PROJETO ILIADA

META A5.1 - Prospecção tecnológica, padronização e aspectos legais em identidade digital descentralizada

Relatório da Meta Física 5:
Pesquisa e Desenvolvimento em Identidade Digital Descentralizada

Relatório do Processo de Seleção dos Projetos

Blockchain em evolução.

Dezembro de 2024

PROJETO ILÍADA
FASE 2

PROJETO ILIADA · CPQD · RNP · MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO · GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

SUMÁRIO

1 Introdução

As Identidades Digitais Descentralizadas (IDD) representam uma evolução significativa na forma como gerenciamos e verificamos identidades no ambiente digital. Tradicionalmente, as identidades digitais são controladas por entidades centralizadas, como governos, instituições financeiras, e grandes empresas de tecnologia. Este modelo centralizado apresenta várias desvantagens, incluindo riscos elevados de violação de dados, falta de privacidade e controle limitado pelos próprios usuários.

As IDDs, por outro lado, colocam o controle das identidades digitais nas mãos dos indivíduos. Utilizando tecnologias como blockchain e criptografia avançada, é possível garantir que os usuários possuam e gerenciem suas próprias identidades digitais, sem depender de intermediários centralizados. Isso proporciona um nível maior de segurança, privacidade e autonomia.

As IDDs têm aplicações potencialmente transformadoras em diversos setores, incluindo finanças, saúde, educação, governança, e-commerce, e muitos outros. Elas oferecem soluções para problemas críticos de segurança e privacidade, facilitando uma verificação de identidade mais segura e eficiente.

Além disso, as iniciativas de padronização, como aquelas conduzidas pelo W3C, DIF, Hyperledger e outras organizações, estão trabalhando para garantir que as IDDs sejam interoperáveis e amplamente adotadas. Essas iniciativas são fundamentais para criar um ecossistema de identidade digital que seja seguro, confiável e centrado no usuário.

Em resumo, as Identidades Digitais Descentralizadas representam um passo importante em direção a um futuro onde os indivíduos têm controle total sobre suas informações digitais, promovendo maior segurança, privacidade e eficiência em um mundo cada vez mais digitalizado.

1.1 Objetivos do Relatório

A meta 5 prevê o desenvolvimento da arquitetura e de componentes de um metassistemas de Identidade Digital Descentralizada (IDD) com sua respectiva aplicação, incluindo atividades de testes de desempenho e escalabilidade. A meta visa também atividades relacionadas com prospecções tecnológicas em IDD, acompanhamentos e contribuições nos grupos de desenvolvimento e padronização.

A atividade 5.1 contempla a realização de prospecção tecnológica com objetivo de identificar novas tecnologias, assim como novos produtos e ferramentas relacionadas com o metassistema IDD. Além da prospecção tecnológica, a atividade prevê-se realização de atividades relacionadas com:

1. Interoperabilidade: monitoramento e participação de fóruns para contribuir com as discussões de interoperabilidade;
2. Padronização: acompanhamento das discussões e elaboração de contribuições nos órgãos de padronização relacionados com IDD, tais como ABNT, ITU, DIF e ToIP (Trust-over-IP);
3. Acompanhamento do estado atual e da evolução do quadro regulatório no Brasil e no exterior, com especial atenção aos aspectos de proteção de dados e privacidade trazidos pelas leis gerais de proteção de dados, tais como o Regulamento Geral de Proteção de dados da União Europeia e a Lei Geral de Proteção de Dados do Brasil (LGPD).

1.2 Público Alvo

Este documento é destinado a todos os envolvidos diretamente e indiretamente na execução do projeto, a saber:

- MCTI;
- RNP;

- CPqD;
- Softex
- Participantes da chamada da meta 5, ou seja, empresas e universidades.

2 Fundamentos de IDD

Identidades Digitais Descentralizadas (IDD) são um conceito emergente que visa devolver o controle das identidades digitais aos indivíduos, removendo a necessidade de intermediários centralizados. A seguir, são apresentados os principais fundamentos de IDD.

2.1 Principais elementos do metassistema

Com o crescimento da internet e o avanço de seus padrões, tecnologias e aplicações, a gestão de identidades digitais tem se tornado cada vez mais relevante, atingindo uma ampla aceitação. Um exemplo notável é a Sovrin, [1] uma rede blockchain permissionada focada em aplicações de identidade digital auto-soberana (NAIK; JENKINS, 2021). A abertura do código da Sovrin levou à criação da *Hyperledger Indy*, um livro-razão distribuído voltado para identidades descentralizadas. Desde sua criação, a Indy se desenvolveu em um projeto robusto, abrangendo diversas aplicações. No final de 2018, sua biblioteca de criptografia foi reconhecida como um projeto autônomo, denominado *Hyperledger Ursa*. Em março de 2019, a parte relacionada a agentes também se tornou um projeto independente, chamado *Hyperledger Aries*. Assim, o *Hyperledger Indy* original se desdobrou em três projetos distintos. Além dos projetos citados acima, existem iniciativas de padronização dos modelos de gerência relacionados a identidade digital, um exemplo, a fundação *Trust Over IP* [2], que trabalha na padronização de uma arquitetura proposição de um ecossistema de confiança digital no qual as interconexões entre cada ecossistema de confiança digital são facilitadas por meio da pilha ToIP (WINDLEY, 2023).

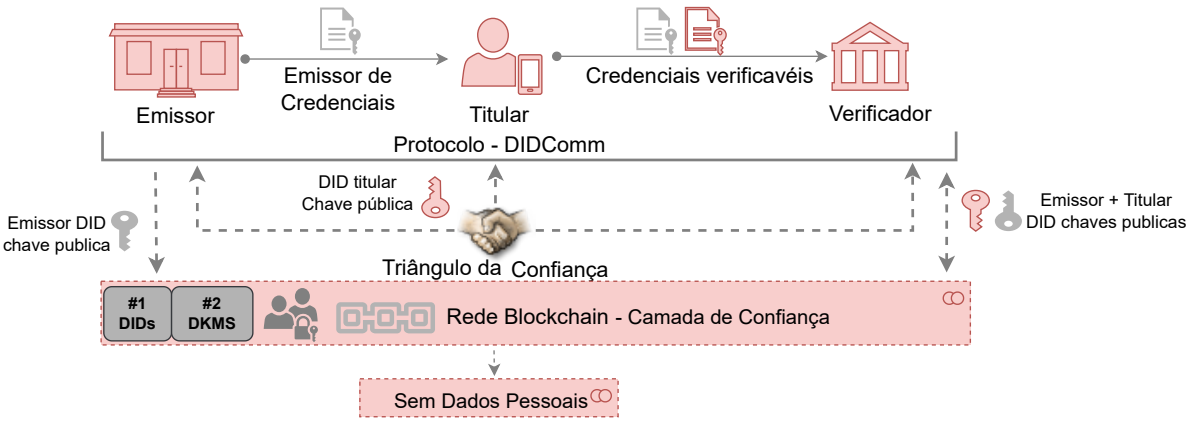

Figura 1: Elementos do metassistema.

Dentro desse contexto são estruturados agentes que constituem elementos no contexto do ecossistema de IDD, onde é possível criar agentes e estabelecer processos de emissão, verificação e utilização de credenciais. A comunicação é realizada através do protocolo de comunicação *DIDcomm*, onde as transações de verificação são realizadas via registros na blockchain conforme a Figura 1 (ÁVILA et al., 2023). É válido ressaltar que na blockchain não se registra nenhum dado sensível, apenas os *schemas* de informações que será atrelado a credencial do usuário.

[1] https://sovrin.org/
[2] https://trustoverip.org/

2.2 Tecnologias de registros distribuídos para IDD

Quando se trata de selecionar a plataforma blockchain ideal, seja *Hyperledger Besu* ou *Hyperledger Indy*, para aprimorar uma solução de identidade digital descentralizada (IDD), a decisão deve ser baseada nas necessidades exclusivas de blockchain e identidade. Cada plataforma oferece recursos exclusivos que podem aprimorar a implementação de sistemas IDD de diversas maneiras (FAN et al., 2022; BERTRAM et al., 2022). Agora, vamos nos aprofundar na perspectiva técnica das vantagens e desvantagens de cada plataforma no contexto de complementação de uma solução IDD.

A estrutura blockchain Hyperledger Besu:

- *Prós*

1. Compatibilidade com EVM: Besu é plenamente compatível com a *Ethereum Virtual Machine (EVM)*, o que facilita o uso de um amplo conjunto de ferramentas e infraestruturas preexistentes, simplificando a integração e o desenvolvimento de aplicações;
2. Versatilidade: Oferece suporte tanto para redes públicas quanto permissionadas, oferecendo flexibilidade para desenvolver soluções de Identidade Digital Descentralizada (IDD) que necessitam de diferentes graus de controle e exposição;
3. Transações Privadas: Besu suporta transações privadas, uma característica crucial para manter a confidencialidade dos dados de identidade em ambientes corporativos;
4. Execução de Contratos Inteligentes: Permite a interoperabilidade entre diferentes blockchains por meio da execução de contratos inteligentes;
5. Modelo de Governança Customizável: Facilita a definição de papéis e responsabilidades dentro da rede, ajustando-se a cada necessidade transacional.

- *Contras*

1. Escalabilidade e Performance: Como um cliente Ethereum, Besu enfrenta desafios relacionados à escalabilidade e latência, especialmente em redes públicas, o que pode representar uma limitação para soluções de IDD de grande escala.
2. Complexidade Técnica: A configuração e manutenção de um nó Besu, particularmente em ambientes que demandam elevados padrões de segurança e privacidade, podem apresentar complexidade considerável.
3. Foco Geral: Embora Besu possa ser adaptado para suportar sistemas de IDD, ele não inclui características específicas de identidade em seu núcleo, exigindo desenvolvimento adicional para atender a requisitos específicos de identidade.

A estrutura blockchain Hyperledger Indy:

- *Prós*

1. Foco em Identidade Digital: Projetado exclusivamente para gerenciamento de identidade, inclui suporte integrado para Identificadores Descentralizados (DIDs) e Credenciais Verificáveis (VCs), tornando-o ideal para aplicações focadas em identidade;
2. Segurança e Privacidade Reforçadas: Com um design centrado em segurança e privacidade, oferece funcionalidades avançadas para o controle de consentimento e gerenciamento de dados pessoais;

3. Interoperabilidade de Identidade: Promove a construção de redes de identidade interoperáveis e escaláveis, perfeitas para sistemas que requerem verificações de identidade confiáveis e descentralizadas;
4. Modelo de Governança Customizável: Facilita a definição de papéis e responsabilidades dentro da rede, ajustando-se a cada necessidade transacional.

- *Contras*

1. Aplicabilidade Restrita: Embora seja altamente eficiente para aplicações de identidade, sua especialização pode limitar a flexibilidade para outros tipos de uso não relacionados diretamente à identidade;
2. Curva de Aprendizado Elevada: As particularidades técnicas e os conceitos de Identidade Auto-soberana exigem um investimento considerável em treinamento e desenvolvimento;
3. Comunidade Menor: Em comparação com Besu e outras plataformas baseadas em Ethereum, Indy possui uma comunidade de usuários e desenvolvedores relativamente menor, o que pode reduzir o suporte e os recursos de desenvolvimento disponíveis.

Dependendo das necessidades específicas do projeto, em alguns casos pode ser vantajoso combinar as duas plataformas de integração. Por exemplo, Besu pode ser utilizado para comunicações gerais e interações com o ecossistema EVM, enquanto Indy pode ser empregado para lidar com questões de identidade digital (BERTRAM et al., 2022). A decisão entre Besu e Indy deve ser tomada com base nos casos de uso, considerandos fatores como o tipo de rede requerida (pública versus permissiva), requisitos de confidencialidade, privacidade, divulgação e identificação específica do programa (FAN et al., 2022). Ambas plataformas oferecem recursos essenciais para o desenvolvimento de soluções de IDD, sendo crucial escolher estrategicamente aquela que melhor se alinhe aos objetivos técnicos e comerciais do projeto.

3 Metodologia utilizada na prospecção

Quando se trata de Identidade Digital Descentralizada (IDD), nossa abordagem envolve o uso de metodologia de prospecção crítica. Isto permite-nos garantir uma pesquisa e análise aprofundada de artigos e trabalhos que contribuem para o desenvolvimento de sistemas robustos e confiáveis. A prospectiva abrange uma série de etapas metodológicas, incluindo a exploração, avaliação e integração de avanços tecnológicos, adaptação às mudanças regulatórias, melhoria das medidas de segurança e privacidade e promoção da interoperabilidade. A seguir descreve-se a abordagem e os elementos-chave da metodologia padrão empregada na prospecção no âmbito da identidade digital descentralizada.

Este processo abrangente inclui a realização de pesquisas e análises de tendências, avaliação de requisitos regulatórios e normativos, desenvolvimento de protótipos, realização de testes de segurança e privacidade, avaliação de interoperabilidade, lançamento de pilotos, coleta de *feedback* para melhoria contínua e, finalmente, escalonamento e implementação das mudanças necessárias.

A metodologia de prospecção em identidade digital descentralizada deve ser rigorosa e adaptável, garantindo que as soluções sejam seguras, conformes e eficazes. A natureza interativa e baseada em evidências deste processo é essencial para o sucesso em um campo tão dinâmico e regulado como o das identidades digitais, nesse contexto alguns assuntos relacionados aos agentes envolvidos no contexto de identidade foram identificados, tais como:

3.1 A necessidade da prospecção em IDD

A exploração de oportunidades no domínio da Identidade Digital Descentralizada (IDD) é um esforço essencial para avançar e abranger soluções que aproveitem tecnologias descentralizadas de identidade digital. Este processo envolve o exame, criação e execução de sistemas que facilitam o estabelecimento, administração e utilização segura, confidencial e eficaz de identidades digitais. O ato de prospectar nesta área é de extrema importância devido a vários fatores, cada um dos quais com implicações significativas tanto para os utilizadores como para as entidades que adotam esta tecnologia (BAI et al., 2022).

A necessidade e as vantagens da prospecção no âmbito da identidade digital descentralizada são evidentes.

- A busca pela inovação e melhoria contínua é essencial:

O campo da tecnologia de identidade digital está em constante estado de evolução. Ao antecipar e abraçar os avanços tecnológicos, podemos melhorar a segurança, a usabilidade e a interoperabilidade dos sistemas descentralizados de identidade digital. Isso envolve a investigação de novos protocolos blockchain, avanços em criptografia e métodos inovadores de interação usuário-serviço.

- Ajustando-se aos requisitos regulamentares:

A evolução das leis e regulamentos de privacidade e segurança de dados, como o GDPR na Europa e a LGPD no Brasil, exige atualizações contínuas. Ao incorporar a previsão, os sistemas descentralizados de identidade digital podem ajustar-se eficazmente a estas modificações, garantindo a adesão aos regulamentos e salvaguardando os direitos dos utilizadores (NEVES, 2021).

- A troca contínua de informações e funcionalidades entre vários sistemas é conhecida como interoperabilidade:

A troca contínua de informações e funcionalidades entre vários sistemas é conhecida como interoperabilidade. A comunicação eficaz entre vários sistemas e plataformas é crucial para a aceitação generalizada de identidades digitais descentralizadas. A exploração destes domínios pode contribuir para estabelecer protocolos e padrões que promovam a interoperabilidade, permitindo a utilização de identidades digitais em diversos setores e contextos.

- A proteção da segurança e da privacidade é de extrema importância:

O processo de prospecção auxilia na identificação de potenciais fragilidades e na formulação de soluções para mitigá-las, garantindo a salvaguarda das identidades digitais contra acessos não autorizados e uso indevido. Isto inclui o estabelecimento de estruturas mais sólidas para a gestão de chaves privadas, práticas de autenticação seguras e estratégias avançadas para preservar a privacidade.

- Promover a aceitação e incentivar a adoção:

O sucesso das soluções descentralizadas de identidade digital depende de uma compreensão abrangente das necessidades dos utilizadores e entidades. Ao participar na prospecção, estas soluções podem ser adaptadas para melhor se alinharem com as expectativas e requisitos dos vários intervenientes, aumentando assim a aceitação e adoção das tecnologias.

- O processo de desenvolvimento de casos de uso é um aspecto essencial do desenvolvimento do projeto:

É crucial explorar e cultivar novas aplicações para identidade digital descentralizada, a fim de mostrar o valor da tecnologia. Esta exploração poderia abranger vários sectores, incluindo cuidados de saúde, finanças, educação e governo, onde a identidade digital tem o potencial de produzir vantagens substanciais em termos de processos simplificados, maior segurança e melhor acesso aos serviços.

Para cultivar um ecossistema resiliente, inexpugnável e flexível, capaz de responder às necessidades presentes e futuras, é imperativo explorar o potencial da identidade digital descentralizada. Essa exploração não apenas alimenta o avanço da tecnologia, mas também garante a praticidade, segurança e aderência às regulamentações existentes das soluções elaboradas. Tais esforços promovem uma aceitação generalizada e produzem benefícios substanciais para a sociedade.

4 Temas Prospectados

Os temas prospectados em Identidades Digitais Descentralizadas (IDD) são vastos e abrangem diversas áreas, refletindo a evolução e o potencial futuro dessa tecnologia. Aqui estão alguns dos temas mais importantes.

4.1 Protocolos de IDD

A base de sistemas de gestão de identidade seguros e independentes reside nos protocolos técnicos de identidade digital descentralizada. Esses protocolos foram desenvolvidos especificamente para capacitar os indivíduos com total autoridade sobre suas identidades digitais, facilitando interações online seguras e confidenciais. Exploramos alguns dos principais protocolos técnicos que estão moldando o cenário da identidade digital descentralizada:

1. DIDs (Identificadores Descentralizados)

   A especificação para DIDs, criada pelo W3C, introduz uma nova forma de identificador que possui alcance global, capacidade de resolução, persistência e propriedade total por parte do detentor da identidade, tudo sem dependência de um órgão governamental centralizado (REED et al., 2020). A funcionalidade principal dos DIDs envolve a conexão entre cada DID e seu Documento DID correspondente, que contém detalhes essenciais para verificar a identidade associada. Esses detalhes incluem chaves públicas, métodos de autenticação e serviços de comunicação.

2. *Verifiable Credentials* (VCs)

   Credenciais verificáveis(VCs) são o segundo ponto de discussão. A especificação *Verifiable Credentials*, fornecida pelo W3C, descreve o processo de geração e utilização de credenciais digitais que podem ser autenticadas sem esforço. Isso facilita a transferência de credenciais entre diversas plataformas e aplicativos, ao mesmo tempo, em que mantém os mais altos níveis de segurança e privacidade (BRUNNER et al., 2020).

   A funcionalidade dos VCs reside na sua capacidade de serem apresentados e autenticados eletronicamente usando métodos criptográficos. Essas credenciais digitais servem para validar qualificações, atributos ou direitos de maneira segura e confiável.

3. DIDComm

   DIDComm, também conhecido como Comunicação Descentralizada de Identificadores, é um protocolo inovador que permite a comunicação segura e privada entre indivíduos e entidades de forma descentralizada. Com o DIDComm, os usuários podem estabelecer conexões verificáveis e à prova de adulteração, trocar mensagens e compartilhar dados sem depender de intermediários centralizados ou comprometer sua privacidade. Esta tecnologia inovadora permite que os

indivíduos assumam o controle de suas informações pessoais e se comuniquem com confiança. DIDComm está revolucionando como interagimos e nos comunicamos na era digital, oferecendo um novo nível de segurança, privacidade e autonomia (CURREN; LOOKER; TERBU, 2022).

A Decentralized Identity Foundation (DIF) e o Hyperledger Aries estão impulsionando o avanço do desenvolvimento nesta área. DIDComm, um protocolo de comunicação, permite que entidades com DIDs troquem mensagens criptografadas e autenticadas com segurança. Este protocolo promove a interoperabilidade e facilita a integração de serviços em vários sistemas de identidade.

A comunicação entre agentes acontece por meio de um mecanismo de mensagem chamado DIDcomm (DID *Communication*). DIDcomm permite uma troca segura e assíncrona de mensagens encriptadas ponto-a-ponto, que geralmente são roteadas por meio de agentes Aries intermediários como definido na Figura 2.

