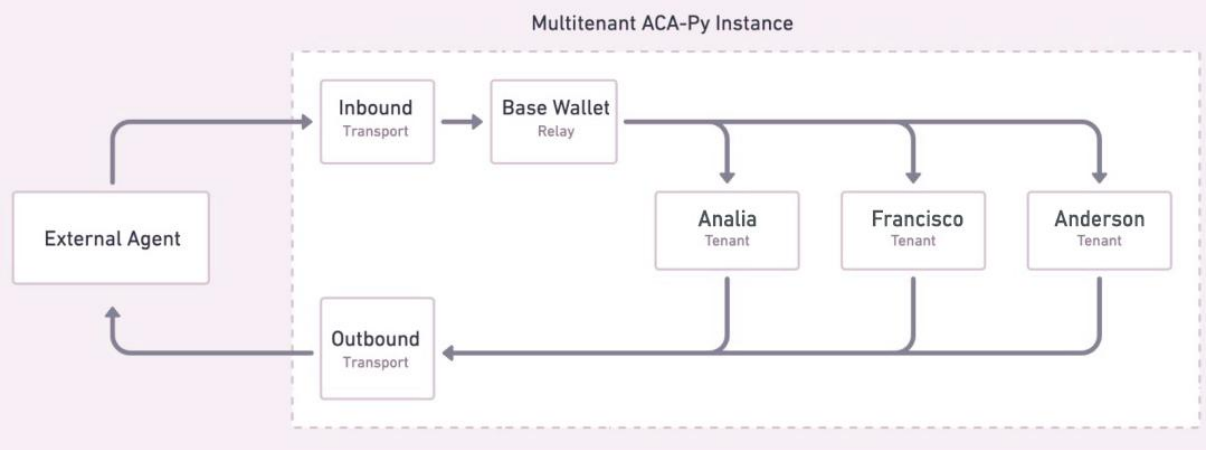

Figura 16. Instâncias *multitenant* do ACA-Py versão 0.7.2. Fonte: Própria.

As *subwallets* usam o mesmo terminal, porém, em uma visão externa ao sistema, não é nítido que os vários proprietários estão usando o mesmo agente. Já a carteira de base (*wallet*) tem como funções gerenciar as *subwallets*, armazenar as configurações e informações de cada uma. Além de encaminhar as respectivas mensagens recebidas para as *subwallets* correspondentes. Os demais recursos estão desabilitados para a carteira, assim ela não pode emitir credenciais, apresentar provas ou realizar quaisquer outras ações que as *subwallets* podem realizar, mantendo uma diferença hierárquica clara entre elas.

Como dito no Capítulo 4, é pré-requisito para o Manifesto de associação possuir um identificador descentralizado e um centralizado válido. Para a funcionalidade de criar um DID, deve-se seguir as etapas descritas abaixo:

1. O usuário solicita a criação de uma carteira (*subwallet* no conceito de *multitenant*) através de uma chamada REST;
2. Obtém um token como resposta com o qual é possível gerar um DID Local;

3. Em seguida, fornece o DID e o *Verkey* (chave pública do DID) para registrá-lo na *ledger*, transformando-o em público.
4. Atribui-se o DID público à *subwallet* do proprietário.

De posse do seu DID, o usuário pode estabelecer conexão com outras entidades/ organizações, solicitar credenciais e enviar provas de seus dados para terceiros. O macroprocesso para emissão de um DID pode ser verificado na Figura 17.