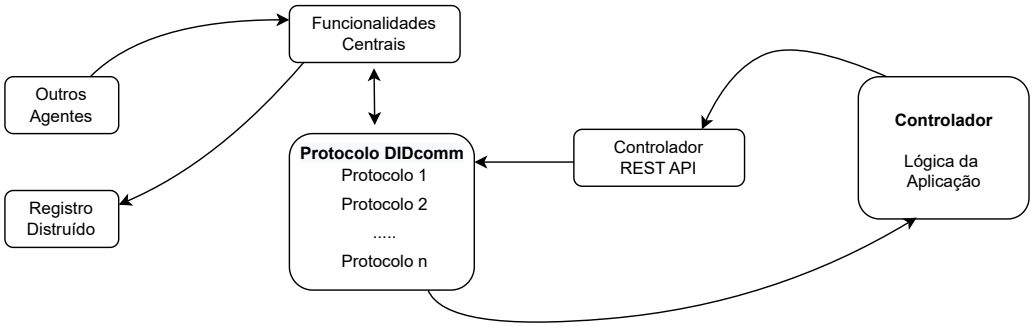

Figura 2: Estrutura interna de comunicação entre Agente Aries

O mecanismo usa uma instância do método did:peer DID *method*, que faz uso de DIDs não publicados na blockchain, utilizados apenas de forma privada entre os dois agentes que se comunicam.

A base dos sistemas descentralizados de identidade digital reside nestes protocolos técnicos, que equipam os indivíduos com os meios para gerir com segurança as suas identidades digitais. Esses protocolos são meticulosamente elaborados para garantir segurança, interoperabilidade e capacidade de oferecer suporte a uma ampla gama de aplicações. Quer se trate de uma verificação de identidade básica ou de uma transação complexa que exige autenticação forte e validação de credenciais, esses protocolos têm tudo sob controle.

4.2 Interoperabilidade e Padrões

A interoperabilidade do padrão DID refere-se à capacidade dos Identificadores Descentralizados (DIDs) produzidos e administrados na rede Hyperledger Indy de serem empregados e reconhecidos em sistemas e redes alternativas que adotam princípios e padrões de identidade descentralizados.

Esta interoperabilidade crucial facilita o estabelecimento de um ecossistema de identidade digital, permitindo aos utilizadores manter a autoridade sobre as suas identidades e utilizá-las perfeitamente em várias plataformas com a máxima segurança e eficiência (YILDIZ et al., 2022). Os principais componentes para garantir a conformidade da interoperabilidade com os padrões globais para o Transtorno Dissociativo de Identidade (TDI) são os seguintes:

1. Conformidade com padrões globais: O design do DID visa alinhar-se com os padrões globais de identidade digital estabelecidos, incluindo aqueles delineados pelo W3C para DIDs. Isso garante que os DIDs criados no Hyperledger Indy possam ser compreendidos e utilizados em outras redes que aderem a esses protocolos padronizados.

2. Especificação para o método DID: A especificação do método DID descreve o processo de geração, resolução e supervisão de DIDs na rede Indy. Ao aderir a esta especificação, outras

redes e sistemas podem compreender e interagir de forma eficaz com DIDs do tipo Indy, promovendo assim uma interoperabilidade contínua.

3. Resolução de DID: O processo de resolução DID envolve a aquisição do documento DID vinculado a um identificador DID específico. Neste documento, podem-se encontrar todos os detalhes essenciais necessários para confirmar a identidade associada ao DID, incluindo chaves públicas e terminais de serviço. Aprova resoluções que permitem a resolução perfeita de DIDs gerados na rede Indy em outras redes compatíveis.

4. Compatibilidade com *Verifiable Credentials* (VCs): Credenciais digitais conhecidas como Credenciais Verificáveis podem passar por verificação criptográfica usando um DID. A compatibilidade da rede Indy com o padrão W3C Verifiable Credentials permite o reconhecimento e aceitação contínuos de credenciais emitidas e verificadas na plataforma por outras plataformas que adotaram este padrão amplamente reconhecido.

5. Interoperabilidade de Chaves Criptográficas: O DID emprega métodos criptográficos que aderem a protocolos universalmente reconhecidos com a finalidade de autenticar e validar identidades. Isto permite uma integração perfeita com outras redes que empregam tecnologias de chave pública semelhantes.

6. Rede de Confiança: Ao interagir com o DID, torna-se possível fazer parte de uma rede de confiança mais extensa, onde várias entidades depositam a sua confiança nas mesmas autoridades certificadoras ou mecanismos de verificação. Consequentemente, as identidades e credenciais que foram verificadas dentro de uma rede podem ser prontamente reconhecidas e aceitas em outras redes que estejam interconectadas dentro da mesma rede de confiança.

Em contextos gerais, os benefícios da interoperabilidade DID, fornece maior flexibilidade aos usuários: os usuários podem usar suas identidades digitais em vários serviços e plataformas sem precisar recriar ou gerenciar diversas identidades (WINDLEY, 2023).

Facilitar a colaboração entre organizações: As organizações podem reconhecer e aceitar identidades e credenciais emitidas por outras entidades, facilitando assim a colaboração e a integração de serviços. Adoção mais ampla de identidades descentralizadas: A interoperabilidade facilita a adoção de identidades descentralizadas porque facilita o acesso e a integração dos sistemas.

Alguns dos exemplos básicos de interoperabilidade estão relacionados a autenticação entre fronteiras, ou seja, um usuário utiliza sua identidade digital baseada em DID, assim é possível acessar diferentes países que aceitam DIDs.

Mais um exemplo está vinculado a serviços financeiros, bancos e outras instituições financeiras podem aceitar identidades e credenciais verificadas por outros bancos ou autoridades reguladoras e diferentes jurisdições.

Em suma, permitir a interoperabilidade dos DIDs é um componente crucial no estabelecimento de uma rede mundial de identidades digitais descentralizadas. Ao garantir que os DIDs criados e mantidos na plataforma Hyperledger Indy possam ser utilizados e autenticados em outras redes compatíveis, o DID facilita a ampla aceitação de identidades digitais seguras, privadas e gerenciadas pelo usuário, promovendo um cenário digital mais confiável e simplificado (WINDLEY, 2023).

4.3 EIDAS 2.0

O eIDAS (The European Digital Identity Regulation) 2.0, ou Regulamento Europeu de Identificação Digital, é um regulamento destinado a melhorar a infraestrutura digital da União Europeia, concentrando-se em identidade digital e autenticação, com o objetivo de assegurar a interoperabilidade, segurança e confiabilidade das transações digitais além das fronteiras. A gestão do eIDAS 2.0

é vital para garantir a incorporação segura e eficiente de tecnologias emergentes, como a Identidade Digital Descentralizada (IDD) e a blockchain, ao ecossistema europeu (EIDAS 2. . . , s.d.).

Fundamentos do eIDAS 2.0 e Governança da Identidade Digital

O objetivo do eIDAS 2.0 é criar uma Identidade Digital Europeia (European Digital Identity - EDI), permitindo que cidadãos e empresas tenham acesso a serviços públicos e privados de maneira segura, simplificada e uniforme em toda a União Europeia. A sua governança abrange uma estrutura sólida que engloba a administração de identidades digitais, autenticação digital e serviços de confiança. A governança do eIDAS 2.0 é fundamentada em normas técnicas e procedimentos operacionais que asseguram a interoperabilidade e a aderência aos requisitos legais e técnicos (REGULATATION EU. . . , s.d.). Ela também assegura a salvaguarda de dados pessoais, conforme o Regulamento Geral de Proteção de Dados (GDPR), possibilitando que indivíduos e organizações detenham total domínio sobre suas identidades e informações. A governança do eIDAS 2.0 é regulada por um conjunto de autoridades e organismos que gerenciam e supervisionam sua implementação e funcionamento. Os principais elementos da governança técnica incluem:

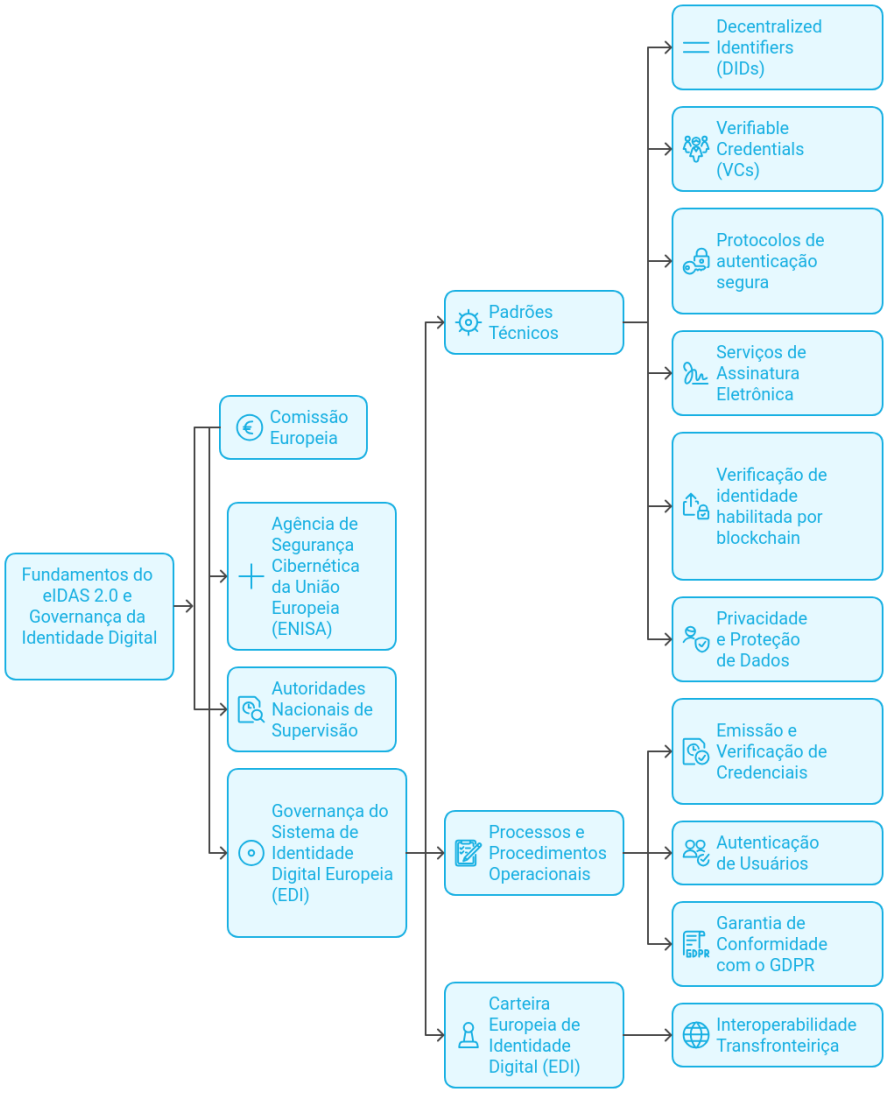

Figura 3: Estrutura de Governança Técnica do eIDAS 2.0

Recentemente, ocorreram algumas alterações ligadas à implementação de tecnologias descentralizadas, tais como Identificações Descentralizadas (DIDs) e Certificados Verificados (VCs) (EIDAS 2. . . , s.d.). Essas tecnologias contribuem para o desenvolvimento de um sistema mais adaptável e seguro para a administração de identidades digitais.

→ DIDs (Identificações Descentralizadas): A partir de 2024, o eIDAS 2.0 possibilita a utilização de DIDs para a criação de identidades digitais descentralizadas, sem a exigência de uma entidade centralizada para validar ou emitir identidades. Isso é um grande progresso, já que as identidades podem ser administradas diretamente pelos cidadãos, sem a necessidade de intermediários, diminuindo assim os custos e os riscos de falhas no sistema;

→ Credenciais Verificáveis (VCs): Com a atualização do eIDAS 2.0, agora é possível utilizar credenciais verificáveis para validar características de identidade, como habilitações educacionais.

As atualizações recentes também apresentaram progressos notáveis em comparação à versão anterior, espelhando as novas demandas do mercado digital globalizado e as inovações tecnológicas em ascensão. No ano de 2024, a Identidade Digital Europeia (EDI) e as tecnologias descentralizadas se consolidaram como elementos fundamentais da regulamentação, aumentando a segurança, a interoperabilidade e a privacidade, ao mesmo tempo que consolidam a confiança nas transações digitais em todo o território europeu (EIDAS 2. . . , s.d.) e (REGULATATION EU. . . , s.d.). No entanto, o ponto crucial desses progressos foi a introdução da identidade digital europeia (European Digital Identity - EDI), que permite que cidadãos e empresas da União Europeia administrem suas identidades digitais de maneira segura, confiável e descentralizada. A implementação da carteira digital possibilitará aos cidadãos guardar e administrar suas identidades digitais, credenciais verificáveis e outros dados pessoais de maneira segura, mantendo total controle sobre suas informações. A EDI Wallet tem a capacidade de autenticar e autorizar em diversos serviços, tanto públicos quanto privados, tanto em âmbitos nacionais quanto transfronteiriços[9]. Em síntese, a governança do eIDAS 2.0 consiste em uma estrutura de múltiplas camadas que combina componentes regulatórios, técnicos e operacionais para assegurar a proteção, a interoperabilidade e a privacidade das identidades digitais em toda a União Europeia. O eIDAS 2.0, ao integrar tecnologias de identificação descentralizada, serviços de confiança e transações digitais seguras, cria uma base essencial para uma economia digital protegida. A estrutura de governança assegura a privacidade, a salvaguarda de dados e a independência do usuário, enquanto possibilita a interoperabilidade e a confiança além das fronteiras. Conforme o eIDAS 2.0 progride, sua integração com tecnologias emergentes e sistemas globais têm um papel crucial na determinação do futuro da gestão de identidade digital.

4.4 EBSI

A European Blockchain Services Infrastructure (EBSI) é um projeto da União Europeia criado para oferecer uma infraestrutura blockchain segura, confiável e interoperável, com o objetivo de apoiar serviços públicos digitais e fomentar a inovação. A governança da EBSI, administrada pela European Blockchain Partnership (EBP), formada por todos os Estados-Membros da União Europeia, Noruega e Liechtenstein, é crucial para assegurar que a infraestrutura opere de forma eficaz, descentralizada e em consonância com as metas da UE (PARTNERSHIP, 2024). EBSI é uma rede blockchain autorizada e descentralizada que proporciona apoio a diversos serviços públicos transfronteiriços, fomentando a confiança e a eficácia. Emprega blockchain para oferecer serviços públicos de forma transparente, segura e interoperável, concentrando-se em campos como a identidade digital, a rastreabilidade de documentos e contratos digitais (PARTNERSHIP, 2024) e (MALHOTRA, 2023). Dentro do contexto de governança da EBSI, é baseado nos conceitos já conhecidos em redes blockchains, como:

1. **Interoperabilidade**: Assegurar uma interação suave entre redes blockchain públicas e privadas.
2. **Descentralização e Sustentabilidade**: Preservar uma organização descentralizada ao mesmo tempo que minimiza o impacto no meio ambiente;
3. **Segurança e Aderência**: Atender às normas da União Europeia, como o Regulamento Geral de Proteção de Dados (GDPR);

4. **Incentivo à Inovação:** Apoiar projetos tecnológicos que melhorem os serviços tanto públicos quanto privados na Europa.

Com isso, é possível identificar como a estrutura da EBSI é organizada, levando em consideração a governança no contexto de redes descentralizadas, além de deixar claro as interações técnicas entre cada Nó(ente da rede) inserido na organização ou empresa (COMMISSION, 2023) e (FERNANDES, 2024). A Figura 4 mostra a estrutura de governança técnica da EBSI.

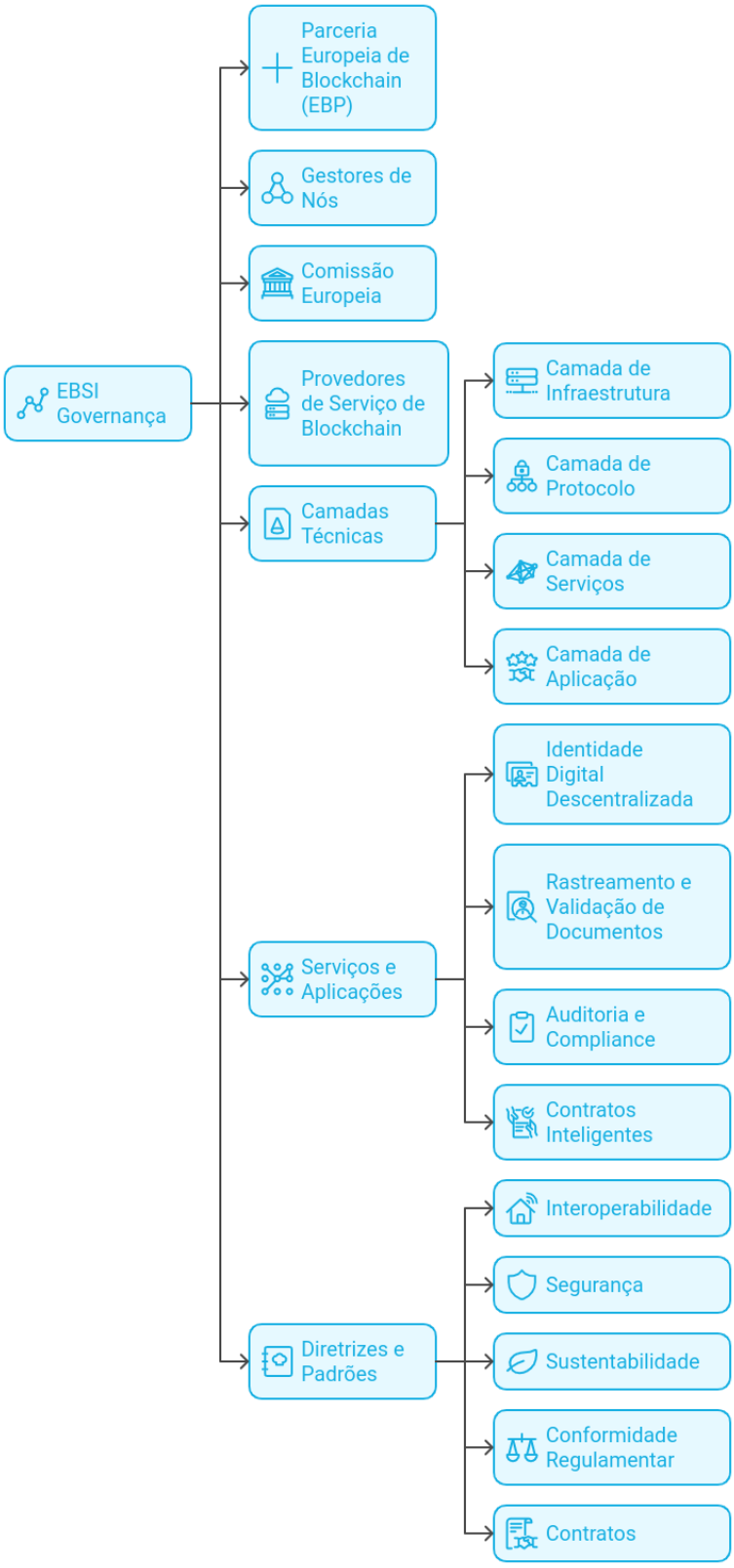

Figura 4: Estrutura de Governança Técnica da EBSI

Com a evolução da estrutura de governança técnica da EBSI, naturalmente pode-se vê alguns benefícios da governança EBSI, como :

1. **Confiabilidade e Descentralização:**: Os Estados-Membros dividem a governança, assegurando a descentralização e a confiança;

2. **Interoperabilidade além das fronteiras nacionais**: Transações e serviços públicos em toda a União Europeia são facilitados;
3. **Innovation and Inclusion**:Incentiva a criação de novos serviços digitais que satisfazem as demandas de cidadãos e corporações;
4. **Proteção Melhorada:** Normas sofisticadas de criptografia e validação diminuem a probabilidade de ataques virtuais.

E com essas evoluções, é mais natural ainda, o surgimento de desafios relacionados ao modelo de governança da EBSI, como:

1. **Escalabilidade:**: Assegurar a capacidade da infraestrutura de suportar um crescimento no volume de transações;
2. **Interoperabilidade Internacional**: Ligar-se a redes blockchain além das fronteiras da UE;
3. **Educação e Adoção**:Estimular a compreensão e aplicação por parte de governos, corporações e indivíduos;
4. **Crescimento dos Casos de Uso:** Expandir a abrangência dos serviços da EBSI em setores como saúde e IoT;
5. **Compatibilidade com eIDAS 2.0:** Sinergia com as identidades digitais auto-suficientes da EDI Wallet;
6. **Colaboração Ampliada com o Setor Privado:** Ações conjuntas para criar soluções inovadoras e eficazes.