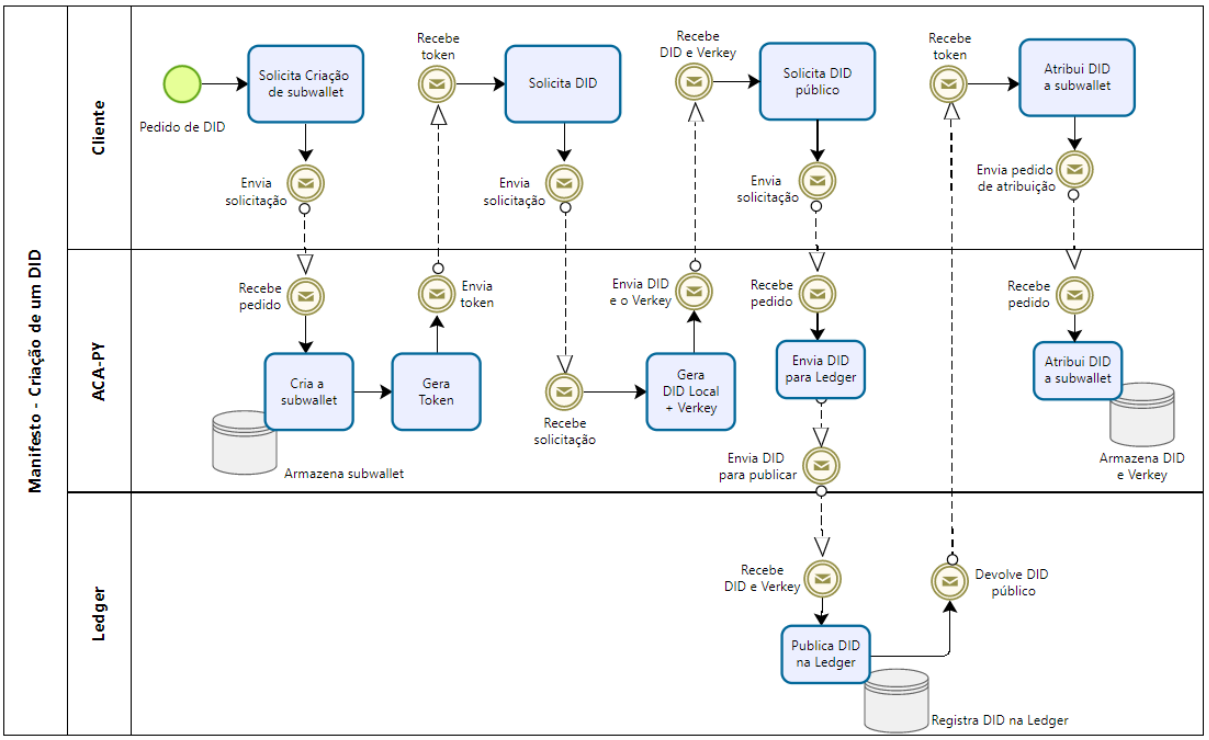

Figura 17. Macroprocesso demonstrando o fluxo da criação do DID. Fonte: Própria.

Ao integrar a aplicação com o aca-py, pode-se verificar o DID criado e publicado na ledger através do endpoint /wallet/did/public, conforme Figura 18.

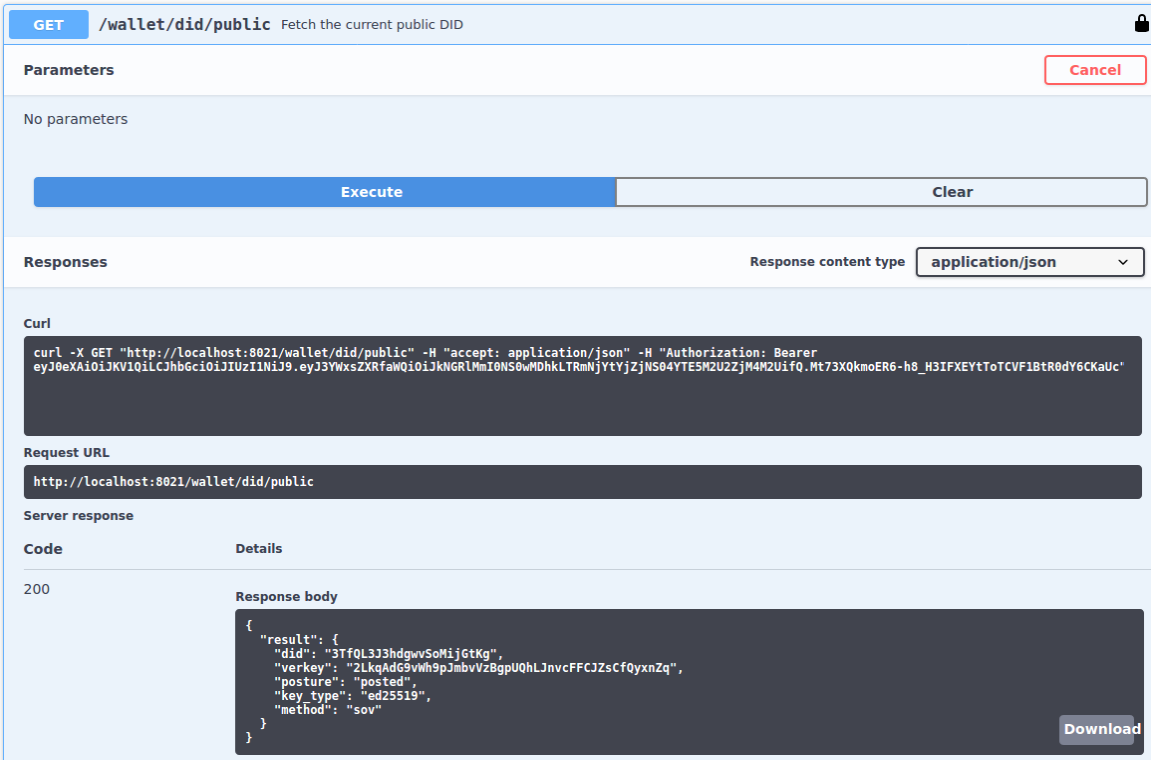

Figura 18. Interface para interação com o identificador descentralizado gerado.

Fonte: *Printscreen* do *endpoint /wallet/did/public* do *aca-py*.

O registro do DID no *ledger* escolhido pode ser feito de duas formas: i) através do sistema do Manifesto e ii) através da interface do *ledger browser*, informando um alias (opcional), o DID local e o *verkey* obtido nos passos anteriores, conforme a Figura 20. A transação é adicionada a um bloco e em seguida adicionada à cadeia de blocos, tornando-o um DID público.

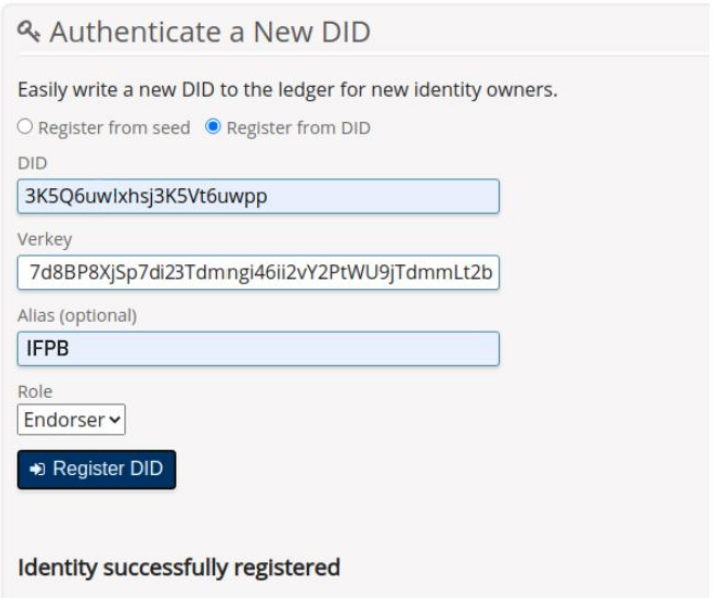

Figura 20. Interface do *Ledger Browser*. Fonte: Própria.

Após obter o DID, segue-se, opcionalmente, para o fluxo de emissão do manifesto. Através do caso de uso Criação do manifesto associação, a entidade deverá informar a instância de DLT na qual o DID foi criado, o DID público, chave privada do certificado digital e seu respectivo certificado, conforme pode ser visualizado na interface mostrada na Figura 19. Ao clicar no botão solicitar, as rotinas implementadas irão produzir as assinaturas digitais, gerar o artefato do manifesto de associação e realizar uma chamada para o registro do manifesto. Através de uma API REST, o manifesto será conduzido em alguns passos para realizar o registro de associação, como também será conduzido para o armazenamento em uma camada de repositório.

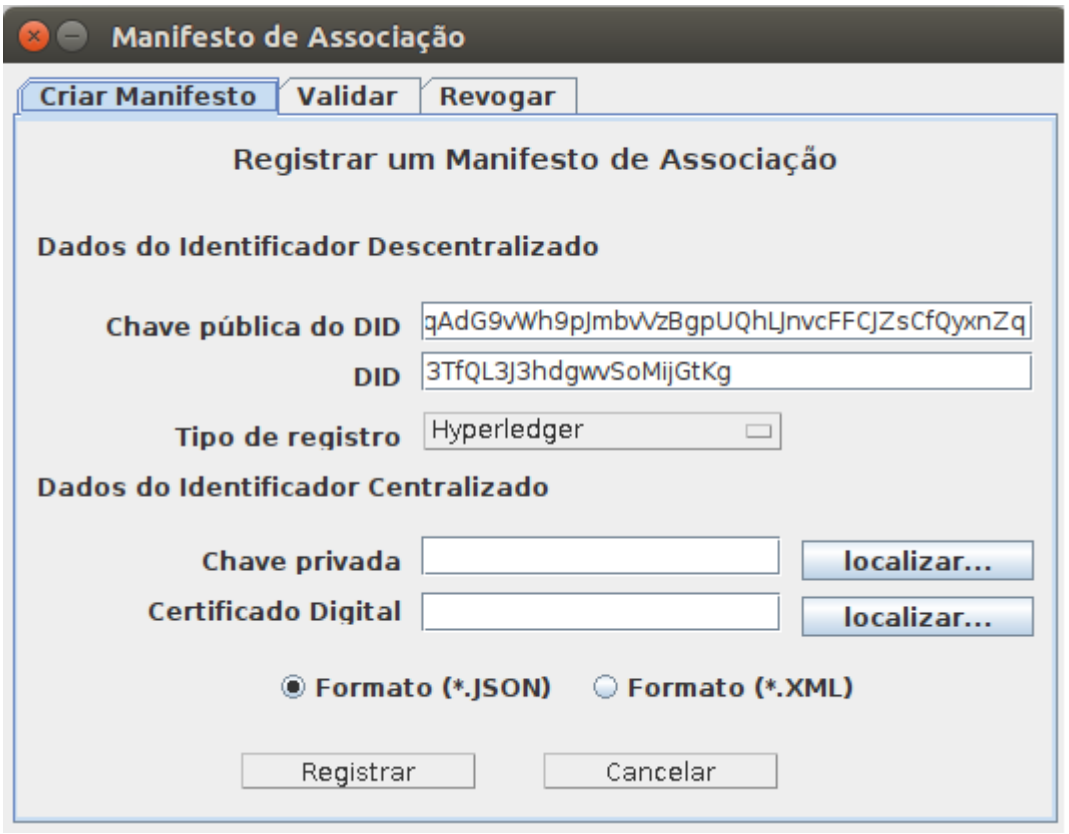

Figura 19. Interface de registro do Manifesto de Associação.

Fonte: Própria.

Como pode ser observado na Figura 19, o manifesto pode ser gerado em dois formatos a escolha da pessoa/entidade: JSON ou XML, pois verificou-se que ele pode ser construído tanto utilizando tecnologia ***JSON Web Signature*** **(JWS)** quanto ***XML Signature***. O padrão ***XML DSig*** realiza assinatura digital de um documento XML e permite verificar se os dados não foram alterados após sua assinatura. O **JWS**[19] é uma especificação para assinatura de

[19] JWS - padrão proposto e especificado pela Internet Engineering Task Force (IETF) através da RFC 7515.

estrutura de dados JSON, que oferece recursos como assinar e verificar um *JSON Web Token* (JWT) e *JSON Web Signature* (JWS) com suporte a vários algoritmos, podendo ser utilizado com chave simétrica, chave assimétrica e também com certificado X.509.

Após informar o certificado digital e sua respectiva chave privada, é iniciada a geração do manifesto de associação que foi desenvolvido utilizando a tecnologia Java 8 como linguagem de programação, bastante robusta quando se trata de linguagem com suporte a vários padrões de assinaturas digitais. Nesta prova de conceito, para a assinatura digital da prova de identidade, utilizou-se o algoritmo RSA com SHA-256 como função de hash. Para a assinatura digital da prova de posse, foi utilizado JWS com algoritmo de curva elíptica Ed25519. Logo, quando o usuário clica em registrar passando as identidades, gera o manifesto duplamente assinado, ficando sob a posse do titular que decidirá quando e com quem compartilhar.