Em resumo, a gestão da EBSI espelha os princípios fundamentais da União Europeia: descentralização, interoperabilidade e segurança. Com uma infraestrutura sólida e padrões claramente estabelecidos, a EBSI está preparada para ser o alicerce de uma revolução digital que interliga cidadãos, corporações e governos em um ambiente seguro e eficaz. A incorporação de tecnologias como DIDs, certificados verificáveis e blockchain com eficiência energética assegura que a EBSI não só satisfaça as demandas presentes, mas também esteja apta a enfrentar os obstáculos do futuro digital.

4.5 OpenID4VC

O OpenID4VC (OpenID para Credenciais Verificáveis) (OPENID FOUNDATION, 2023) (GITHUB, 2024a) é um padrão emergente desenvolvido com o propósito de integrar credenciais verificáveis (VCs) aos ecossistemas existentes de OpenID e OAuth, os quais são padrões abertos amplamente usados para autenticação e autorização em sistemas de identidade digital para promover segurança e interoperabilidade. O OpenID, a partir do uso de um protocolo baseado em HTTP, possibilita aos usuários utilizar uma única identidade digital para acessar múltiplos serviços, dentro do conceito de autenticação única (Single Sign-On - SSO). Por sua vez, o OAuth (Open Authorization) é focado em autorização e faz uso de tokens efêmeros com permissões específicas de modo a separar autenticação (verificação de quem solicita o acesso) de autorização (definição daquilo que esse usuário pode fazer após o acesso). O OAuth também garante maior controle sobre acessos feitos por aplicativos de terceiros, em nome de um usuário, a recursos protegidos, evitando com isso a exposição das credenciais do usuário. Para tanto, são definidos alguns papéis, a saber: o dono do recurso (resource owner), o servidor onde o recurso se encontra (resource server), o servidor que autoriza o acesso ao recurso (authorization server) e o cliente que solicita acesso ao recurso. E, na interação entre esses papéis, uma solicitação do cliente para acessar um dado recurso deve,

primeiramente, obter uma autorização do dono do recurso e utilizá-la em seguida para obter do servidor de autorização um token de acesso a ser apresentado ao servidor que armazena o recurso, para somente então ter acesso a ele (durante um período definido). A integração das VCs aos ecossistemas de OpenID e OAuth permite que organizações utilizem uma estrutura familiar para emitir e verificar VCs de forma segura, promovendo interoperabilidade e gerenciamento de identidades descentralizadas.

A OpenID4VC consiste de três especificações:

- OpenID para Emissão de VCs (OID4VCI): Define uma API e mecanismos de autorização correspondentes baseados em OAuth para emissão de Credenciais Verificáveis;
- OpenID para Apresentações Verificáveis (OID4VP): Define um mecanismo sobre o OAuth 2.0 para permitir a apresentação de reivindicações na forma de VCs como parte do fluxo de protocolo.
- Provedor OpenID Auto-Emitido v2: Permite que usuários finais usem Provedores OpenID (OPs) que eles controlam

Seus principais aspectos são:

1. **Emissão de Credenciais (OpenID4CI)**: Usuários podem solicitar VCs por meio de um aplicativo de carteira digital. O processo envolve a interação entre a carteira, um servidor de autorização (para obter tokens de acesso) e um sistema de emissão de VCs, garantindo a emissão segura e com consentimento do usuário.
2. **Apresentação e Verificação (OpenID4VP)**: Usuários podem apresentar suas VCs a terceiros verificadores (como prestadores de serviços). O OpenID4VP utiliza mecanismos existentes do OpenID para facilitar o compartilhamento interoperável de credenciais, mantendo nas mãos do usuário o controle sobre seus dados.
3. **Compatibilidade e Interoperabilidade**: O OpenID4VC suporta múltiplos formatos de credenciais (como as VCs definidas pelo W3C) e diversos conjuntos criptográficos. Ele prioriza a interoperabilidade em diferentes ecossistemas de identidade digital, evitando vínculos obrigatórios a fornecedores específicos.
4. **Estruturas de Confiança:** A confiança é mantida através de relações bem definidas entre as partes emissoras e verificadoras. O OpenID4VC também pode ser usado em conjunto com outros protocolos, como o DIDComm, para fluxos de trabalho descentralizados mais amplos.

Em janeiro de 2024, foi concluída a primeira análise aprofundada de segurança da OpenID4VC, com o objetivo de aumentar a confiança na segurança de suas especificações. A análise incluiu os protocolos OID4VCI e OID4VP e usou o Web Infrastructure Model (WIM), modelo formal detalhado da web, desenvolvido pela Universidade de Stuttgart, para modelar a interação dos protocolos em um ecossistema e provar que são seguros com relação à definição de segurança sob certas suposições e decisões de modelagem. A definição de segurança usada na análise abrangeu várias propriedades importantes em torno da emissão e apresentação de credenciais; em particular, que um atacante não deve ser capaz de se passar por um usuário honesto, dar início a um fluxo de login no dispositivo de um usuário ou forçar um usuário a fazer login sob uma identidade escolhida pelo atacante. A adoção do OpenID4VC vem crescendo, com destaque para iniciativas como a Estrutura Europeia de Identidade Digital (EUDI) ou sua menção em normas que vêm sendo elaboradas pela ISO. A título de exemplo, em abril de 2023, 18 carteiras no projeto EBSI da Comissão Europeia já davam suporte às especificações OID4VCI e OID4VP. Por outro lado, no âmbito da ISO, três rascunhos de norma (ISO/IEC TS 23220-4, TS 18013-7 e TS 23220-3) tratam de aspectos da OID4VP ou da OID4VCI. Todos esses desdobramentos são um indicativo do potencial do OpenID4VC como tecnologia base em sistemas de identidade digital.

4.6 OpenIDDidcomm

O objetivo do projeto OpenIDDidcomm foi criar uma extensão para os protocolos OpenID4VCI e OpenID4VP com vistas a criar um canal DIDComm para comunicação. São elencados diversos casos de uso nos quais a combinação dos protocolos OpenID4VCI e OpenID4VP com o DIDComm traz vantagens. De modo geral, qualquer caso de uso no qual os participantes se beneficiam do DIDComm pode incorporar o OpenIDIDComm. O caso de uso considerado mais óbvio é a comunicação entre as partes envolvidas após a credencial ter sido emitida. Mas há outras várias possibilidades:

- Revogação de credencial;
- Emissão de VCs em lote;
- Diploma digital;
- Credencial de empregador;
- Registro criminal;
- Emissão de habilitação de condutor iniciada na carteira

Em sua página no Github (GITHUB, 2024b), o projeto OpenIDDidcomm descreve como sua motivação o fato de que os protocolos OpenID4VCI e OpenID4VP atualmente não dispõem de recurso para permitir comunicação entre as partes envolvidas e que a inclusão desse recurso foi conseguida por meio do DIDComm, que é um protocolo generalista de transporte de mensagens baseado em Identificadores Descentralizados (DIDs).

Como ilustrado na Figura 5, uma abordagem descrita na página do projeto é aquela que usa o conceito inerente de escopos do OAuth 2.0. O parâmetro de escopo do Access Token é estendido com o valor DIDComm para expressar o uso para a criação do canal DIDComm. A Wallet então envia um DIDComm Ping contendo o Access Token para criar uma correlação de sessão.

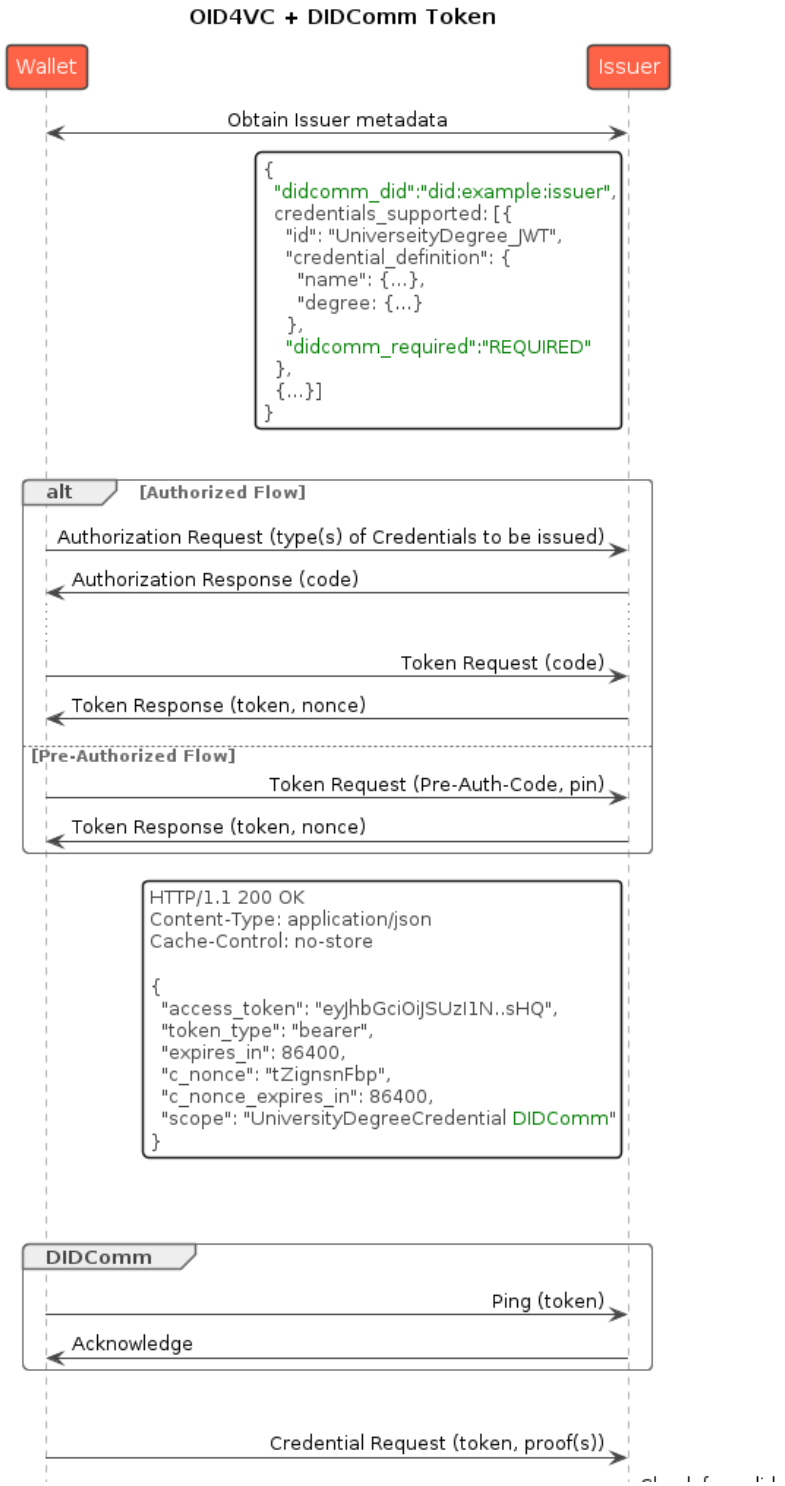

Figura 5: Requisição e autorização utilizando OpenIDDidcomm

Fonte: (GITHUB, 2024b).

Por fim, os responsáveis pelo projeto OpenIDDidcomm chamam a atenção para o fato de a solução ainda (por ocasião da elaboração deste relatório) ser considerada uma prova de conceito, e não um produto final.

4.7 Privacidade e Segurança de Dados

Privacidade e segurança de dados é um aspecto de alta importância em sistemas computacionais, e tornou-se um problema legal após as leis de proteção de dados. Privacidade é uma questão

sensível em blockchain, pois a natureza descentralizada da tecnologia permite que os dados do *ledger* sejam armazenados em diversos dispositivos simultaneamente para garantir disponibilidade e tolerância a falhas da tecnologia. Em sistemas descentralizados quando dados sensíveis ou não autorizados são armazenados existe a dificuldade de remoção dos mesmos, pois o armazenamento descentralizado torna difícil a tarefa de remover dados em todos os participantes, em especial na *ledger* de blockchain, construída para adicionar e atualizar dados somente. Portanto, a medida que mais blocos são adicionados, de maneira criptográfica, mais difícil computacionalmente torna-se remover dados de um determinado bloco adicionado anteriormente, por ser necessário alterar os *hash* de todos os blocos posteriores em sequência inversa do crescimento da cadeia até o bloco que possui os dados em questão, que se caracteriza como violação de segurança da blockchain. Por conta das especificidades técnicas mencionadas, deve haver criterioso cuidado, planejamento e escolha de quais dados devem ser inseridos na blockchain, para evitar que dados sensíveis ou indesejados possam ser adicionados na cadeia.(FALAZI et al., 2019)

Embora a inserção de dados sensíveis ou não autorizados na *ledger* seja uma questão de riscos para a privacidade dos usuários, existem outras formas que a privacidade dos dados de usuários pode ser comprometida, como técnicas de ataques a carteira, ao issuer ou verifier comprometendo a segurança e privacidade do usuário (STODT et al., 2024).

4.7.1 Zero-Knowledge Proof

Prova de conhecimento zero (Zero-Knowledge Proof - ZKP) é um mecanismo criptográfico desenvolvido para que uma pessoa ou entidade possa provar matematicamente a um verificador o conhecimento ou a posse de determinada informação ou dado, sem revelar a informação sensível. O mecanismo é útil para realizar comprovações com grau elevado de certeza matemática, preservando a privacidade. O mecanismo de prova consiste na execução de operações entre o provador e o verificador nas fases de testemunho, desafio e resposta. Inicialmente na fase de testemunho o provador realiza a computação de uma prova e envia para o verificador. Em seguida na fase de desafio o verificador realiza diversas perguntas ao provador e por fim na fase de resposta o provador envia as respostas para o verificador que por fim pode aprovar ou rejeitar a prova gerada.

O mecanismo de prova de conhecimento zero segue três princípios elementares para que nenhum dado indevido seja vazado ou disponibilizado para o verificador e que provas verdadeiras sejam sempre aceitas e provas falsas sejam sempre rejeitadas. O princípio de completude garante que o verificador sempre será convencido a aceitar que a declaração do provador é verdadeira quando o mesmo provar que tal é como verdadeira, em outras palavras, sempre que o provador mostrar que a prova é verdadeira o verificador aceitará a prova. O princípio de solidez refere-se ao verificador rejeitar uma prova quando o provador não conseguir atestar que a declaração é verdadeira, isto é, o provador não conseguir burlar o verificador a aceitar uma prova falsa. Por fim, o princípio de conhecimento zero que consiste na garantia que o provador não fornece nenhuma informação útil ou sensível ao verificador, em outros termos o verificador consegue aceitar a declaração do provador como verdadeira sem aprender nada sobre a informação sensível que a prova refere-se (SUN et al., 2021).

Em termos gerais existem dois tipos de provas de conhecimento as interativas e não-interativas. Em ZKPs interativas o provador e verificador comprometem-se mutuamente num protocolo de troca de mensagens na forma de requisições desafio-resposta em múltiplas rodadas de interação para atestar a validade ou não da declaração do provador. A troca de mensagens ocorre de maneira síncrona similar ao que ocorre no protocolo de internet TCP/IP e durante as interações o provador tem como objetivo convencer o verificador que sua declaração é verdadeira sem revelar informações sensíveis (ZHOU et al., 2024). Por outro ZKPs não-interativas realizam o processo de prova e verificação sem a necessidade de sincronização e troca de mensagens entre provador e verificador, este tipo de ZKP é relevante para cenários nos quais a troca direta de mensagens não é adequada ou viável, como em

blockchain. A figura 6 apresenta as etapas de uma prova de conhecimento zero.

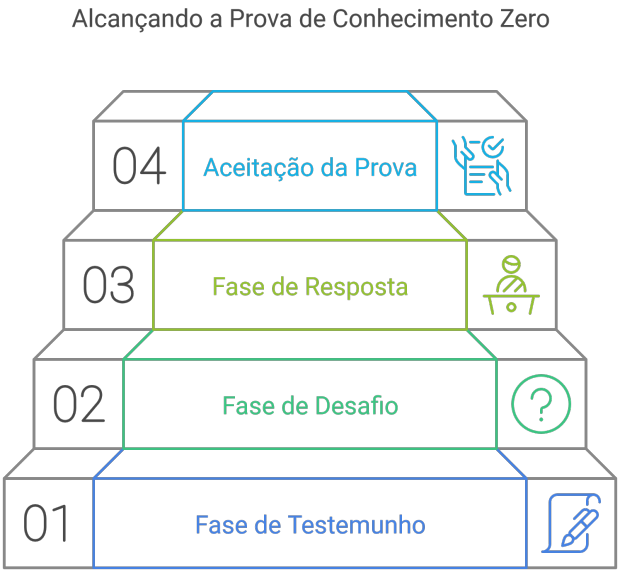

Figura 6: Fases de prova de conhecimento zero

a) **Zero-Knowledge Succint Non-Interactive Argument of Knowledge (zk-SNARKs)**

zk-Snarks são mecanismos de prova de conhecimento zero utilizados em contextos que de comunicação sincronização entre prover e verifier. As zk-SNARKs possuem a vantagem de criar provas pequenas que são computacionalmente rápidas para serem verificadas e utilizam criptografia de curvas elípticas, o ponto negativo é a necessidade de um setup inicial entre prover e verifier, o que torna necessário certo nível de confiança entre os atores, entretanto em blockchains as SNARKs foram adaptadas para que o procedimento de setup seja realizado entre atores não confiáveis (CAPKO; VUKMIROVIĆ; NEDIĆ, 2022) (THIBAULT; SARRY; HAFID, 2022). A Figura 7 apresenta uma visão geral de zk-SNARKs

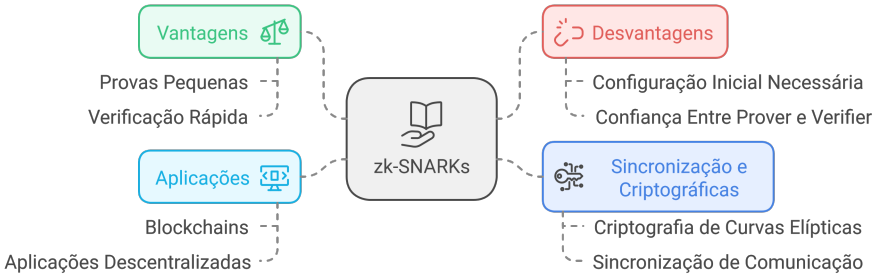

Figura 7: Visão geral zk-SNARKs

b) **Zero-Knowledge Scalable Transparent Argument of Knowledge (zk-STARKs)**

zk-STARKS são mecanismos de prova de conhecimento zero que utilizam como mecanismos criptográficos funções de resumo ou funções Hash, como o keccak-256. Este mecanismo não necessita de setup inicial e as provas são transparentes, o que as torna adequadas para utilização em blockchains e aplicações descentralizadas em que a confiabilidade está distribuída entre os participantes. As STARKs utilizam técnicas e conceitos matemáticos diferentes das SNARKs, tais como interpolação polinomial e criptografia baseada em reticulados (lattice) e implementam correções de erros. Uma vantagem das STARKs é sua resistência a computadores

quânticos, diferentemente das SNARKs, que utilizam como princípio matemático o problema do logaritmo discreto e, assim, são suscetíveis a ataques quânticos. Entretanto, o aspecto negativo das STARKs é que as provas são maiores que as provas das SNARKs, sendo, portanto, menos eficientes computacionalmente (ZHOU et al., 2024) (CAPKO; VUKMIROVIĆ; NEDIĆ, 2022). A Figura 8 apresenta os principais aspectos de provas de conhecimento zero STARKs.