Ainda sobre os detalhes da implementação, vale destacar que arquitetura de código seguiu o padrão Model-View-Controller (MVC), cujo objetivo é separar o projeto em três camadas independentes, que são o modelo, a visão e o controlador. Essa separação em camadas ajuda na redução de acoplamento, promove o aumento de coesão nas classes do projeto, facilita a manutenção do código e a reutilização em outros projetos. Através da camada de visão foi disponibilizada uma interface para que o detentor das identidades pudesse criar identificador descentralizado, solicitar a associação com seu certificado digital e consultar seu DID mapeado entre outras operações. Essa interface solicita requisições para uma classe que atua como a camada *controller*, através de outra classe expondo uma API RESTful que atende às requisições. Esta camada do controlador quem conhece o responsável por executar certas funcionalidades.

6.3. Avaliação

Buscando observar os resultados dos testes para validar o protótipo, conforme previsto no objetivo específico descrito no item 6 da Seção 1.2, foram feitas algumas validações, descritas a seguir.

6.3.1. Resultados

Para comprovar a validade do manifesto de associação gerado, utilizamos o verificador de conformidade do Instituto Nacional de Tecnologia da Informação (ITI), que é uma autarquia federal vinculada à Casa Civil da Presidência da República e responsável pelas políticas da ICP-Brasil. O ITI disponibiliza um verificador de conformidade de assinatura digital para validar documentos assinados em padrões como CAdES, XAdES e PAdES. Como o ITI não disponibiliza um serviço para ser consumido a partir de uma aplicação por padrões de consumos como o REST ou SOAP, a validação do manifesto de associação foi feita enviando uma requisição HTTP para o verificador do ITI e realizamos o tratamento da resposta obtida. Para melhor ilustração do resultado obtido, exibimos na Figura 21 a resposta da interface do verificador de conformidade.

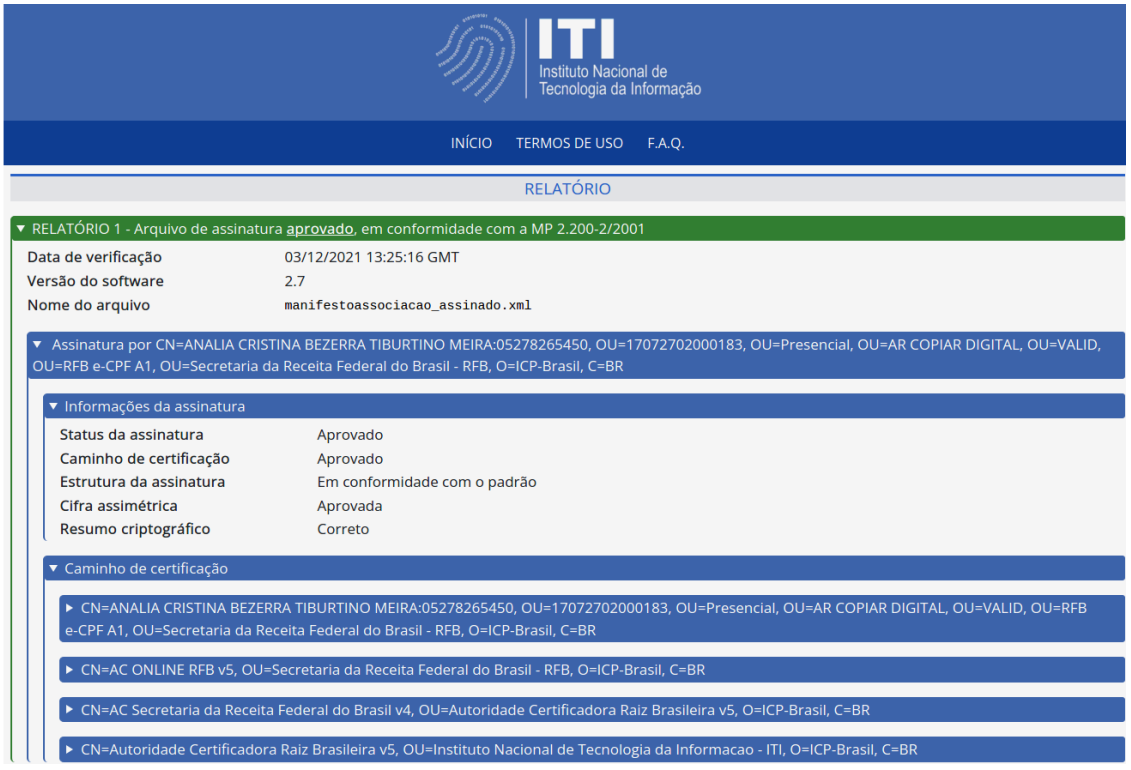

Figura 21. Interface do Verificador de Conformidade de assinaturas digitais do ICP-Brasil.
Fonte: *Printscreen* do Verificador do ITI.

Conforme observado na Figura 21, verifica-se que o documento assinado e submetido foi aprovado pelo ITI. Esta validação também está sendo realizada e verificada através do protótipo, conforme Figura 22. Para a implementação desta funcionalidade foi seguido o protocolo de verificação descrito na Seção 4.1.

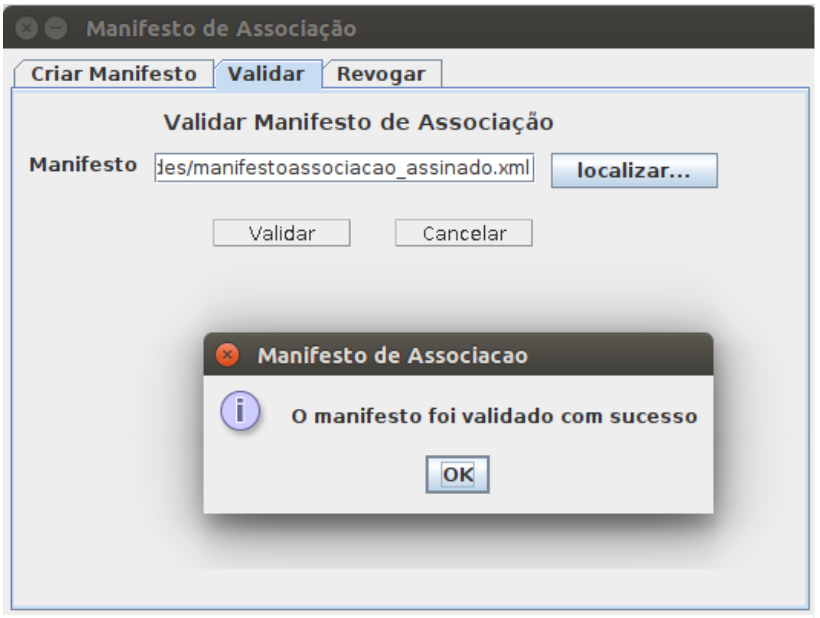

Figura 22. Validador do protótipo que realiza a verificação de conformidade de assinaturas digitais do ICP-Brasil. Fonte: Própria.

A **Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEdu)**[20] é o serviço de certificação digital oferecido pela **Rede Nacional de Ensino e Pesquisa (RNP)** que provê infraestrutura para a emissão de certificados digitais e chaves de segurança que viabiliza a emissão de certificados digitais do tipo SSL (Secure Sockets Layer), denominado eduID. Os certificados são instalados nos servidores web das instituições clientes da RNP, implementando a comunicação criptografada, aumentando a segurança no acesso e a credibilidade em relação à instituição. Ele é válido em todo sistema acadêmico e de pesquisa brasileiro, e pode ser usado por alunos, professores e servidores com acesso à Comunidade Acadêmica Federada (CAFe).

Buscando verificar a interoperabilidade do manifesto desenvolvido com outro certificado digital centralizado, foi emitido um certificado ICPEdu e gerado um manifesto integrando/associando o DID ao eduID. Na Figura 23, pode ser vista no Bloco de Controle, a assinatura realizada com o eduID.

[20] ICPEdu - https://pessoal.icpedu.rnp.br

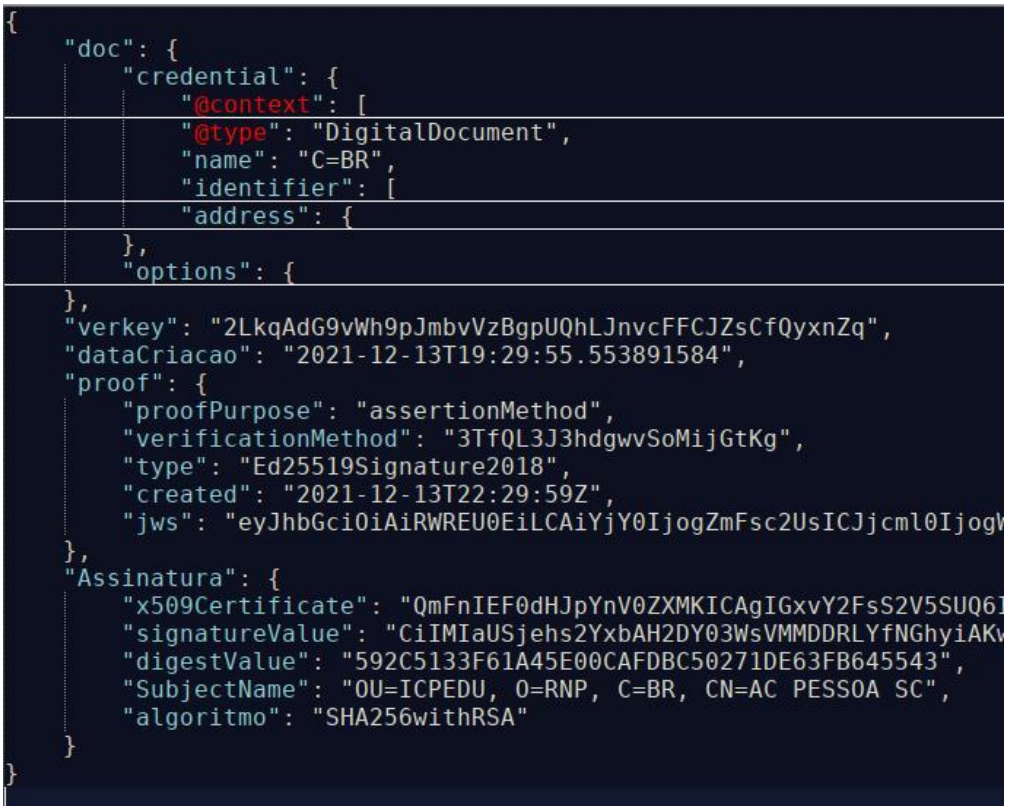

Figura 23. Bloco de controle do Manifesto de Associação assinado com o DID e o eduID.