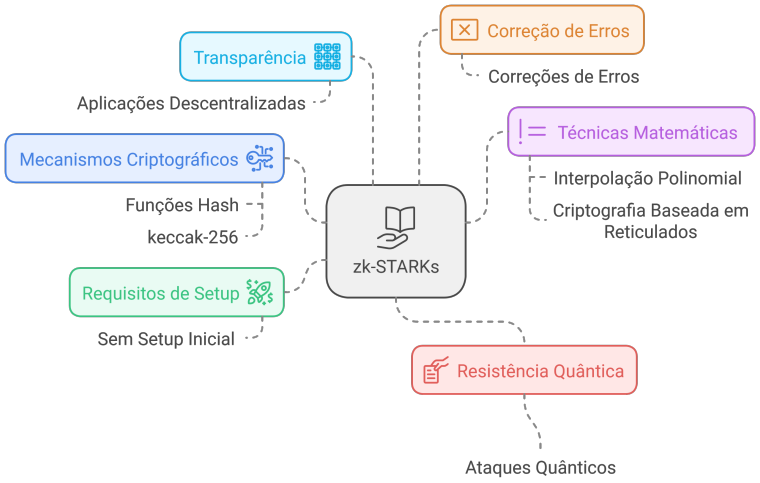

Figura 8: Visão geral de zk-STARKs

4.7.2 Premissas de Segurança em IDD

Existem algumas premissas para que as Identidades dos usuários sejam utilizadas de maneira segura e confiável, garantindo que quem está utilizando a credencial é de fato o usuário dono dos dados, e estes dados não serão vazados ou utilizados de maneira indevida. As premissas não são exaustivas, e conforme a evolução da utilização de IDD podem surgir novas premissas para garantir a segurança e privacidade dos usuários (SOLTANI; NGUYEN; AN, 2021)

1. Controle: Usuários devem possuir o controle para gerenciar os dados de sua identidade da forma que desejarem.
2. Acesso: Usuários devem ter acesso aos próprios dados de forma que não deve haver impedimentos ou filtros em relação aos dados do usuário sem prévio consentimento.
3. Transparência: O tratamento dos dados dos usuários por sistemas deve permitir transparência ou visibilidade dos processos para os donos dos dados, de forma que os usuários tenham conhecimento de finalidade, e operações que estão sendo realizadas com seus dados.
4. Persistência: Identidades digitais descentralizadas devem possuir longevidade e persistência até o momento em que explicitamente sejam desativadas pelo dono da credencial.
5. Portabilidade: Os donos de credenciais devem ser capazes de conseguir portar ou mover suas credenciais de um serviço de identidade para outro, incluindo mover de localidade ou país, de forma que seja possível utilizar a mesma credencial independente da jurisdição ou barreiras legais de forma a garantir a durabilidade e disponibilidade de dos atributos de identidade, além de garantir flexibilidade para os usuários e a liberdade de escolher serviços de identidade com os quais poderão interagir.

4.7.3 Ataques em IDD

Ataques de segurança em Identidades Digitais Descentralizadas (IDD) representam um desafio crescente na era digital. Alguns dos principais tipos de ataques incluem:

4.3.2.1 Ataque de roubo de dados e identidade

Os riscos de privacidade relacionados às aplicações de identidade digital descentralizada envolvem aspectos de vazamento de dados, acesso não-autorizado, não revogado de dados, ataque sybil de identidade em carteiras.

Dados de Identidade Digital Descentralizada (IDD) estão suscetíveis a ataques de diferentes formas, desta maneira, é importante garantir que em todas as etapas de utilização de uma identidade seja garantido a segurança e privacidade dos dados. Um dos principais alvos de ataque em IDD são as carteiras dos usuários de credenciais, pois de modo geral os dispositivos dos usuários possuem relativamente menor segurança e são mais propensos a sucesso em casos de ataque. Por este motivo, a segurança e a privacidade dos dados dos usuários podem estar em risco. Roubo de identidade acontece quando um atacante acessa dados da carteira do usuário para então realizar diversas operações não-autorizadas.

Problemas na infraestrutura da rede blockchain ou vulnerabilidades no mecanismo de autenticação podem permitir que um agente malicioso acesse diretamente dados ou credenciais das carteiras dos usuários.

Outra forma de ataque ocorre utilizando a arquitetura e funcionalidades de IDD para captura de dados no processo de verificação de credenciais utilizando o ataque de aumento de credenciais. Este ataque ocorre quando um verificador malicioso ou verificador confiável, que foi atacado solicita informações a mais no processo de verificação para obter dados do usuário. Outra forma de realizar este ataque ocorre realizando verificações repetidas do usuário com intuito de obter dados suficientes para encontrar o usuário alvo com base nas informações fornecidas. A Tabela 1 apresenta os vetores de ataque e como funcionam (NAIK; GRACE; JENKINS, 2021).

Tabela 1: Ataque de roubo de dados e identidade (NAIK; GRACE; JENKINS, 2021).

Vetor de Ataque	Descrição
Acesso não-autorizado a carteira do usuário	Atacante ou stakeholder acessa a carteira ou dados da carteira de maneira não-autorizada. Pode ocorrer do usuário conceder acesso a suas credenciais sem conceber o risco envolvido.
Coleta por modificação de verificação.	Um verificador comprometido pode requisitar mais informações do usuário que o necessário, através de rodadas de verificação e com mais informações é possível detectar o usuário na rede, obter dados sensíveis e possivelmente estender a credencial utilizando um emissor com segurança comprometida.
Ataque aos Dados em Plano de fundo	Atacante pode utilizar dados em plano de fundo e combinar com dados apresentados pelo usuário no processo de verificação de credenciais com intuito de identificar o usuário utilizando dados de segundo plano com objetivo de vincular pseudônimos. A diferença deste ataque para o anterior é que neste não há requisição adicional de dados.

4.3.2.2 Técnicas de ataque de credenciais falsas

Existem diversos vetores de ataque que exploram vulnerabilidades com intuito de obter identidades falsas. Um atacante pode falsificar um agente emissor (Issuer) na rede sem que haja a verificação adequada deste emissor falso. O vetor de ataque pode ocorrer de duas maneiras, primeiramente um ataque a infraestrutura de rede no qual seja possível roubar credenciais administrativas (p.ex:chaves privadas) para que seja possível realizar uma nova assinatura de identidade usando a chave furtada. Outra maneira de realizar o ataque é através de conexão eclipse, na qual nós maliciosos atuam como

man-in-the-middle do emissor verdadeiro e os usuários. Neste ataque as conexões direcionadas para o agente emissor são transferidas primeiramente para o nós maliciosos que manipulam os dados de forma que as informações armazenadas na ledger são os dados inseridos pelos nós maliciosos (NAIK; GRACE; JENKINS, 2021). A Tabela 2 apresenta os ataques de credenciais falsas.

Tabela 2: Técnicas de ataque de credenciais falsas (NAIK; GRACE; JENKINS, 2021).

Vetor de Ataque	Descrição
Criação de credenciais falsas no Issuer	Um atacante pode, com ajuda de outras técnicas de ataque, realizar a criação de identidades falsas de usuário ou fazer a rede reconhecê-lo como emissor verdadeira e a partir de então realizar emissão de diversas credenciais falsas.
Falsificação de emissor	Um atacante pode realizar ataque de eclipse no emissor, fazendo com que todos os dados transferidos ao emissor sejam primeiramente enviados ao atacante que age como emissor, o atacante recebe os dados, realiza tratamento malicioso e envia para o emissor verdadeiro, tendo acesso e podendo criar uma credencial falsa. Outra maneira é um atacante criar um agente falso e conectar-se com o emissor, conforme dados são trafegados o agente falso consegue criar uma credencial falsa para agir na infraestrutura de IDD.
Alteração(amend) de credencial emitida	Um atacante pode obter a chave privada, em seguida realizar alteração de credenciais e assinar com a chave privada furtada..

4.3.2.3 Ataque de Negação de Serviço

Ataques de negação de serviço podem ser realizados contra os usuários de credenciais (holders), emissores de credenciais (issuers), verificadores (verifiers) ou validadores blockchain através de um fluxo intenso de tráfego de pacotes de rede com intuito de esgotar os recursos de processamento de um ou participante da rede. Usuários de credenciais podem estar mais vulneráveis a este tipo de ataque pois de modo geral seus equipamentos possuem menos recursos de processamento e não são preparados para combater esta forma de ataque. Os vetores de ataque de negação de serviço podem ser aplicados em algum participante da rede causando esgotamento de recursos, por exemplo nos validadores, para causar fila e congestionamento de transações na *blockchain* (NAIK; GRACE; JENKINS, 2021). A Tabela 3 apresenta os vetores de ataque de negação de serviço.

Tabela 3: Ataques de negação de serviço (NAIK; GRACE; JENKINS, 2021).

Vetor de Ataque	Descrição
Negação de serviço ao host	Um atacante pode realizar inundação de requisição ao emissor, verificador ou dispositivo do usuário, inviabilizando que o dispositivo em ataque realize operações na rede
Negação de serviço na infraestrutura blockchain	O ataque de DoS na blockchain é realizado inundando os nós de infraestrutura blockchain para esgotar os recursos e não permitir que novas transações sejam realizadas.
Interrupção de serviços de IDD	Interrupções de serviços de IDD podem ocorrer de diversas formas, incluindo ataques de negação de serviço. As outras maneiras podem ser: inclusão de validador falso, quebra de regras de governança e número insuficiente de validadores.

4.7.4 Avaliação de Risco e Mitigação

Tabela 4: Avaliação e mitigação de risco para ataque de roubo de dados e identidade (NAIK; GRACE; JENKINS, 2021).

Vetor de ataque	Risco	Mitigação
Acesso não-autorizado a carteira do usuário	Médio	Utilizar autenticação multifatorial (MFA), bem como controle de acesso para restringir acessos a carteira. Realizar atualização frequentemente no software de carteira, utilizar criptografia em todas as etapas de utilização da carteira, impedir interação da carteira com aplicações de terceiros não-autorizados e limitar privilégios de acesso da carteira a infraestrutura de IDD quando o acesso estiver ocorrendo a partir de redes públicas ou desconhecidas.
Coleta por modificação de verificação	Médio	Implementar políticas na rede de IDD limitando aos verificadores acesso ao mínimo de informação dos usuários, padronizar processo de verificação de identidade para todos os verificadores, tornar o procedimento de verificação transparente para o usuário de forma que seja possível a suspeita de ações indesejadas de verificadores, implementar votação e limiar de aprovação de verificadores quando um destes requisitar mais informações dos usuários.
Ataque aos Dados em Plano de fundo	Médio	Implementar políticas para limitar o acesso dos verificadores ao mínimo de informações possíveis dos usuários, padronizar o processo de verificação e torná-los públicos e conhecidos aos usuários.

Tabela 5: Avaliação e mitigação de risco para ataque de credenciais falsas (NAIK; GRACE; JENKINS, 2021).

Vetor de ataque	Risco	Mitigação
Criação de credenciais falsas no Issuer	Médio	Utilizar autenticação multifatorial (MFA), bem como controle de acesso para restringir acessos a carteira. Realizar atualização frequentemente no software de carteira, utilizar criptografia em todas as etapas de utilização da carteira, impedir interação da carteira com aplicações de terceiros não-autorizados e limitar privilégios de acesso da carteira a infraestrutura de IDD quando o acesso estiver ocorrendo a partir de redes públicas ou desconhecidas.
Falsificação de emissor	Médio	Implementar políticas na rede de IDD limitando aos verificadores acesso ao mínimo de informação dos usuários, padronizar processo de verificação de identidade para todos os verificadores, tornar o procedimento de verificação transparente para o usuário de forma que seja possível a suspeita de ações indesejadas de verificadores, implementar votação e limiar de aprovação de verificadores quando um destes requisitar mais informações dos usuários.
Alteração(amend) de credencial emitida	Médio	Implementar políticas para limitar o acesso dos verificadores ao mínimo de informações possíveis dos usuários, padronizar o processo de verificação e torná-los públicos e conhecidos aos usuários.

Tabela 6: Avaliação e mitigação de risco para ataque de negação de serviço (NAIK; GRACE; JENKINS, 2021).

Vetor de ataque	Risco	Mitigação
Negação de serviço ao Host	Médio	Monitoramento dos serviços e alertas para ataques de negação de Serviço, utilizar firewall, utilizar blackhole routing.
DoS na Blockchain	Médio	Utilizar mecanismos de consenso com rigoroso processo de confiança e validação de blocos, monitoramento de blocos órfãos, utilizar mecanismo de pontuação de confiança de participantes da rede, utilizar mecanismo de punição de ações suspeitas na rede.
Interrupção de serviços de IDD	Médio	Implementar observabilidade e monitoramento de comportamentos suspeitos na rede, implementar mecanismos de proteção contra ataques de negação de serviço no provider, implementar políticas estritas de autorização e acesso.

4.7.5 Agentes pessoais (*Personal Agents*)

Os agentes pessoais são softwares que usam tecnologias de reconhecimento de fala, processamento de linguagem natural (PLN), inteligência artificial (IA) e aprendizado de máquina para entender e responder a comandos de usuários. Eles podem executar uma variedade de tarefas, desde fornecer informações e realizar ações específicas até controlar dispositivos conectados em uma

casa inteligente (YEUNG et al., 2023). A aplicação destes vai além do cenário clássico de assistente pessoal, sendo capaz de executar tarefas mais complexas em ambientes diversos como descritos nas subseções abaixo.

4.7.6 IDD e *Personal Agents for things*

A identidade digital descentralizada pode ser aplicada aos mais diversos cenários como meio de alcançar confiança. De tal forma, ao aplicar IDD no ambiente de *Personal Agents* para "coisas" é possível garantir tanto a integridade das mensagens quanto prover um mecanismo seguro de compartilhamento de dados. Isto é, usando identificadores descentralizados para identificar dispositivos permite a criação de políticas de compartilhamento e soberania sobre as informações produzidas. Além disso, também é viável a tomada de decisões automatizadas por parte dos agentes, com base em suas percepções e papéis (YU et al., 2021).

4.7.7 IDD e segurança em *Personal Agents*

Agentes pessoais podem executar tarefas de maneira autônoma que antes exigia a presença ou execução pessoal, a ação dos agentes permite ganho de tempo, velocidade de execução e autonomia. Embora a utilização de agentes pessoais apresenta vantagens, existem aspectos de segurança e privacidade que precisam ser abordados. Um dos primeiros aspectos está relacionado a privacidade dos dados de usuário, os agentes necessitam de contexto e uma quantidade significativa de dados do usuário para realizar as operações, desta forma, é necessário garantir que os dados não sejam vazados do agente, tampouco que o agente realize transmissão de informações sensíveis a terceiros. Outro ponto importante é a necessidade de proteger o agente de vulnerabilidades e ataques, pois caso um atacante consiga explorar vulnerabilidades pode ocorrer vazamento de grande quantidade de informações sensíveis dos usuários (SAMI et al., 2024).

4.7.8 IDD e *Personal Agents* for People

A combinação de identidade digital descentralizada (IDD) e agents People fornecem um paradigma avançado para gerenciar e usar identidades digitais em um ambiente cada vez mais conectado e automatizado. Esta integração foi projetada para aumentar a privacidade, segurança e autonomia do usuário, ao mesmo tempo que promove interações personalizadas e eficientes com serviços digitais.

Primeiro, é importante entender os conceitos e detalhes de cada tema, como o que são identidades digitais descentralizadas (IDDs), são sistemas que permitem aos usuários controlar e gerenciar sua própria identidade sem depender de uma autoridade central. Esses sistemas são baseados em tecnologias como blockchain e garantem que os usuários possam comprovar a autenticidade de suas identidades e credenciais de forma segura e verificável.

Personal Agents for People, são programas de software ou sistemas de IA que agem como assistentes digitais pessoais, ajudando os usuários a gerenciar suas interações digitais. Esses agentes podem realizar tarefas variadas, desde agendar compromissos até gerenciar e-mails e interagir com outros sistemas digitais em nome do usuário.

Baseado nas pesquisas e como os estudos caminham, chegamos em alguns pontos em comum e como IDD e *Personal Agents* se complementam:

- Autonomia e Controle:

1. IDD: Proporciona aos usuários controle total sobre suas identidades e dados associados.
2. *Personal Agents*: Utilizam esse controle para agir eficientemente em nome dos usuários, acessando serviços e realizando transações conforme as preferências e permissões pré-definidas pelo usuário.

- Privacidade e Segurança:

1. IDD: Assegura que os dados pessoais são armazenados de forma segura e compartilhados apenas sob consentimento explícito do usuário.
2. *Personal Agents*: Podem gerenciar dinamicamente as permissões de acesso a dados, ajustando-as conforme as necessidades e preferências do usuário, e negociando a privacidade com terceiros.

- Interoperabilidade e Integração:

1. IDD: Facilita a interoperabilidade entre diferentes plataformas e serviços, utilizando padrões abertos e descentralizados para a gestão de identidades.
2. *Personal Agents*: Aproveitam essa interoperabilidade para integrar-se e comunicar-se com uma variedade de sistemas e serviços, promovendo uma experiência de usuário fluida e personalizada.

- Automatização de Processos:

1. *Personal Agents*: Podem automatizar rotinas e decisões com base nas preferências do usuário e nas informações acessíveis através da IDD.
2. IDD: Fornece a infraestrutura segura e confiável necessária para que essas automações ocorram sem riscos para a privacidade ou segurança do usuário.

- Serviços Personalizados:

1. *Personal Agents*: Adaptam os serviços e interações ao perfil e necessidades do usuário, desde recomendações personalizadas até ajustes automáticos em configurações de privacidade.
2. IDD: Garante que todos os dados utilizados para personalizar esses serviços sejam geridos de forma transparente e sob o controle do usuário.

A interação entre Identidade Digital Descentralizada e *Personal Agents* for People representa uma evolução significativa na maneira como os usuários interagem com o mundo digital. Isso não apenas fortalece a privacidade e a segurança, mas também melhora a conveniência e a eficácia das interações digitais, proporcionando uma experiência verdadeiramente personalizada e automatizada. Essa integração é um passo importante para um futuro digital mais seguro, privado e centrado no usuário.

4.8 Hyperledger Anoncreds

AnonCreds é um projeto Hyperledger que permite credenciais verificáveis com privacidade aprimorada. A tecnologia em si não é nova, pois originalmente fazia parte do Hyperledger Indy, o projeto de registro de identidade digital. No entanto, agora ele foi separado do Indy para poder ser usado para credenciais verificáveis em ledgers como Hyperledger Fabric ou Hyperledger Besu baseado em Ethereum, ou outros.

O conceito central que sustenta AnonCreds, Indy e Project Aries é permitir que os usuários compartilhem dados de identidade com outras pessoas, mas apenas quando necessário. Por exemplo, em um bar, alguém pode provar que tem idade para beber e talvez compartilhar uma foto vinculada à credencial sem revelar seu nome e endereço.

AnonCreds, que significa Anonymous Credentials, usa criptografia Zero Knowledge Proof (ZKP) para permitir esses tipos de divulgações seletivas. O conceito pode funcionar bem para algumas aplicações e talvez menos para outras. Se um processo financeiro envolver a conformidade com o seu cliente, pode ser necessário compartilhar alguns dados e, certamente, seu nome.

No âmbito de identidade digital, o AnonCreds tem atraído um pouco de polêmica. AnonCreds é anterior ao padrão de credenciais verificáveis do W3C e não cumpre totalmente. Ele também usa criptografia que não é aprovada pelo NIST. O fato de haver 25 patrocinadores de projetos demonstra a extensão de seu apoio. Ao mesmo tempo, o projeto AnonCreds parece disposto a revisitar o esquema de assinatura digital e, no futuro, apoiar a apresentação de credenciais usando o modelo de dados W3C.

4.8.1 Motivação

A motivação para criar o Hyperledger AnonCreds é extrair uma importante tecnologia de credencial verificável que protege a privacidade de ser explicitamente vinculada ao Hyperledger Indy e permitir seu uso com qualquer registro de dados verificável (VDR) apropriado. Embora o Hyperledger Indy seja uma boa plataforma para compartilhar objetos AnonCreds, não é a única, e essa transição do AnonCreds para um projeto autônomo permite que usuários investidos em outras plataformas de armazenamento distribuído usem AnonCreds.

AnonCreds é importante porque se baseia em vários recursos importantes de proteção de privacidade baseados em ZKP que não estão atualmente disponíveis com outros tipos de credenciais verificáveis. Esses incluem:

O ato de apresentar reivindicações de credenciais verificáveis pelo sistema AnonCreds não expõe identificadores correlativos do titular. Isso é particularmente importante para alguns governos, ao significar que o uso de credenciais verificáveis pelo sistema não requer introduzir um novo identificador para indivíduos, evitando assim a sobrecarga legislativa correspondente. A não correlação das apresentações dos titulares para os verificadores atende às crescentes exigências globais de regulamentação de privacidade, como o GDPR.

O sistema AnonCreds apóia a noção de um “segredo de link” baseado em ZKP, que permite a vinculação de credenciais emitidas a um titular e a vinculação de várias credenciais apresentadas juntas ao mesmo segredo/proprietário do link.

Esse sistema permite a minimização do compartilhamento de dados, suportando tanto a divulgação seletiva (compartilhando apenas algumas declarações em uma credencial) quanto os predicados ZKP (comprovando uma expressão baseada em declaração, como “Tenho mais de 21 anos” com base na data de nascimento sem ter de compartilhar a data de nascimento).

A apresentação verificável pelo sistema pode incluir reivindicações derivadas de credenciais verificáveis de várias fontes, com uma vinculação provando que as credenciais foram todas emitidas para o mesmo titular. As apresentações verificáveis utilizando o sistema AnonCreds são derivadas de suas credenciais verificáveis de origem, garantindo que o titular não esteja fornecendo ao verificador sua credencial verificável bruta/original.

Ao separar o sistema AnonCreds de Indy, é permitida uma adoção mais ampla, pois os grupos que consideram seu uso não estariam limitados a uma implementação baseada em Indy. Com uma base de usuários mais ampla, surge um interesse adicional na evolução do sistema, e esperamos ver como resultado um interesse maior de criptógrafos aplicados. Embora muitos tenham implantado com sucesso soluções baseadas no sistema ao redor do mundo, ele não é uma solução perfeita e precisa continuar a evoluir. A revogação no sistema atual é menos do que ideal. Outros esquemas de assinatura prometem versões “melhores e mais rápidas” do sistema. Com o AnonCreds como um projeto autônomo, os esforços na próxima geração serão focados. Tais evoluções devem manter os recursos de proteção de privacidade do sistema, como não correlação, divulgação seletiva, predicados

e vinculabilidade.

As principais características que fazem o sistema AnonCreds existir podem ser definidas em dois níveis distintos:

- Nível *ledger*: O que deve ser escrito em um registro de dados verificável para o sistema funcionar na prática.
- Nível de credencial e SDK: Quais técnicas criptográficas devem ser empregadas em um SDK para fornecer ao sistema seus recursos de preservação de privacidade.

Para a pilha *AnonCreds* existente, no *Hyperledger Indy*, esses dois níveis podem ser representados pela Figura 9.

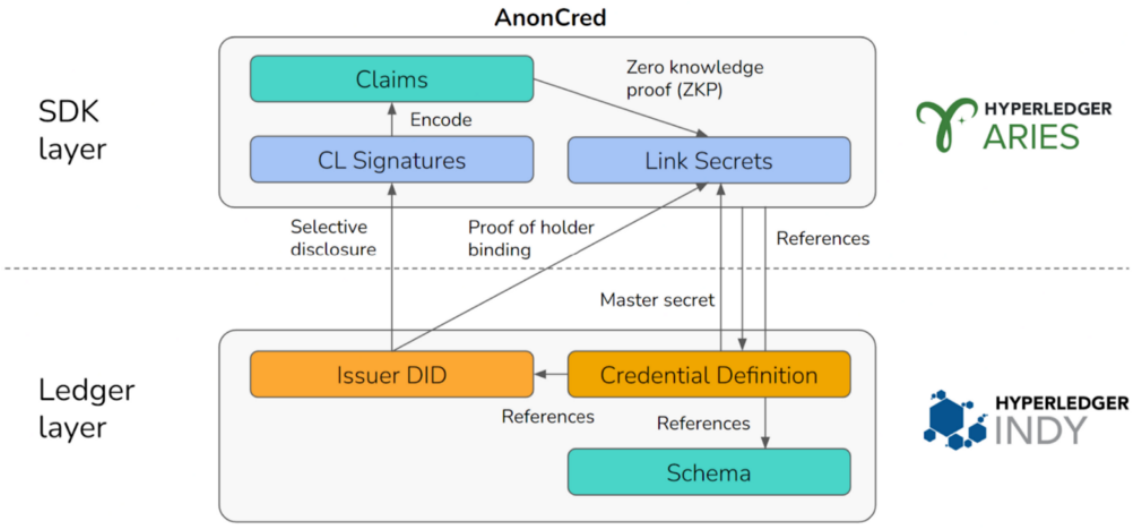

Figura 9: Pilha do AnonCreds

Aqui, o *Hyperledger Indy* é importante para oferecer suporte a *AnonCreds*, pois até o momento é o único blockchain de identidade que pode oferecer suporte nativo a transações de DIDs, esquemas, definições de credenciais (e registro de revogação opcional) gravadas no livro-razão.

Os *AnonCreds* podem ser apresentados no formato padrão W3C VC *Data Model*, e as próximas etapas para o modelo incluem alcançar a conformidade com o W3C *Verifiable Credentials Data Model Standard* (SEDLMEIR et al., 2021).

4.8.2 Arquitetura

A seguir, mostramos como o componente AnonCreds irá interagir com os diversos componentes de um Agente SSI, o serviço de gerenciamento de chaves para um Agente, outros Agentes e Registros de Dados Verificáveis (VDRs) (SHCHERBAKOV, 2024). Observe os métodos AnonCreds *Registrar* e *Resolver* que definem o comportamento de gravação e leitura de AnonCreds para um VDR específico segundo a Figura 10.

A arquitetura *"to-be"* é conceitualmente semelhante ao que temos hoje com o Hyperledger Indy, estendida separando AnonCreds em sua própria biblioteca e formalizando APIs independentes de razão entre AnonCreds e os métodos *Registrar*/*Resolver*. Conforme indicado pelo número de implementações independentes já criadas usando as bibliotecas AnonCreds existentes, o ajuste das APIs é um esforço relativamente pequeno. É claro que, com a implementação de APIs de registrador/resolvedor, fica muito mais fácil usar VDRs além do Indy, especialmente para casos de

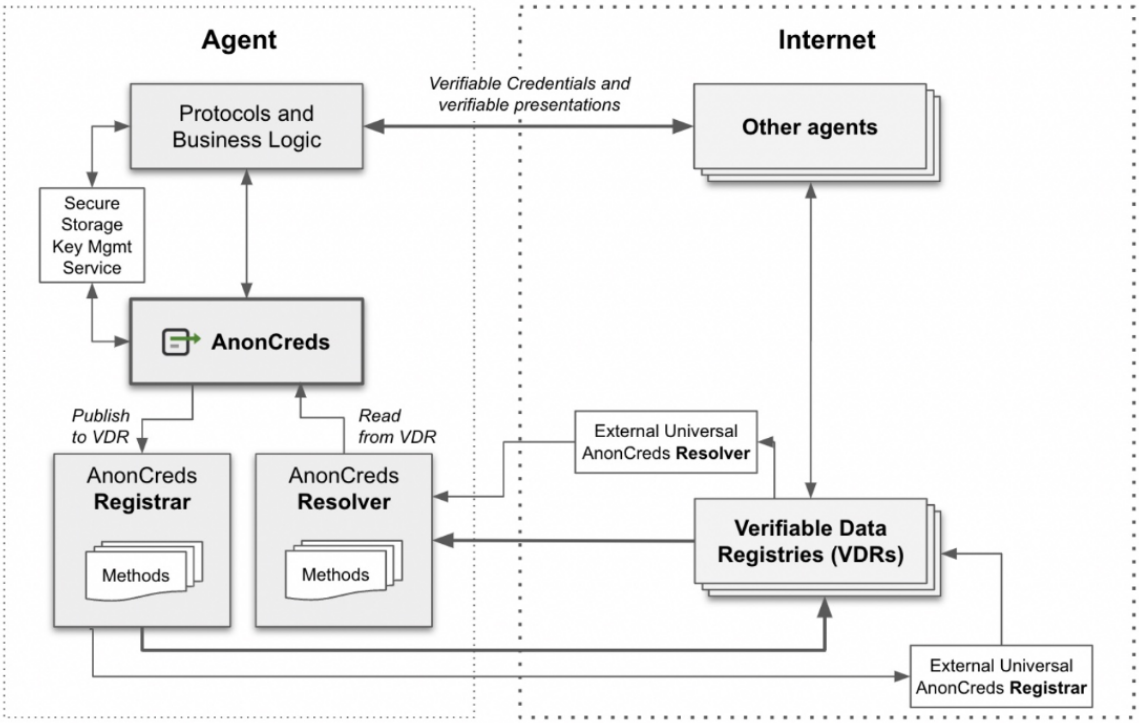

Figura 10: Agentes e Registros de Dados Verificáveis (VDRs)

uso somente de resolvedor (titular e verificador) (SHCHERBAKOV, 2024). Além de uma mudança nas dependências dentro do Aries Frameworks, deve haver pouco ou nenhum impacto no uso de AnonCreds pelas implementações existentes. A comunidade mais ampla e o subsequente foco mais amplo no AnonCreds *"Next"* trarão melhorias significativas nas capacidades, especialmente nas áreas de revogação e esquemas de assinatura adicionais que retêm os recursos do AnonCreds.

4.9 Fontes utilizadas

Como forma de embasamento das pesquisas e do estado da arte relacionado a prospecção, foi realizado um estudo da arte considerando os últimos 5 anos de publicações. Como base de indexação foram escolhidas a IEEE, ACM e Scopus, considerando algumas palavras-chave como "IA and Blockchain and Multiagent and Self-Sovereign Identity", e dentro desse contexto tivemos alguns retornos que julgamos pertinentes como: (CHAVALI; KHATRI; HOSSAIN, 2020; SALAH et al., 2019; VOS; ISHMAEV; POUWELSE, 2020; STOKKINK; POUWELSE, 2018; PFEIFFER; BUGEJA, 2021; SHAGUN et al., 2023).

5 Casos de Uso Relevantes

Os casos de uso relevantes em Identidades Digitais Descentralizadas (IDD) abrangem uma variedade de setores, cada um beneficiando-se das características únicas de segurança, privacidade e autossoberana. Aqui estão alguns dos principais casos de uso:

5.1 Desafio IDD

A Identidade Digital Descentralizada (IDD) é uma plataforma para a infraestrutura de aplicações de identidade digital, contendo um conjunto de APIs para a definição, emissão e autenticação de credenciais armazenadas em uma carteira digital. Fornece uma autenticação digital segura e confiável por meio de credenciais verificáveis em blockchain.

O SOU iD é a carteira digital da plataforma de identidade descentralizada que faz parte do ecossistema do CPQD. Com o SOU iD os dados são armazenados no formato de credenciais digitais reutilizáveis que são emitidas por entidades de confiança e que garantem a legitimidade da informação. Isso possibilita a validação instantânea das informações e reduz fraudes, tudo com total respeito à Lei Geral de Proteção de Dados (LGPD).

Para a primeira implementação da aplicação SOU iD, escolhemos participar do workshop WRNP, promovido pela Rede Nacional de Ensino e Pesquisa (RNP), no contexto do Simpósio Brasileiro de Redes de Computadores (SBRC). Este workshop, organizado pela RNP em colaboração com o SBRC, é parte de um evento científico anual realizado pela Sociedade Brasileira de Computação (SBC) em parceria com o Laboratório de Redes de Computadores (LARC). A esta implementação deu-se o nome de Desafio IDD.

O Workshop RNP (WRNP) é um evento de referência para a comunidade acadêmica, com o objetivo de aproximar o público dos avanços tecnológicos e dos principais tópicos em discussão na área de Pesquisa e Desenvolvimento em Tecnologias de Informação e Comunicação (TIC), tanto no Brasil quanto no exterior.

O evento oferece uma oportunidade única através de uma feira com expositores, patrocinadores e gamificação, na qual os participantes que visitam os estandes concorrem a um prêmio de maneira interativa. Cada expositor disponibiliza adesivos aos visitantes, os quais são colecionados em uma "cartelinha". Ao completar essa cartela, o visitante tem a chance de participar de um sorteio e ganhar prêmios.

A jornada de gamificação e premiação do evento era realizada de forma muito manual, o que não condiz com um workshop de tecnologia. Existe uma oportunidade não aproveitada de aplicar a digitalização do evento e educar visitantes e organizadores sobre conceitos de IDD.

Identificamos uma oportunidade nessa dinâmica para modernizar a gamificação do processo de premiação do WRNP, utilizando credenciais verificáveis para educar visitantes e organizadores sobre os conceitos da nova tecnologia IDD de maneira prática. Cada participante teria uma carteira digital, enquanto cada expositor possuiria um QR code exclusivo. O visitante capturaria esse QR code, armazenando-o em sua carteira digital como uma credencial verificável. Com diversas credenciais de diferentes estandes em sua carteira digital, o participante poderia emitir sua "credencial da sorte"para a premiação de forma simplificada.

O detalhamento do desenvolvimento deste caso de uso está descrito no relatório da atividade A5.3. No anexo A deste documento constam fotos do evento realizado em Niterói/RJ, nos dias 20 e 21 de Maio de 2024.

5.2 Desafios da IDD relacionados à experiência de usuário

Com base no que foi observado no caso de uso supracitado (Desafio IDD), podemos afirmar que a Identidade Digital Descentralizada proporciona grandes avanços na prevenção de violação de dados, fraudes de identidade e perda de privacidade decorrentes da falta de segurança e controle dos modelos centralizados de identidade digital. Contudo, apesar das oportunidades de proteção de dados e do potencial de transformação digital da IDD em diversos setores, faz-se necessário analisar de forma crítica os desafios para tornar a tecnologia acessível, segura e fácil de usar para sua adoção independente do nível de familiaridade do público com a tecnologia (SOUZA et al., 2022).

Apesar do foco predominante das pesquisas atuais em Identidade Digital Auto Soberana (SSI) se voltarem nos aspectos técnicos de segurança e privacidade, a Experiência do Usuário (UX) representa um fator igualmente determinante para a adoção de qualquer tecnologia. Os conceitos de SSI, sofisticados e complexos, muitas vezes não se alinham com o modelo mental dos usuários finais (SOUZA et al., 2022; KHAYRETDINOVA et al., 2022), ou seja, suas interfaces e processos podem estar distantes dos padrões de uso e jornadas habituais dos serviços, produtos e aplicações com as quais

estes usuários estão familiarizados, criando barreiras para a adoção.

A adoção de uma nova tecnologia depende de diversos fatores, como conhecimento prévio dos usuários, facilidade de uso, custo e disponibilidade. Para um sistema descentralizado de gestão de Identidades Digitais, o principal obstáculo é sua complexidade. Superar o modelo dos sistemas centralizados, onde as interações são intermediadas por uma terceira parte, será um grande desafio (DIB; TOUMI, 2020).

5.2.1 Comportamento de usuários e usabilidade

O comportamento dos usuários é um fator relevante no desenvolvimento de sistemas de IDD, uma vez que soluções com fluxos e jornadas muito complicadas podem comprometer significativamente sua adoção. Usuários frequentemente buscam alternativas mais convenientes, mesmo que isso coloque em risco sua privacidade e segurança, ainda que as preocupações com estes aspectos estejam crescendo (DIB; TOUMI, 2020).

Para os usuários poderem gerenciar sua identidade digital sem dependências de terceiros centralizadores de dados, é necessária sua compreensão e capacitação na tecnologia. Alguns dos principais problemas para a experiência são:

- Os conceitos e fluxos da interface não se encaixam nos modelos mentais com os quais os usuários estão familiarizados.
- As ferramentas oferecem ações como obter, gerenciar e proteger chaves privadas, senhas, credenciais, entre outras, que são complexas de serem executadas e/ou não são apresentadas de forma clara, podendo ser realizadas incorretamente.
- O status de desenvolvimento das soluções no mercado frequentemente não corresponde ao que é anunciado, com funcionalidades essenciais muitas vezes ausentes; essa disparidade entre a promessa e o desempenho real pode prejudicar a reputação das soluções de IDD.

5.2.2 Percepção de valor

Um dos grandes benefícios apresentados em favor dos sistemas de IDD é colocar os usuários no controle de suas identidades. No entanto, este benefício apresenta uma maior responsabilidade e mais esforço por parte desses usuários para gerenciar e utilizar essas identidades e credenciais.

É necessário considerar que a abordagem da gestão de IDD e os princípios de Identidade Auto Soberana não foram inicialmente fundamentados em estudos empíricos relacionados à necessidade dos usuários, e existem incertezas com relação a se os usuários realmente desejam ter tanto controle sobre seus dados de identidade em interações digitais. Segundo resultados de estudos sobre gestão de identidade na web (ROSSNAGEL et al., 2014), usuários preferem sistemas simples, onde intermediários tomam conta de seus dados.

Os aspectos técnicos, mesmo associados aos benefícios citados de proteção de segurança e privacidade, não são suficientes para a difusão e adoção de novas tecnologias, é argumentado que para o sucesso de um produto no mercado é necessário considerar aspectos multidisciplinares e socioeconômicos, que muitas vezes são negligenciados (KHAYRETDINOVA et al., 2022).

Exigir uma interação complexa sem oferecer benefícios claros para além da maior proteção à privacidade é um obstáculo, visto que muitos usuários não conseguem avaliar pessoalmente a eficácia dessa proteção - o que leva a uma situação descrita por (KHAYRETDINOVA et al., 2022) como “mercado de limões”, cenário onde os consumidores não conseguem diferenciar produtos de alta e baixa qualidade. Sem considerar a importância de comunicar adequadamente o valor de uma nova tecnologia, ela pode se tornar menos atraente para esses usuários, levando a uma menor adoção. O benefício percebido de mais controle do usuário e mais privacidade precisa superar as desvantagens,

como maior esforço para gerenciar as credenciais, maior responsabilidade para proteger o dispositivo utilizado, backup mais complicado em caso de perda de credenciais e, no estado atual, falta de maturidade e problemas de experiência na usabilidade.

5.2.3 Acessibilidade

Um sistema de gestão de identidades não pode excluir ou impedir pessoas de participar do seu ecossistema independente de suas habilidades ou deficiências (VOLKOV, 2020). O papel da acessibilidade no desenvolvimento de produtos digitais não deve ser abordado apenas como uma exigência técnica e/ou legal, mas como um elemento essencial e estratégico para garantir o acesso universal para que a solução seja amplamente adotada por uma base diversificada de usuários.

Além de garantir a conformidade com a legislação e regulamentações vigentes, a acessibilidade também resulta em melhorias na usabilidade e na experiência do usuário, uma vez que designs acessíveis resultam em produtos mais intuitivos e fáceis de utilizar para todos os usuários.

5.2.4 Escalabilidade

Para ter sucesso no mercado, a solução precisa atrair um grande número de usuários e partes interessadas - emissores, verificadores, apresentando vantagens e benefícios maiores do que as soluções concorrentes. A escalabilidade necessária para alcançar uma ampla base de usuários não depende apenas das especificações técnicas, mas também deve resultar de uma excelente experiência voltada para o cliente. Para que obtenham sucesso e avancem na Curva de Adoção de novas tecnologias, as soluções em IDD devem se tornar menos complexas para o entendimento dos usuários finais, evitando que os mesmos continuem a utilizar sistemas centralizados devido à sua maior simplicidade. O foco da UX neste sentido pode ser a carteira de identidade, que corresponde ao principal componente do ecossistema onde existe interação do usuário (VOLKOV, 2020).

5.3 Pesquisas de experiência de usuário no contexto de IDD

Um estudo realizado em 2022 com foco na usabilidade de soluções de gestão de Identidade Descentralizada observou que o problema de usabilidade das soluções atuais é significativo e pode comprometer o sucesso no mercado de tecnologias inovadoras (KHAYRETDINOVA et al., 2022). Nos testes - realizados com 18 participantes que avaliaram 23 soluções de Identidade Digital baseadas em blockchain - concluiu-se que embora o conceito de IDD seja familiar para os desenvolvedores, ele não é comunicado de forma clara aos usuários finais. Isso impede que os usuários aproveitem os benefícios descritos de privacidade e segurança, uma vez que os modelos mentais dos desenvolvedores não correspondem aos dos usuários comuns. Familiarizados com sistemas centralizados, tradicionais e hierárquicos, os usuários têm dificuldade na utilização e gestão de credenciais verificáveis e identidades digitais descentralizadas.

Em outro estudo (SOUZA et al., 2022), realizado no CPQD entre 2021 e 2022 utilizando uma carteira digital para a autenticação segura de pessoas a partir da leitura de QR code e apresentação de credenciais verificáveis, concluiu-se que o uso é mais difícil do que a autenticação via usuário/senha. Este estudo evidenciou a necessidade de tornar os processos mais flexíveis para abranger diferentes contextos de uso, bem como a importância de envolver os usuários no desenvolvimento de produtos de IDD e o desafio do equilíbrio entre segurança e usabilidade nesses sistemas.

Mais recentemente, o Desafio IDD do WRNP 25 realizado em 2024, ofereceu uma oportunidade prática para testar o ecossistema de IDD. Durante o evento, os participantes usaram credenciais digitais para provar sua presença e participar de um sorteio. O feedback ao vivo revelou dificuldades no entendimento e cumprimento da jornada de emissão e verificação, problemas de performance e questões de usabilidade na interface da carteira. No formulário de satisfação enviado após o evento,

16 participantes relataram que conseguiram usar a solução de forma autônoma, 29 precisaram de suporte, e 4 desistiram de participar. Este caso de uso é detalhado no capítulo Desafio IDD deste documento e no relatório da atividade A5.3.