Fonte: Própria.

6.3.2. Análise e Discussão

Esta seção apresentou os testes realizados com a implementação da prova de conceito e a validação do manifesto gerado através de sua integração com aplicações reais. O consumo de uma API REST é uma operação comum no âmbito de sistemas distribuídos. Este procedimento foi adotado em nossa integração para possibilitar o consumo de serviços cujo desenvolvimento não estava no escopo deste trabalho. Esta operação pôde ser implementada sem maiores dificuldades, mesmo envolvendo diferentes linguagens de programação.

A associação das chaves do certificado digital e assinaturas de chaves ED25519, além de proporcionarem maior segurança, também vincularam de forma confiável as identidades de um titular. Outrossim, as premissas voluntária e auto-verificável do manifesto permitiram a coexistência de publicidade e privacidade dos itens associados em uma mesma carteira.

Outro ponto desenvolvido foi a possibilidade de gerar o manifesto em dois formatos, JSON e XML, o que possibilita atender um nicho de mercado mais amplo e manter a compatibilidade com diversas especificações, sobretudo as adotadas nesta implementação.

Além disso, o protótipo foi desenvolvido prevendo o suporte a novas implementações de registros descentralizados, como outras *blockchains*, além da *Hyperledger* adotada e validada nestes experimentos. A decisão sobre quais padrões e *blockchains* deveriam ser adotados fez parte de um levantamento realizado referente às estratégias aplicáveis a esta solução.

7. CONCLUSÃO

Este capítulo apresenta as considerações finais sobre este trabalho, assim como apresenta algumas limitações que foram encontradas durante a pesquisa. Por fim, serão apresentadas sugestões de trabalhos futuros.

7.1. Considerações finais

Esta pesquisa fornece uma compreensão dos benefícios, desafios e oportunidades dos sistemas de identidades descentralizadas, baseadas ou não em DLT. Discute os componentes desses tipos de sistemas e identifica os padrões emergentes e suas propriedades, bem como os esforços atuais de especificações para sistemas de identidades descentralizadas.

A pesquisa incluiu a investigação de uma forma verificável de estabelecer a associação entre identificadores descentralizados e entidades do mundo real (pessoas físicas ou pessoas jurídicas). A implementação de uma prova de conceito do mecanismo de associação proposto possibilita a integração entre a tradicional abordagem de identidade digital centralizada, para fortalecer, quando necessário, a legitimidade de uma identidade descentralizada.

Através da implementação do protótipo e dos testes realizados pode-se verificar que é possível validar um manifesto de associação de forma autocontida, bem como verificou-se que, por estar associado a uma identidade centralizada, o manifesto obteve de forma natural validade jurídica.

Esta dissertação foi estruturada de forma que a leitura fosse conduzida proporcionando um entendimento acerca do tema e também sobre a problemática apresentada. Observou-se que este projeto possui relação com muitas áreas de pesquisa, como DLT, identidade digital, credenciais verificáveis e segurança da informação. Dependendo da perspectiva escolhida, cada uma dessas áreas poderia gerar outras narrativas para a problemática.

Durante o início da etapa de desenvolvimento da prova de conceito desta pesquisa, surgiu a oportunidade de submetê-la a seleção de um projeto de pesquisa da Rede Nacional de Ensino e Pesquisa (RNP) com a qual foi firmada uma parceria. Neste momento da implementação, algumas dificuldades foram encontradas devido à dinâmica evolução das tecnologias de livro razão distribuído. Destacaram-se as modificações nas versões dos softwares que foram integrados ao protótipo para proporcionarem serviços que fugiam ao escopo desta pesquisa, como também a necessidade de incorporar várias dependências e bibliotecas.

Outra dificuldade, encontrada na etapa de testes, foi com relação a obtenção de certificado digital gratuito para tentar realizar a prova de conceito com outra identidade centralizada além do certificado digital proposto (ICP-Brasil).

Ao levantar instâncias da *blockchain Hyperledger* no *google cloud* também tivemos alguns entraves, como o bloqueio por parte do serviço de nuvem fornecido, pois por várias vezes o seu uso foi classificado como suspeito, sendo identificado como tentativa de mineração de criptomoedas. No entanto, após retratações, as instâncias voltavam a ser liberadas. Contudo estes bloqueios atrapalhavam a evolução natural do desenvolvimento e por isso optou-se por levantar uma *blockchain* localmente.

Apesar destas dificuldades, foi possível concluir o desenvolvimento em tempo hábil. Visando avaliar a proposta, foram realizados experimentos de integração do protótipo com aplicações reais, através das quais pode-se demonstrar ser uma solução viável e que atinge a finalidade para a qual se dispõe.

Foi dado início ao processo de registro de software no INPI; cujo código-fonte foi disponibilizado no repositório GitHub[21].

7.2. Trabalhos futuros

Mesmo alcançando o objetivo desta pesquisa, tanto em termos do levantamento do estado da arte, como em termos de desenvolvimento da prova de conceito, alguns fatores importantes foram observados e podem ser verificados em um segundo momento. Estes pontos serão levantados nesta seção.

- Revogação do Manifesto de Associação

  Foram implementadas a criação do manifesto de associação e sua validação, porém o requisito de revogação deste manifesto é outra funcionalidade que merece ser discutida em trabalhos futuros relacionados a esta pesquisa, para o caso de o titular dos dados perder a chave privada associada à identidade descentralizada. Para solucionar cenários relacionados ao comprometimento do acesso, deve-se pensar em um modo de realizar a revogação do artefato criado.