5.4 Recomendações para melhorias futuras

O desenvolvimento de sistemas de gestão de IDD deve considerar aspectos multidisciplinares para evitar soluções que são amigáveis à privacidade mas pouco funcionais na prática. Para que os usuários possam usufruir dos benefícios de segurança e privacidade, eles precisam de ferramentas e assistência utilizáveis, que não tornem a experiência frustrante.

As interfaces, principalmente a UX das carteiras digitais - ponto principal de interação de usuários com o sistema, precisam ser otimizadas para um uso simplificado e intuitivo. É necessário fornecer recursos explicativos, instruções básicas como descrições e *walkthroughs* amigáveis, explicando como e por que utilizar funcionalidades específicas. Fluxos e jornadas devem fazer referência a modelos mentais familiares aos usuários, facilitando a curva de aprendizado dos mesmos sobre a tecnologia. Com relação à segurança, deve-se considerar a implementação de sistemas de recuperação para proteger usuários de perdas acidentais de credenciais.

A participação ativa dos usuários finais em pesquisa, estudos e testes de usabilidade é essencial para identificar e solucionar problemas de experiência dos sistemas de IDD. Além de utilizáveis, as soluções devem ser acessíveis a um público diverso, atendendo guidelines de acessibilidade digital e conformidade com legislações. As interfaces devem ser compatíveis com leitores de tela e jargões técnicos devem ser evitados para garantir que usuários possam utilizar a solução de forma eficaz independente de suas habilidades ou limitações.

Para aumentar a adoção, os desenvolvedores devem criar uma experiência intuitiva e prática, que não exija dos usuários a necessidade de compreender os conceitos de IDD. Informar os usuários sobre como seus dados serão usados e armazenados, e oferecer opções de controle sobre essa utilização, aumenta a confiança e percepção de segurança. Soluções que envolvem interações complexas devem comunicar seu valor de forma clara, demonstrando benefícios concretos que superam as desvantagens percebidas.

Para substituir de forma eficaz os sistemas centralizados, os sistemas descentralizados devem atingir um nível de maturidade e robustez adequados ao serem lançados no mercado. A escalabilidade deve ser considerada garantindo que o sistema possa suportar uma ampla base de usuários e aplicações em contextos diversos de uso. As soluções de IDD não devem atender apenas às necessidades de segurança e privacidade, mas oferecer também uma experiência de usuário que promova uma adoção ampla, acessível e sustentável.

5.5 *Hardware Security Module*

Módulo de Segurança de Hardware (Hardware Security Module - HSM) são hardwares reforçados que realizam gestão e proteção de chaves criptográficas para procedimentos de assinatura e verificação de certificados digitais. Com a utilização de um HSM as chaves privadas deixam de ser armazenadas em ambientes inseguros, como variáveis de ambiente, e passam a ser armazenadas no HSM. Quando é recebida uma requisição de assinatura ou validação de certificado, a requisição é enviada para HSM realizar as etapas assinatura ou comprovação de certificado.

Os HSMs possuem diversos mecanismos de proteção contra violação. Estes mecanismos de proteção garantem que os dados não serão vazados ou violados, mesmo em caso de ataque físico ao equipamento, pois quando é realizada uma tentativa de ataque físico os sensores e travas garantem a inviolabilidade da informação e em último caso podem realizar a destruição dos dados para garantir a inviolabilidade.

A Dinamo Networks é uma empresa de tecnologia da informação com foco em segurança

cibernética. A companhia possui diversas soluções de segurança da informação como cloud, cofre e HSM. Atualmente a Dinamo está presente em diversos países, no Brasil a empresa provê soluções de segurança para o Banco Central (Pix e Drex), nota fiscal eletrônica, conectividade social, prontuário eletrônico e imposto de renda.

Em relação ao produto HSM a Dínamo possui três opções de aparelhos: Dinamo CD, Dinamo XP e Dinamo ST. Os modelos disponíveis utilizam o mesmo *firmware* interno e funcionalidades, porém apresentam diferenças na capacidade de processamento criptográfico e armazenamento de chaves.

Os HSMs utilizam *Server Master Key* como componente de segurança para inicialização do equipamento e acesso seguro ao equipamento. A Server Master Key é uma chave gerada e armazenada de maneira derivada em cartões físicos, o armazenamento ocorre guardando partes da chave em cada cartão de maneira matematicamente confiável, de forma que para realizar o acesso físico é necessário um número N do Total de M cartões para liberar o acesso ao equipamento. Os serviços do HSM são habilitados somente após a inserção da Server Master Key (cartões) e desbloqueio do cartão através do PIN, então os serviços e partições estão disponíveis para utilização.

O HSM Dinamo é desenvolvido na linguagem C, e possui APIs em Java e Dot Net para facilitar a integração do HSM com aplicações clientes. A API Java utiliza a Java Native Interface (JNI) para realizar a comunicação com ambiente nativo para execução de comandos de sistema operacional, a JNI ainda permite que seja implementado dentro do código trechos de código nativo com linguagem C.

Na implementação do HSM é utilizado *Java Cryptography Architecture (JCA) e Java Cryptography Extension (JCE)* para. A JCA é integrada com Core Java API e realiza as operações básicas de criptografia compatíveis com Sistema Operacional, enquanto que a JCE realiza operações criptográficas avançadas.

5.5.1 Integração HSM com Hyperledger Besu

Para realizar a integração do HSM com Hyperledger Besu inicialmente é necessário criar certificados seguros para conexão da blockchain com o HSM. O processo de integração tem como pressuposto que a blockchain com ambiente configurado e os nós em execução.

Integrando o Besu com o HSM Dinamo é necessário, com a rede em execução, criar uma pasta certs para armazenar os certificados. Em seguida copiar para a pasta certs o script generate_certs_pki responsável pela criação dos certificados. Em seguida é necessário verificar a chave java da autoridade certificadora, o arquivo jks. Em seguida verificar a p12, inserindo o comando openssl e a senha.

Porém o HSM ainda não está completamente pronto para a utilização com o Besu, é necessário ainda configurar o PKCS#11 e a integração utilizando o cliente de conexão do HSM com a blockchain para que seja possível utilizar os certificados e chaves dos nós blockchain de maneira segura.

5.5.2 Configuração do PKCS#11 e integração com Besu

Primeiramente é necessário realizar o download e instalação do cliente Dinamo para sistemas operacionais Linux. Em seguida é necessário criar uma pasta para configurar o PKCS#11, esta pasta pode ser criada no caminho /opt com nome dinamo. Dentro deste diretório é necessário criar o arquivo p11config.cfg e em seguida inserir instruções de código contidas na documentação. Em seguida será necessário configurar as variáveis de ambiente do PKCS#11 no arquivo .bashrc para que estejam disponíveis para o cliente Dinamo.

O passo seguinte é realizar o download, instalação e configuração do hsmutil, um cliente que realiza a conexão com o HSM. Com o cliente hsmutil instalado e configurado, é necessário criar os certificados e chaves dos nós blockchain no HSM e transferir para os nós. Na interface de conexão

do hsmutil com o HSM existem opções para gerar certificados e chaves, inserindo os comandos guiados pelo menu e em seguida inserindo senha para armazenar os certificados e chaves. Com os certificados e chaves gerados, é necessário fazer os testes com os nós blockchain e verificar se a rede e conexões estão funcionando corretamente, pois se estiver funcionando as assinaturas digitais serão realizadas com chaves armazenadas no HSM.

5.5.3 Integração HSM com Hyperledger Fabric

Para realizar a integração do Hyperledger Fabric (HF) com HSM primeiramente é necessário que o sistema operacional dos nós suporte a integração com a PKCS#11 utilizada pela Dinamo. Como normalmente é utilizado docker para executar os nós, algumas imagens como Alpine Linux não possuem compatibilidade com o PKCS#11. Nestes casos é necessário alterar a imagem docker no dockerfile para utilizar um sistema operacional compatível com PKCS#11.

O HSM Dinamo permite que sejam criados usuários e partições independentes para cada organização e componente para realizar separação entre componentes e aumentar a segurança.

Para realizar a integração é necessário que a rede do HF esteja funcionando corretamente e o cliente hsmutil configurado, como no exemplo do Hyperledger Besu. Utilizando o hsmutil é possível criar os usuários e senha para cada nó do HF. Em seguida definir a variável de ambiente do gopath no arquivo.profile. Posteriormente é necessário recompilar os containers fabric e fabric-ca com suporte a PKCS#11.

5.5.4 Integração dos componentes Fabric com HSM

Para configurar os componentes *fabric-ca(cliente e server), peer, orderer e fabric tools* é necessário gerar primeiramente as imagens com suporte a *PKCS#11* editando o arquivo *DockerFile*, em seguida compilar as imagens para as alterações serem aplicadas. Em seguida é necessário criar pastas e alterar arquivos de configuração conforme a documentação.Na etapa seguinte os arquivos de configuração são alterados para que cada organização e nó utilizem o *PKCS#11* ditando alguns arquivos para conexão dos dados armazenados no HSM com HF. Em seguida é realizado o redirecionamento de chave e certificados nas configurações dos *ontainers* do nó para buscar as informações no HSM. Realizadas estas etapas, é possível utilizar o *Hyperledger Fabric* com os nós buscando as informações de chave e certificado diretamente no HSM, garantindo a segurança e privacidade dos dados dos nós.

6 Governança em IDD

O objetivo central desta seção é estudar modelos de governança que possam ser aplicados para gerenciar sistemas de identidade digital descentralizada (IDD). Para tanto, é necessário entender os contextos em que soluções de IDD podem ser aplicadas, que problemas elas resolvem, que vantagens trazem para as várias partes interessadas, mas também aquilo que elas demandam dessas mesmas partes, tanto em termos de envolvimento quanto de comprometimento.

Uma iniciativa de criação de uma solução de IDD visa sanar dores do setor econômico ou institucional onde a solução é aplicada. Assim, por exemplo, no setor de varejo, sobretudo na efervescente dimensão do e-commerce, essas dores começam com as dificuldades na filiação *(onboarding)* de usuários às plataformas varejistas, na maioria pela falta de uma autenticação ágil, prática e confiável das informações e dos documentos fornecidos, e chegam à etapa final das jornadas de compra *(checkout)*, na qual as dores se traduzem em abandonos de carrinhos, muito em razão do dilema entre exigir dos usuários uma interação mais simples ou privilegiar a prevenção de fraudes.

No setor financeiro, uma solução de IDD pode endereçar questões tais como a unificação dos processos de cadastro de clientes nas diversas linhas de negócio de uma instituição financeira

(banco comercial, seguradora, corretora de investimentos, plano de saúde, etc.) de modo a evitar que o cliente precise refazer o mesmo processo nos vários CNPJs da empresa holding, e a cada vez seja tratado como um desconhecido. E, em termos de ganhos, uma solução de IDD pode dar acesso a descontos ou taxas mais favoráveis em razão da maior confiança que sua identidade digital descentralizada traz para todo o ecossistema.

No âmbito institucional, se apresenta um contexto semelhante ao exemplificado para o setor financeiro, com a diferença de que se trata, neste caso, de dificuldades do acesso do cidadão a serviços públicos digitais, em razão da falta de padronização e de interoperabilidade entre órgãos. Cabe ressaltar que, independentemente do setor onde a solução de IDD seja implementada, sempre haverá um ecossistema de atores em torno dela, com variados níveis de envolvimento na iniciativa, distintos papéis em sua cadeia de valor e, consequentemente, diferentes responsabilidades e prerrogativas frente aos demais participantes, e a gestão desse ecossistema é uma dimensão fundamental da governança.

É também importante destacar que uma solução de IDD é possibilitada por um amplo conjunto de elementos e componentes que podem ser estratificados em camadas temáticas que vão da infraestrutura das redes de nós que registram transações e chaves criptográficas, passa pelos agentes de software (carteiras digitais) e pelos canais de comunicação segura entre eles, envolve os papéis que formam o triângulo da confiança (emissor de VCs, titular de VCs, verificador) e outros complementares, e chega aos ecossistemas de atores econômicos e institucionais que viabilizam a solução de IDD e, por essa razão, podem assumir um ou alguns dos referidos papéis.

A representação dessas distintas camadas, e de suas respectivas governanças, é um dos aspectos-chave do modelo aqui proposto, que tem como uma de suas referências principais o modelo estratificado proposto pela fundação Trust over IP (ToIP) (TOIP..., s.d.), como discutido adiante.

Por fim, mas não menos importante, cabe notar que o ciclo de vida de uma solução de IDD percorre distintas fases, cada uma com suas prioridades e especificidades no que toca à governança. E também aqui um dos requisitos de um modelo abrangente e flexível é uma correta representação dessas fases. Nesse particular, e como discutido a seguir, o modelo aqui proposto baseou-se no framework formulado pelo grupo de trabalho P2145 do Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE)(IEEE, 2022) sendo voltado a aplicações baseadas em blockchain. Esse modelo de referência foi aqui ajustado para cobrir melhor as fases iniciais do ciclo de vida, dada a importância dessas na viabilização da solução de IDD.

6.1 Desenvolvimento conceitual do modelo de governança

O tema da governança das redes e das aplicações baseadas em blockchain é ainda objeto de pesquisa nos setores acadêmico, governamental e corporativo, e os princípios e definições que guiaram o desenho desta estrutura de governança baseiam-se numa visão abrangente e atualizada dos estudos existentes. Entre as definições encontradas na literatura para essa governança, destacam-se as seguintes:

> “a governança é crítica para administrar um consórcio eficaz, dada a volatilidade da inovação do blockchain e os interesses divergentes dos participantes. A confiança é introduzida por meio de uma entidade, aceitável para todos, que exerce controle sobre o acesso e que toma decisões sobre a associação e o gerenciamento da aliança” (MUNDIAL, 2018)

> “a governança de redes blockchain é o instrumento que trata de quem faz as regras e de quem as aplica. Não se trata apenas de quem controla a blockchain, mas também de mecanismos de resolução em caso de colapso tecnológico, inadimplência contratual e crime” (OCDE, 2018)

> “a governança é um meio de alcançar a direção, o controle e a coordenação das partes-interessadas no âmbito de um projeto blockchain para o qual elas conjuntamente contribuem” (PELT et al., 2021)

> “a governança deve se fundamentar em três princípios: regras, reguladores e participantes, os quais devem existir harmonicamente. A governança se divide em dois tipos: direta e representativa, cada uma delas com vantagens e desvantagens” (MASSESSI, 2019)

> “a governança costuma ser centrada em um conjunto de qualidades: transparência, integridade, desempenho eficaz e colaboração” (WATSONLAW, 2018)

> “a governança pode ser analisada a partir de quatro categorias: consenso, incentivos, informação e estrutura decisória” (BLOCKONOMI, 2020)

> “a governança deve garantir a segurança e solidez da rede projetada para o benefício de todos os participantes [...] e gerenciar a atividade, conectividade, mudanças de software, acordos contratuais e finalização de transações para cada participante da rede” (ACCENTURE, 2019)

> “a governança define todas as ações, tais como processos de tomada de decisão, relacionadas à criação, à atualização e ao abandono de regras formais e informais de um sistema. Essas regras podem ser códigos (por ex., contratos inteligentes), leis (por ex., multas para infratores), processos (o que deve ser feito se algo acontecer) ou responsabilidades (quem deve fazer o quê). Ela se divide em governança da rede blockchain, governança de fundos e governança de projetos” (BOSANKIC, 2018)

> "a governança possibilita a uma plataforma lidar com o imprevisto e o inesperado"(BARRERA, 2019)

Partindo inicialmente dessas e de outras definições, o modelo aqui descrito evoluiu em busca de um formato mais adequado para aplicações de IDD baseadas em blockchain e chegou, como já mencionado, a uma combinação de dois modelos: o proposto pelo grupo de trabalho P2145 do IEEE para aplicações baseadas em blockchain e o concebido pela Fundação ToIP especificamente para aplicações de IDD. As razões para essa opção de combinar dois modelos complementares são discutidas a seguir.

O modelo de referência para governança de soluções baseadas em blockchain, proposto pelo IEEE, é um dos principais hoje disponíveis. Ele identifica cinco dimensões-chave a serem avaliadas e geridas: (i) políticas que pautam as decisões tomadas no âmbito da governança (princípios, contratos, regras, etc.); (ii) práticas adotadas para conferir efetividade à governança (métodos ágeis, metodologias de gestão de risco, etc.); (iii) pessoas (físicas e jurídicas) envolvidas e interessadas na aplicação e em sua governança (responsáveis, partes interessadas, etc.); (iv) processos decisórios e gerenciais formalizados no modelo; e (v) incentivos para que todas as partes interessadas se engajem em todas as dimensões da governança. O modelo IEEE define ainda que a governança precisa aplicar essas cinco dimensões temáticas principais a três metas distintas, que envolvem reconhecer e tratar: (i) o ecossistema de partes interessadas; (ii) as camadas de natureza tecnológica (rede, livro razão, protocolo, e aplicações); e (iii) o ciclo de vida da aplicação e de sua governança. Esse modelo e suas dimensões são ilustrados na Figura 11:

De modo análogo, o modelo de governança proposto pela Fundação ToIP para aplicações de IDD também distingue camadas temáticas para a governança, como ilustradas na Figura 12. A primeira camada engloba todos os recursos das redes DLT e os métodos ligados aos identificadores descentralizados. A segunda cuida dos agentes de software que criam as carteiras digitais e os

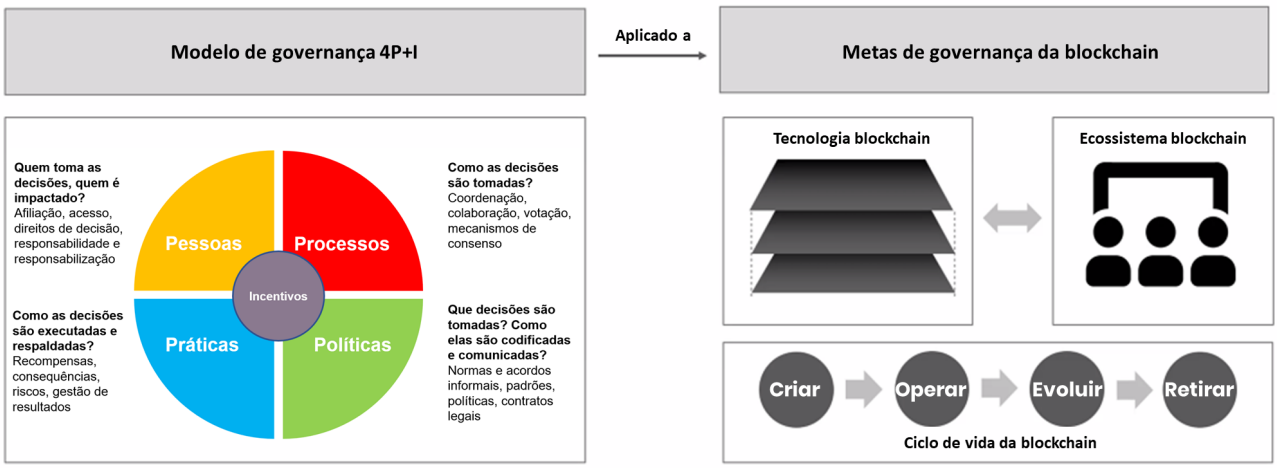

Figura 11: Cinco dimensões do modelo aplicadas às metas de governança (Fonte: IEEE - tradução do CPQD)

canais seguros de comunicação entre elas. Juntas, essas duas camadas asseguram aquilo que o modelo define como “confiança técnica”. Por sua vez, a terceira camada refere-se às relações entre os entes participantes da solução no que trata do papel que cada um assume nas transações: emissores das VCs, titulares das VCs emitidas, verificadores das VCs apresentadas pelos titulares, seguradores de transações, etc.

Por fim, a quarta e última camada diz respeito ao nível de envolvimento de cada ente no ecossistema em torno da solução de IDD. Esses níveis podem variar do de usuários finais ao de responsáveis pelo financiamento e pela oferta e da solução, passando pelo dos participantes de testes piloto. E, em conjunto, as camadas 3 e 4 constituem o que o modelo define como a “confiança humana” da solução.

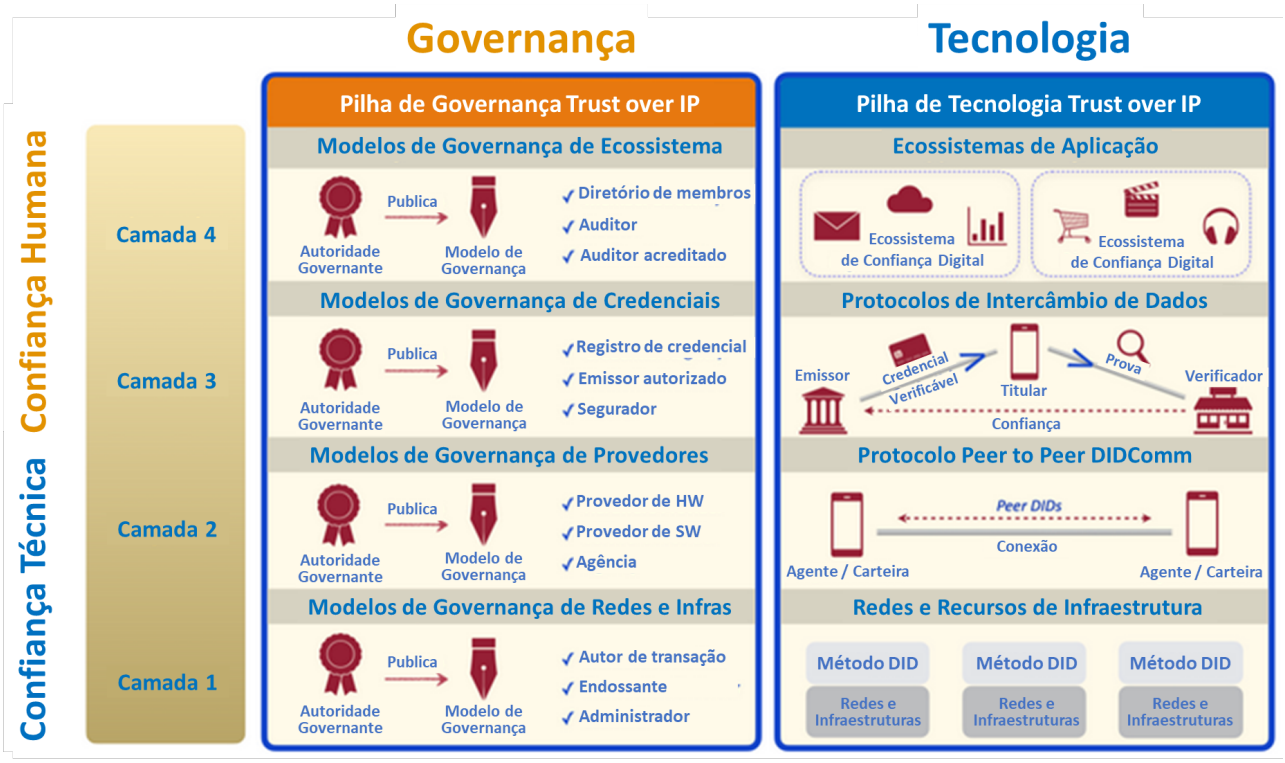

Figura 12: Níveis de participação na solução e em seu ecossistema

Uma terceira questão relevante para o desenho do modelo de governança de uma solução de IDD

e de seu ecossistema é a identificação dos possíveis níveis de envolvimento dos atores, que podem variar do nível máximo de envolvimento, sendo o dos entes responsáveis pela criação, evolução e operação da solução, até o nível mínimo, sendo o de fruição dos benefícios da solução, na condição de usuários. Em um nível intermediário de envolvimento encontram-se as empresas e instituições que, embora não sendo parceiras na criação da solução, participam do seu ecossistema nos papéis de emissoras ou verificadoras de VCs, ou de provedoras de componentes da solução.

É importante notar que esses possíveis níveis de participação tendem a surgir em diferentes fases do ciclo de vida da solução, conforme ilustrado na Figura 12, e para cada nível de envolvimento e papel assumido na solução haverá correspondentes direitos e responsabilidades, previstos na governança. Alguns aspectos da governança referem-se exclusivamente ao relacionamento entre os responsáveis pela criação da solução, outros afetam também os participantes de pilotos da solução, enquanto os demais mecanismos são voltados ao ecossistema mais amplo de participantes da solução já consolidada, e partes interessadas em torno dela. E cada nível de envolvimento implica casos de uso (processos) específicos.

Finalmente, outra consideração importante para o desenho da governança de soluções de IDD é a lista de princípios fundamentais que essas devem assegurar ou possibilitar. Foram aqui considerados 20 princípios propostos por (GERBER, 2022), conforme resumidos na Tabela 7. Alguns desses princípios, como os de autenticidade, verificabilidade e privacidade, podem ser considerados inerentes a quaisquer soluções de IDD, enquanto outros, como os de delegação e interoperabilidade, podem depender dos casos de uso e do contexto em que uma solução de IDD é operacionalizada.

Tabela 7: Vinte princípios pertinentes a aplicações de IDD

Princípio	Definição
Existência	Toda IDD deve pertencer a um usuário que exista fora do mundo digital
Representação	Um mesmo usuário pode ter qualquer número de IDDs que o representem
Autenticidade	É possível provar que os dados de uma IDD são de fato do usuário em questão
Verificabilidade	Toda informação na IDD do usuário pode ser verificada por prova (distribuída)
Controle	Os usuários de IDD são proprietários e têm total controle sobre seus dados.
Delegação	A gestão da IDD pode ser delegada (no todo ou em parte) a um procurador
Consentimento	A apresentação de dados de IDD só pode ocorrer com consentimento do titular
Persistência	A IDD deve persistir no tempo e o titular manter controle sobre seus dados
Acesso	O usuário de IDD deve poder acessar seus dados a qualquer tempo
Transparência	Sistema, regras e políticas de IDD devem ser transparentes (padrões abertos)
Portabilidade	Uma IDD deve ser recuperável e portável entre dispositivos/usuários/agências
Interoperabilidade	A IDD deve interoperar através de fronteiras, tecnologias e implementações
Privacidade	Dados e alegações da IDD devem permanecer privados e o titular anônimo
Minimalidade	A IDD deve conter e compartilhar o mínimo necessário de dados do titular
Descentralização	A infraestrutura deve ser descentralizada, sem controle central dos dados
Proteção	A proteção dos direitos do usuário independe da adesão de outros atores
Participação	O usuário é livre para usar a solução IDD, mas deve ter uma solução sem IDD
Usabilidade	A solução de IDD deve ser amigável e simples para a maior parte dos usuários
Equidade	A IDD deve ser justa e independer de gênero, etnia, nacionalidade e religião
Consistência	A experiência independe de onde e quando o usuário utiliza a solução de IDD

Embora os princípios sejam um dos pilares da dimensão das políticas, a definição de quais princípios opcionais serão assegurados pela solução ocorrerá à luz da proposta de valor almejada para ela. Por essa razão, na dimensão das práticas os princípios devem ser discutidos pelos entes

responsáveis pela solução em dinâmicas de identificação da proposta de valor e dos casos de uso prioritários e considerados tanto na definição final da dimensão das políticas, quanto nas das demais dimensões (pessoas e processos). Como exemplo, o princípio da “interoperabilidade”, caso seja priorizado, condiciona a que quaisquer adesões de novos atores ao ecossistema, na dimensão das pessoas, pressupõem a estrita observância dos padrões e das normas adotados na solução, na dimensão das políticas.

6.2 Modelagem da governança conforme as fases do ciclo de vida

No modelo adotado, foi mantida a visão do IEEE de ciclo de vida da solução e de seu ecossistema, mas optou-se por dar maior ênfase à sua jornada inicial, dividindo a fase de criação em duas: criação e ampliação, visto que cada uma delas tem desafios e necessidades muito específicos: a fase de criação envolve a formação da parceria e o refinamento da proposta de valor da solução, enquanto na fase de ampliação sobressaem ações de divulgação da iniciativa, por meio de eventos e redes de contatos e a adesão de novos atores, bem como atividades de validação da solução, por meio de pilotos e provas de conceito com a participação de atores daquele setor econômico ou daquele âmbito institucional.

Em contrapartida, o modelo adotado combinou numa única fase, denominada reposicionamento, as fases que no modelo IEEE tratam de evolução e encerramento da solução. Optou-se por esse arranjo ao se assumir que na fase de reposicionamento, se e quando ela for necessária, os participantes do ecossistema, em especial os responsáveis pela iniciativa, vão reavaliar toda a proposta de valor da solução para reposicioná-la no mercado ou, em último caso, encerrá-la. Seguindo essa proposta de divisão das fases, são ilustrados a seguir tópicos de governança relevantes para cada dimensão e para cada fase do ciclo de vida, com foco nas fases de criação, ampliação e operação. As Figuras Figura 13, Figura 14, Figura 15 ilustram essas respectivas fases na perspectiva da “confiança humana” da solução, ao passo que as Figuras Figura 16, Figura 17 e Figura 18 o fazem na visão da “confiança técnica”.

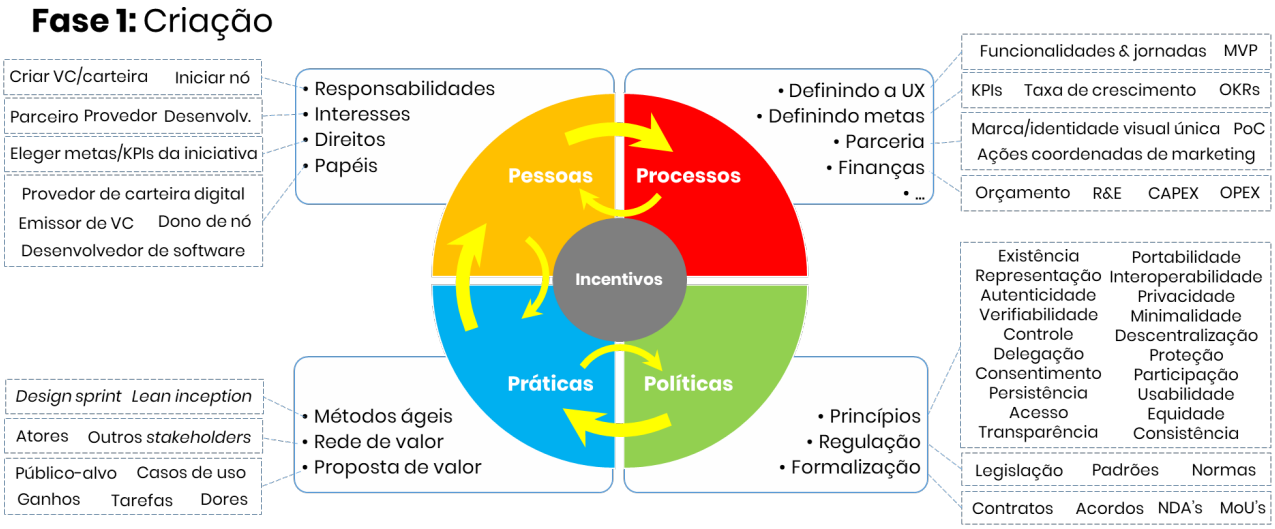

Figura 13: Tópicos de governança da fase de criação da camada de confiança humana

Conforme mostrado nas figuras, os tópicos prioritários da governança variam conforme a fase do ciclo de vida onde a solução se encontra. Se na fase de criação as práticas predominantes incluem o uso de metodologias ágeis como design sprint e lean inception para o desenho e validação da proposta de valor da solução, na fase de operação as práticas voltam-se mais à gestão de riscos e incidentes, por exemplo.

Como sugerido pelas setas amarelas mais grossas (apontando no sentido horário), há uma

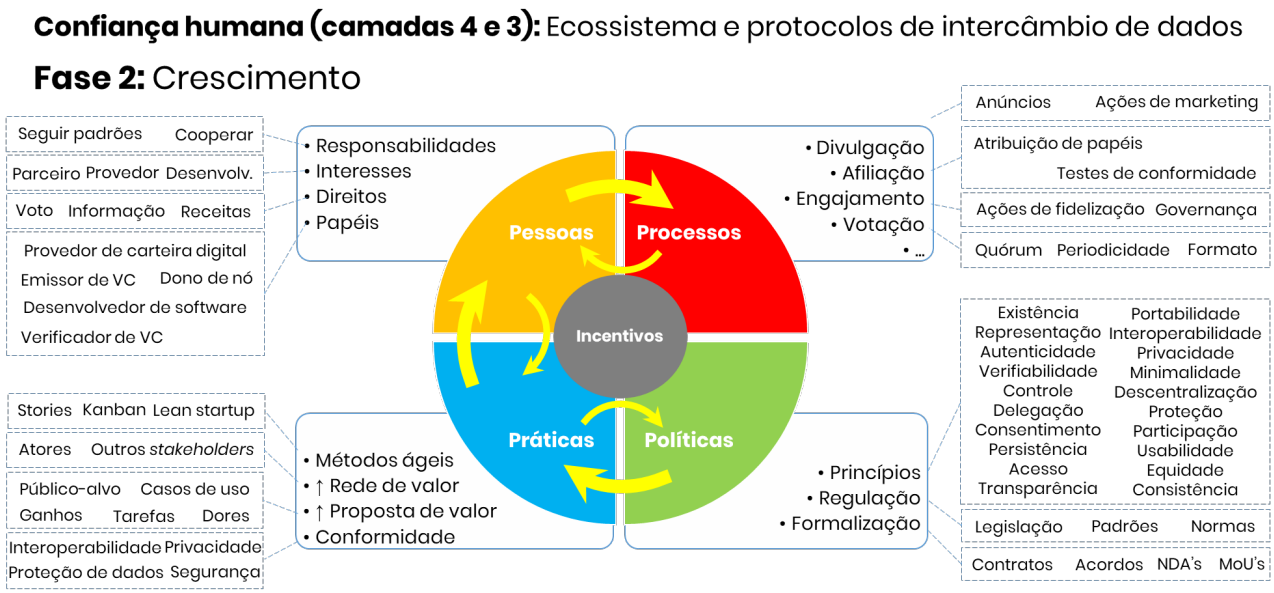

Figura 14: Tópicos de governança da fase de criação da camada de confiança humana

Figura 15: Tópicos de governança da fase de criação da camada de confiança humana

precedência típica entre as dimensões da governança. Parte-se das políticas, que englobam princípios fundamentais de IDD, a legislação vigente no contexto em que a solução será implementada e os contratos e acordos entre os responsáveis pela iniciativa para, em seguida, aplicar práticas (métodos ágeis, etc.) a fim de desenhar e validar a proposta de valor da solução e priorizar os casos de uso mais relevantes (dentro de um contexto de produto mínimo viável - MVP). E em função dessa proposta, definem-se para as pessoas (jurídicas e físicas) os papéis, deveres e direitos cabíveis, e traduzem-se todas essas definições em processos (casos de uso) formais da governança.

Cabe destacar, contudo, que essa sequência não é linear e está sujeita as reiterações (indicadas pelas setas mais finas, que apontam no sentido anti-horário). Assim, por exemplo, pode ocorrer que definições feitas na proposta de valor e nos casos de uso visados para a solução, na dimensão das práticas, impliquem alterar definições feitas na dimensão das políticas, por exemplo, na lista de princípios a serem observados (visto que alguns são opcionais) ou em aspectos da formalização da parceria (cláusulas contratuais, acordos, etc.). Embora menos prováveis e mais trabalhosas, alterações na regulação podem se mostrar necessárias caso uma proposta de valor muito relevante

dependa de ajustes nas regras vigentes, a ponto de justificar que os responsáveis pela iniciativa levem esse pleito aos entes reguladores.

Nesse mesmo sentido, definições e escolhas feitas na dimensão dos processos com vistas a assegurar mais agilidade, transparência, responsabilização, etc., podem implicar ajustes nas atribuições de direitos e deveres na dimensão precedente, que trata das pessoas (atores e partes interessadas).

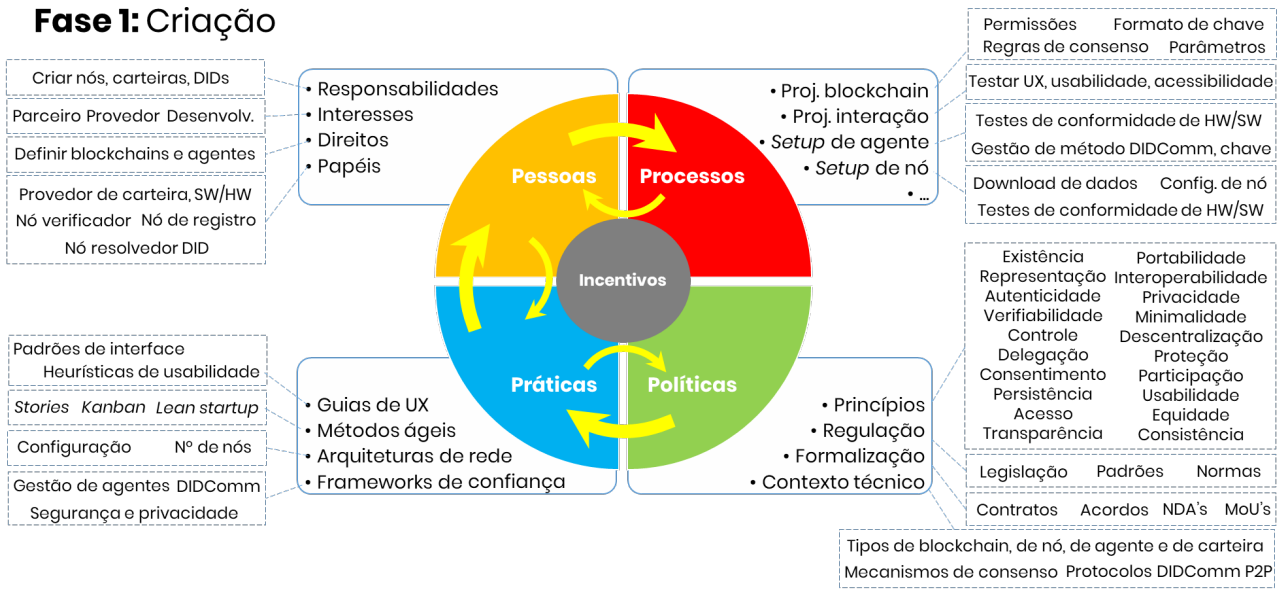

Figura 16: Tópicos de governança da fase de criação da camada de confiança técnica

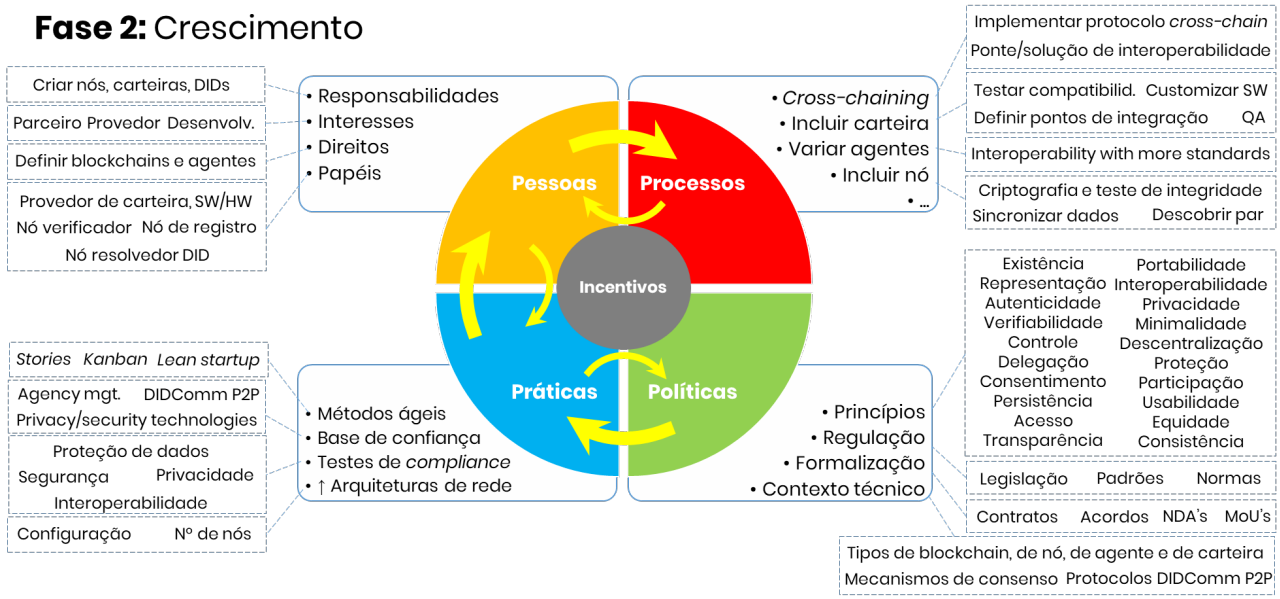

Figura 17: Tópicos de governança da fase de criação da camada de confiança técnica

A exemplo do que foi descrito para fases do ciclo de vida na camada de confiança humana, o desenho da governança precisa fazer um exercício semelhante para a camada de confiança técnica, conforme ilustrado nas figuras a seguir. Vale ressaltar que no âmbito da confiança técnica a dimensão das políticas deve considerar, além das questões de princípios, regulação e formalização já relevantes para a "confiança humana", também questões relacionadas ao contexto técnico no qual a solução se encontra. Isso inclui os tipos existentes de DLTs e blockchains, de nós, de mecanismos de consenso, de protocolos, etc.