- Análise da Lei Geral de Proteção de Dados (LGPD)

  Outro fator crucial é a questão da privacidade e a experiência do usuário, pois nesse modelo os titulares herdarão novas responsabilidades, como a necessidade de gerenciar não só suas chaves privadas, mas também seu Manifesto de Associação. Neste sentido relacionado à privacidade, cabe ainda realizar uma análise sobre a LGPD para regulamentar o tratamento de dados, quanto a sua utilização,

[21] https://github.com/Analia-meira/mapeamento-identidades

processamento, armazenamento e exclusão, buscando garantir que o *LinkedID* esteja em conformidade com esta lei.

Como se trata de um protótipo que utiliza uma *blockchain* como tecnologia de registro distribuído, deve-se buscar uma análise segura e minuciosa desse tratamento de dados pessoais, tais como o direito ao esquecimento (exclusão dos dados pessoais de uma base) e o direito à retificação (alteração dos dados pessoais) que esbarram em umas das propriedades da base de uma *blockchain*: a imutabilidade.

- Mensageria de Eventos

  Uma outra linha de continuidade deste trabalho é com relação a implementação de um mecanismo para mensageria de eventos que ocorrem entre os agentes para o uso das funcionalidades ofertadas pela adoção do *webhook*. Por exemplo, desenvolver um componente responsável por monitorar um agente e propagar por meio de um barramento de mensageria todos os eventos relevantes que ocorram com esse agente monitorado, desde solicitações de conexões à emissão de credencial ou a solicitação para apresentação de uma credencial verificável.

- Credenciais Verificáveis

  Durante a implementação do protótipo, principalmente no desenvolvimento do caso de uso de emissão do manifesto de associação, foram desenvolvidas algumas funcionalidades para possibilitar a emissão de credenciais verificáveis, como um plus ao *LinkedID*. Por exemplo, foram implementadas as classes para **estabelecer conexões** entre os agentes envolvidos. Através dessa funcionalidade, um detentor de um DID pode estabelecer uma conexão com um emissor de credenciais verificáveis para solicitar uma credencial. Após ter uma conexão estabelecida, o emissor pode emitir uma credencial e enviar para ser armazenada na *subwallet* do detentor.

  Foi implementada a funcionalidade para **solicitar credencial**, através da qual o titular solicita uma credencial a um emissor de um *schema* público específico de credencial; e **emitir credencial**, que emite uma credencial para um titular de um *schema* existente. Porém, não fazia parte do escopo deste trabalho a criação de um *schema* público para emissão de Manifesto de Associação. Devido à proximidade conceitual das especificações aqui levantadas (DID e credenciais verificáveis), sugere-se que seja realizado um estudo sobre a publicação de um esquema deste tipo.

  Também seria complementar a este trabalho pesquisar e implementar o **Consentimento de credencial**, criando uma funcionalidade que exibe os atributos de um *schema* e permite ao titular informar quais destes serão compartilhados com um terceiro. São muitos os dados pessoais relacionados a uma identidade. No entanto, sua exibição por completo, quando precisa validar uma informação, não se faz necessário e atenta contra a segurança da informação e o direito à privacidade. Por esta razão,

indica-se fortemente o desenvolvimento de uma funcionalidade destas para sistemas de identidades digitais.

REFERÊNCIAS BIBLIOGRÁFICAS

ALLEN, Christopher. *The Path to Self-Sovereign Identity.* 2016. Disponível em: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html. Acesso em: 20 nov 2019.

AMADO, Aécio. 2020. *Estratégia de Governo Digital 2020-2022*. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2020-04/publicado-decreto-que-lanca-estrategia-de-governo-digital-2020-2022. Acesso 30 abr 2020.

AMARAL, J. N., Buro, M., Elio, R., Hoover, J., Nikolaidis, I., Salavatipour, M., Stewart, L., & Ken Wong, K. 2011. *About Computing Science Research Methodology*.

BASHIR, I. 2017. *Mastering Blockchain: Distributed ledgers technology, decentralization and smart contracts explained*. 2ª edição. Packt Publishing.

BHATTACHARYA, M. P., Zavarsky, P., and Butakov, S. (2020). *Enhancing the security and pri-vacy of self-sovereign identities on hyperledger indy blockchain.* In2020 *International Symposium on Networks, Computers and Communications* (ISNCC), *pages* 1–7.

BENET, J. 2014. *IPFS - content addressed, versioned, P2P file system*. CoRR, abs/1407.3561.

BERNARDI, E. F. F. et al. 2017. *A implementação do blockchain Hyperledger Fabric em ambiente linux utilizando containers docker*. Passo Fundo - RS.

BUHR, R.J.A. 1998. *Use case maps as architectural entities for complex systems*, IEEE Transactions on Software Engineering. Vol 24, Issue 12, Dec 1998, pp. 1131–1155.

CAMERON, K. 2005. *The laws of identity*. Disponível em: https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf Acesso em: 20 nov 2019.

CAO, Y.; YANG, L. A Survey of Identity Management Technology.International Conferenceof Information Theory and Information Security (ICITIS), IEEE, 2010

COULOURIS, G. 2009. *Distributed Systems: Concepts and Design*, 4/e. [S.l.]: Pearson Education, 2009. ISBN 9788131718407.

CLAUß, S. and Köhntopp, M. 2001. *Identity Management and Its Support of Multilateral* Security.Comput. Netw., 37:205–219.

CPQD. 2021. *"Relatório Anual 2020"*. Disponível em: https://www.cpqd.com.br/wp-content/uploads/2021/06/Relatorio_Anual_2020_CPQD.pdf Acesso em: 10 mar 2021.

CRYPTOID. 2020. *Como outros países implementaram a Identidade Digital.* Disponível em: https://cryptoid.com.br/certisign/como-outros-paises-implementaram-a-identidade-digital/ Acesso em: 28 maio 2020.

GEORGE, Nathan. 2020. *Announcing Hyperledger Aries, infrastructure supporting interoperable identity solutions*. Disponível em: https://www.hyperledger.org/blog/2019/05/14/announcing-hyperledger-aries-infrastructure-supporting-interoperable-identity-solutions Acesso em: 10 jul 2020.

DUNPHY, P., Petitcolas, F. A. "*A first look at identity management schemes on the blockchain". IEEE Security & Privacy*, 16(4), p20-29, 2018.

GUEDES, Aline. 2018. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/538714/Cidadania622.pdf?sequence=1&isAllowed=y Acesso em: 10 abr 2019.

ITU-T, 2009. Disponível em: file:///C:/Users/Analia/AppData/Local/Temp/T-REC-Y.2720-200901-I!!PDF-E.pdf Acesso em 13 nov 2019.

LEMOS, R. 2020. *Caos em bases de dados de cidadãos cobra seu preço na pandemia de coronavírus*. [S.l.]: Folha de São Paulo, 2020. Disponível em: https://www1.folha.uol.com.br/autores/ronaldo-lemos.shtml Acesso em: 03 abr 2020. Citado na página 11.

LUX, Zoltán A.; Thatmann, Dirk; Zickau, Sebastian; Beierle, Felix. 2020. *Distributed-Ledger-based Authentication with Decentralized Identifiers and Verifiable Credentials*. Disponível em: https://arxiv.org/pdf/2006.04754.pdf. Acesso em: 17 Jul 2020.

MATSUURA, Sérgio. 2020. *Inspiração para o Brasil? Com identidade digital, Índia superou o desafio de cadastrar população de mais de 1 bilhão*. Disponível em: https://oglobo.globo.com/economia/inspiracao-para-brasil-com-identidade-digital-india-superou-desafio-de-cadastrar-populacao-de-mais-de-1-bilhao-2-24457804 Acesso em: 14 jun 2020.

MOTA, Renato. 2020. *Quais documentos oficiais possuem versões digitais e como usá-los*. Disponível em: https://olhardigital.com.br/dicas_e_tutoriais/noticia/quais-documentos-oficiais-possuem-versoes-digitais-e-como-usa-los/105238 Acesso em: 20 ago 2020.

Narayanan A, et al. (2016) The interactome of CCT complex - A computational analysis. Comput Biol Chem 64:396-402

NAKAMOTO, Satoshi. 2008. "*Bitcoin: A Peer-to-Peer Electronic Cash System*". Disponível em: https://bitcoin.org/bitcoin.pdf Acesso em: 20 abr 2019.

PIRES, A.; Militão, J. Integração Contínua com Jenkins. In: . Novatec. 2019. v. 1. ISBN 978-85-7522-722-0. Disponível em: https://novatec.com.br/livros/jenkins. Citado na página 32. Acesso em: 10 jan 2020.

PREUKSCHAT, A., Reed, D. 2021. *Self-Sovereign Identity.* [S.l.]: Manning - Edição Kindle.

REED, Drummond. Allen, Christopher. Sabadello, M. et al. 2020. *Decentralized Identifiers (DID) v1.0. Core architecture, data model, and representations*. Disponível em: https://w3c-ccg.github.io/did-core/ Acesso em: 28 ago 2020

El Haddouti, Samia; Kettani, M.. (2019). Analysis of Identity Management Systems Using Blockchain Technology. 1-7. 10.1109/COMMNET.2019.8742375

MANCINI, Claudia. 2020. "*Serpro desenvolve ID autossoberana e cria solução que chama atenção de comunidade internacional*". Disponível em: https://www.blocknews.com.br/governos/serpro-desenvolve-id-soberana-e-cria-solucao-que-chama-atencao-de-comunidade-internacional/ Acesso em: 02 Fev 2021.

SABADELLO, Markus. ZAGIDULIN, Dmitri. 2021. "*Decentralized Identifier Resolution (DID Resolution) v0.2*" Disponível em: https://w3c-ccg.github.io/did-resolution Acesso em: 20 abr 2021.

SONNINO, A. Al-Bassam M., Bano S., Meiklejohn S., and Danezis G.Coconut. 2018: "*Threshold issuance selective disclosure credentials with applications to distributed ledgers*". arXiv preprint arXiv:1802.07344, 2018.

SPORNY, Manu, LONGLEY, D. Chadwick D. 2020. *Verifiable Credentials Data Model 1.0. Expressing verifiable information on the Web*. Disponível em: https://w3c.github.io/vc-data-model/ Acesso em: 20 jun 2020.

TERBU, O. BASART I., et al. 2020. *"Self-Issued OpenID Connect Provider DID Profile."* Disponível em https://identity.foundation/did-siop/ Acesso em: 19 Jul 2020.

WANGHAM, M.; MELLO, E. R. 2010. "*Gerenciamento de Identidades Federadas."* Disponível em: https://www.researchgate.net/publication/228401861_Gerenciamento_de_Identidades_Federadas. Citado na página 11. Acesso em: 20 jan 2020.