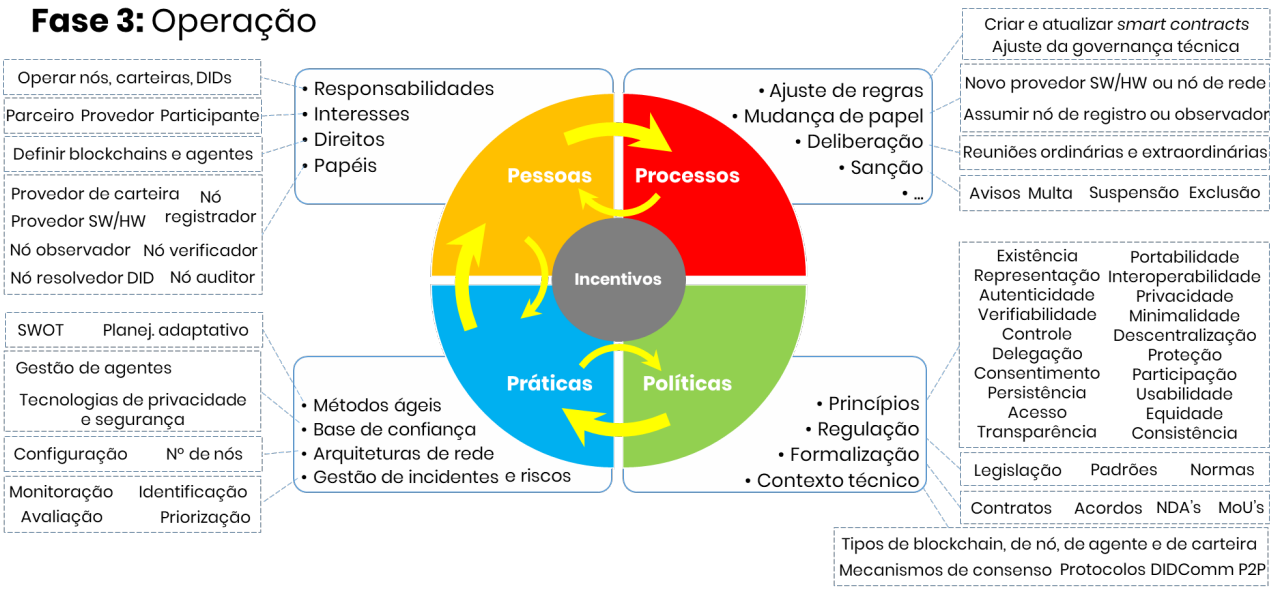

Figura 18: Tópicos de governança da fase de criação da camada de confiança técnica

6.3 Aspectos legais e regulatórios

6.3.1 A identidade digital no Brasil

No Brasil, os aspectos legais e regulatórios da identidade digital são críticos para garantir a segurança, a privacidade e a eficácia das soluções de identidade implementadas. À medida que os serviços públicos e privados continuam a tornar-se mais digitalizados, o país formulou uma série de leis e regulamentos para regular a utilização e gestão de identidades digitais (MARTINS; HOSNI, 2019). A seguir estão os principais aspectos legais e regulatórios relacionados à identidade digital no Brasil:

1. Lei Geral de Proteção de Dados Pessoais (LGPD)

- Descrição: A LGPD (Lei nº 13.709/2018), inspirada no GDPR europeu, regula o tratamento de dados pessoais de indivíduos no Brasil. A lei estabelece regras detalhadas sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais.
- Impacto na Identidade Digital: A LGPD impõe a necessidade de consentimento explícito do titular dos dados para seu processamento, além de garantir direitos como acesso, correção e exclusão de dados. Isso afeta diretamente como as entidades que oferecem serviços de identidade digital devem manejar as informações dos usuários (SANTOS, 2020).

1. Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)

- Descrição: A ICP-Brasil é um conjunto de técnicas, práticas e procedimentos implementados pelo governo brasileiro para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais.
- impacto na Identidade Digital: Ela fornece a base legal para a emissão de certificados digitais utilizados em identidades eletrônicas, como e-CPF e e-CNPJ, assegurando que transações digitais possuam a mesma validade jurídica que suas equivalentes físicas (ICP-BRASIL, s.d.).

1. Decreto sobre Governo Digital

- Descrição: O Decreto nº 10.332/2020 estabelece a Estratégia de Governo Digital para o período de 2020 a 2022. Ele visa promover a transformação digital dos serviços públicos, melhorar a eficiência e ampliar o acesso aos serviços governamentais.
- Impacto na Identidade Digital: O decreto fortalece o uso de plataformas como o Gov.br, que centraliza o acesso a serviços públicos através de uma identidade digital única por cidadão, promovendo a integração e a simplificação dos serviços públicos digitais (AVELINO; POMPEU; FONSECA, 2021).

1. Marco Civil da Internet

- Descrição: O Decreto nº 10.332/2020 estabelece a Estratégia de Governo Digital para o período de 2020 a 2022. Ele visa promover a transformação digital dos serviços públicos, melhorar a eficiência e ampliar o acesso aos serviços governamentais.
- Impacto na Identidade Digital: O decreto fortalece o uso de plataformas como o Gov.br, que centraliza o acesso a serviços públicos mediante uma identidade digital única por cidadão, promovendo a integração e a simplificação dos serviços públicos digitais (SCHREIBER, 2022).

Os aspectos legais e regulatórios sobre identidade digital no Brasil são basicamente projetados para construir um ambiente seguro e confiável para a digitalização de serviços e a proteção de dados pessoais, promovendo uma maior eficiência na prestação de serviços públicos e privados.

6.3.2 A IDD e a LGPD

A relação entre a Identidade Digital Descentralizada (DDI) do Brasil e a Lei Geral de Proteção de Dados Pessoais (LGPD) é complexa e importante, envolvendo a interseção de tecnologias avançadas de gerenciamento de identidade com regulamentações rígidas de privacidade e proteção de dados(ANDRADE, 2024). O IDD promove o gerenciamento seguro e autônomo da identidade dos usuários, enquanto a LGPD protege a privacidade e os dados pessoais. Os dois são complementares em muitos aspectos. Dentro desse contexto, foi definido alguns pontos de relação importantes e como IDD suporta os princípios da LGPD.

- Controle do Usuário sobre Dados Pessoais
- Minimização de Dados
- Segurança e Privacidade por Design
- Transparência e Prestação de Contas

Apesar da complementaridade, a implementação da IDD no quadro da LGPD pode enfrentar desafios, como:

- Interpretação e Cumprimento da Lei: A natureza descentralizada e às vezes anônima da IDD pode complicar a aplicação das normas da LGPD, que exige clareza quanto aos responsáveis pelo tratamento dos dados.
- Complexidade Tecnológica: A implementação de sistemas de IDD que cumpram totalmente os requisitos da LGPD pode ser tecnicamente desafiadora, especialmente em termos de gestão de consentimento e revogação em ambientes descentralizados.
- Educação e Conscientização: Tanto os usuários quanto os operadores de sistemas de IDD precisam estar bem informados sobre suas responsabilidades e direitos sob a LGPD, o que requer esforços substanciais de educação e treinamento.

Em suma, a interação entre IDD e LGPD representa uma oportunidade para fortalecer a proteção de dados pessoais no Brasil, oferecendo aos usuários maior controle e segurança sobre suas informações. No entanto, é essencial que tanto as soluções tecnológicas quanto às práticas regulatórias evoluam juntas para garantir que as promessas de ambas as abordagens sejam plenamente realizadas.

7 Iniciativas de Padronização

As iniciativas de padronização em Identidades Digitais Descentralizadas (IDD) são cruciais para garantir a interoperabilidade, segurança e adoção em larga escala. Aqui estão algumas das principais iniciativas de padronização em IDD:

7.1 Decentralized Identity Foundation (DIF)

A Decentralized Identity Foundation (DIF) é uma organização colaborativa formada por um grupo diversificado de líderes da indústria, desde startups de tecnologia até grandes empresas, focada no desenvolvimento de uma infraestrutura interoperável para identidades digitais descentralizadas. O objetivo principal da DIF é promover a adoção de tecnologias que permitam a criação, gestão e utilização de identidades digitais controladas pelos próprios usuários, eliminando a dependência de autoridades centrais (KYRIAKIDOU; PAPATHANASIOU; POLYZOS, 2023). O objetivo principal do DIF é criar um ambiente descentralizado e inclusivo para a identidade digital, promovendo a cooperação entre diversas entidades e defendendo a utilização de padrões e tecnologias abertas. O DIF pretende realizar o seguinte:

1. O foco principal é o desenvolvimento e a promoção de padrões técnicos que sejam interoperáveis, adotados globalmente e que facilitem a comunicação e integração contínuas entre diversas plataformas e sistemas.
2. Ao dar prioridade à privacidade e ao controle dos utilizadores, é crucial garantir que as tecnologias desenvolvidas colocam o poder dos dados nas mãos dos utilizadores.
3. Promover a colaboração: promova uma atmosfera colaborativa entre diversas partes interessadas, como empresas, desenvolvedores e entidades reguladoras, para incentivar o avanço e a aceitação de identidades descentralizadas.

A DIF colabora com outras organizações e consórcios, como o World Wide Web Consortium (W3C) e a Trust over IP Foundation, para garantir que os padrões e as soluções propostas sejam amplamente aceitos e facilmente integráveis com outros sistemas e tecnologias. Em resumo, a Decentralized Identity Foundation é uma peça chave no movimento para um futuro digital mais seguro, privado e centrado no usuário, trabalhando na vanguarda da tecnologia de identidades digitais descentralizadas. Com seu foco em padrões abertos, colaboração e inovação, a DIF está ajudando a moldar a infraestrutura necessária para a próxima geração de serviços digitais e interações online.

7.2 Trust over IP (ToIP)

Trust over IP (ToIP) é uma iniciativa global para estabelecer uma arquitetura de confiança completa para a Internet. O modelo ToIP combina a tecnologia blockchain com outros protocolos da Internet para permitir a troca segura, confiável e verificável de dados e credenciais digitais entre partes na Internet. A principal missão do ToIP é fornecer uma infraestrutura que apoie a confiança técnica (proteção e segurança de dados) e a confiança humana (normas legais e sociais), garantindo assim interações digitais seguras e confiáveis (DAVIE et al., 2019). A abordagem é dividida em quatro

camadas: a camada de utilidade de transporte, a camada de protocolo de troca de dados, a camada de credenciais e, finalmente, a camada de governança, com cada camada se baseando na camada anterior para criar um sistema de confiança digital abrangente (BADIROVA et al., 2024).

7.3 Open Wallet Foundation

A Open Wallet Foundation (OWF) visa desenvolver um conjunto padrão de APIs abertas para carteiras digitais, promovendo a interoperabilidade e integração entre diferentes sistemas e plataformas. A OWF planeja promover uma infraestrutura digital mais inclusiva e acessível que permita que as carteiras digitais operem de forma segura e eficiente, mantendo elevados padrões de segurança e privacidade. As carteiras digitais alimentadas pelo OWF conseguirão armazenar uma ampla gama de ativos digitais, incluindo dinheiro, identidades, credenciais e outros tipos de dados pessoais. A fundação visa promover o desenvolvimento e a adoção de tecnologias de carteira digital, tornando-as mais acessíveis e acessíveis a usuários e empresas em todo o mundo (BAUM et al., 2024).

7.4 W3C DID methods

O método W3C DID (Decentralized Identifier) faz parte de uma especificação desenvolvida pelo World Wide Web Consortium (W3C) para criar um sistema de identidade digital totalmente controlado pelo usuário. DID é um identificador único que permite a um sujeito (pessoa, organização, coisa) provar controle sobre ele por meio de métodos criptográficos sem a necessidade de uma autoridade centralizada (SHCHERBAKOV, 2024).

Cada DID aponta para um documento DID que contém as informações necessárias para verificar o DID e pode incluir chaves públicas, serviços associados e outras informações. A abordagem DID define como estes identificadores e documentos são criados, atualizados, analisados e retirados com base em diferentes tecnologias e plataformas, permitindo a sua interoperabilidade e adaptabilidade entre diferentes sistemas. Isto facilita uma ampla gama de aplicações, como sistemas de verificação de identidade, assinaturas eletrônicas e emissão de credenciais verificáveis, promovendo maior segurança e privacidade nas interações online.

8 Conclusões

Neste relatório foi apresentado um estudo detalhado sobre identidade digital descentralizada e seus principais desafios referente à Meta 5.1 do projeto Iliada. Foram elencados tópicos como os principais cenários de aplicações desse novo paradigma, projetos em andamento e modelos de padronização. Como resultados também foi descrita uma prova de conceito chamada desafio IDD, ver Seção 5, que se propôs a aplicar conceito de IDD em um ambiente de mundo real, mais precisamente no evento WRNP. O experimento comprovou a capacidade de IDD da garantia de autenticidade dos dados providos e de seus donos. Por fim, foram discutidos as iniciativas emergentes de padronização de IDD pelo mundo, como Anoncreds, W3C DID methods e Decentralized Identity Foundation. Em trabalho futuros serão abordados temas como *OpenID for VCs* e EIDAs 2, além do estudo de novos cenários de aplicações.

Referências

ACCENTURE. *Governing DLT Networks - DLT Governance for Private Permissioned Networks*. 2019. Junho de 2019, Disponível em: https://www.accenture.com/_acnmedia/accenture/redesign-assets/dotcom/documents/global/2/accenture-governing-dlt-networks.pdf.

ANDRADE, Luana. *Identidade digital e garantia dos direitos fundamentais*. Editora Dialética, 2024.

AVELINO, Daniel Pitangueira de; POMPEU, João Cláudio Basso; FONSECA, Igor Ferraz da. Democracia digital: mapeamento de experiências em dados abertos, governo digital e ouvidorias públicas. Instituto de Pesquisa Econômica Aplicada (Ipea), 2021.

ÁVILA, Ismael MA et al. Relato de Experiência do Processo de Implantação do Testbed para Gestão de Identidades Digitais Descentralizadas. In: SBC. ANAIS do II Workshop de Testbeds. 2023. P. 25–37.

BADIROVA, Aytaj et al. Towards Robust Trust Frameworks for Data Exchange: A Multidisciplinary Inquiry. In: GESELLSCHAFT FÜR INFORMATIK EV. OPEN Identity Summit 2024. 2024. P. 15–26.

BAI, Yirui et al. Decentralized and self-sovereign identity in the era of blockchain: a survey. In: IEEE. 2022 IEEE International Conference on Blockchain (Blockchain). 2022. P. 500–507.

BARRERA, C. *A framework for blockchain governance design: the Prysm Group Wheel*. 2019. Prysm Group, Apr 2019, Disponível em: https://medium.com/prysmeconomics/a-framework-for-blockchain-governance-design-the-prysm-group-wheel-703279c1b0dd.

BAUM, Carsten et al. Cryptographers' Feedback on the EU Digital Identity's ARF, 2024.

BERTRAM, Magdalena et al. Analysis of the Anonymous Credential Protocol'AnonCreds 1.0'used in Hyperledger Indy, 2022.

BLOCKONOMI. *What is Blockchain Governance? Complete Beginner's Guide*. 2020. Jul 2020, Disponível em: https://blockonomi.com/blockchain-governance/.

BOSANKIC, L. *Blockchain governance: takeaways from nine projects*. 2018. Medium, Apr 2018, Disponível em: https://medium.com/@leo_pold_b/blockchain-governance-takeaways-from-nine-projects-8a80ad214d15.

BRUNNER, Clemens et al. Did and vc: Untangling decentralized identifiers and verifiable credentials for the web of trust. In: PROCEEDINGS of the 2020 3rd International Conference on Blockchain Technology and Applications. 2020. P. 61–66.

CAPKO, D; VUKMIROVIĆ, Srđan; NEDIĆ, Nemanja. *State of the art of zero-knowledge proofs in blockchain. 2022 30th Telecommunications Forum (TELFOR)*. IEEE, 2022.

CHAVALI, Bhaskar; KHATRI, Sunil Kumar; HOSSAIN, Syed Akhter. AI and blockchain integration. In: IEEE. 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO). 2020. P. 548–552.

COMMISSION, European. *EBSI: The European Blockchain Services Infrastructure*. Brussels, 2023. Accessed: 2024-11-30.

CURREN, Sam; LOOKER, Tobias; TERBU, Oliver. Didcomm messaging. *s Draft*, v. 1, 2022.

DAVIE, Matthew et al. The trust over ip stack. *IEEE Communications Standards Magazine*, IEEE, v. 3, n. 4, p. 46–51, 2019.

DIB, Omar; TOUMI, Khalifa. Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions. *Annals of Emerging Technologies in Computing (AETiC)*, v. 4, n. 5, p. 19–40, 2020. Available at SSRN: https://ssrn.com/abstract=3785452. DOI: 10.33166/AETiC.2020.05.002.

EIDAS 2.0. https://www.european-digital-identity-regulation.com/.

FALAZI, Ghareeb et al. Process-based composition of permissioned and permissionless blockchain smart contracts. In: IEEE. 2019 IEEE 23rd International Enterprise Distributed Object Computing Conference (EDOC). 2019. P. 77–87.

FAN, Caixiang et al. Performance analysis of hyperledger besu in private blockchain. In: IEEE. 2022 IEEE international conference on decentralized applications and infrastructures (DAPPS). 2022. P. 64–73.

FERNANDES, L. A. *Governança em Infraestruturas Blockchain: Um estudo de caso da EBSI*. 2024.

GERBER, F. *A Use Case Oriented Survey of Self-Sovereign Identity*. 2022. Diss. (Mestrado) – École Polytechnique Fédérale de Lausanne. Disponível em: https://infoscience.epfl.ch/record/296053.

GITHUB. *openid4vc GitHub*. 2024. Disponível em: <https://github.com/topics/openid4vc>.

_____. *OpenIDIDComm GitHub*. 2024. Disponível em: <https://github.com/IDunion/OpenIDIDComm/blob/main/README.md>.

ICP-BRASIL, ASSINATURAS DIGITAIS NA. Infraestrutura de Chaves Públicas Brasileira.

IEEE. *Blockchain governance standards*. 2022. Grupo de Trabalho P2145, Disponível em: https://standards.ieee.org/ieee/2145/10143/, Acesso em: março de 2024.

KHAYRETDINOVA, Alina et al. Conducting a Usability Evaluation of Decentralized Identity Management Solutions. In: PROCEEDINGS of the Conference on Digital Identity Management 2022. 2022. DOI: 10.1007/978-3-658-33306-5_19.

KYRIAKIDOU, Chalima Dimitra Nassar; PAPATHANASIOU, Athanasia Maria; POLYZOS, George C. Decentralized identity with applications to security and privacy for the internet of things. *Computer Networks and Communications*, p. 244–271, 2023.

MALHOTRA, P. *Blockchain in Europe: Infrastructure and Innovation*. 2. ed. London: Blockchain Press, 2023.

MARTINS, Pedro; HOSNI, David. O Livre Desenvolvimento da Identidade Pessoal em Meio Digital: Para além da proteção da privacidade?(The Free Development of Personal Identity in the Digital Environment: Beyond the Privacy Protection?) *MARTINS, Pedro*, p. 46–5, 2019.

MASSESSI, D. *Blockchain Governance In A Nutshell*. 2019. Medium, Janeiro de 2019, Disponível em: https://medium.com/coinmonks/blockchain-governance-in-a-nutshell-67903c0d2ea8.

MUNDIAL, Banco. *Blockchain Governance and Regulation as an Enabler for Market Creation in Emerging Markets*. 2018. Note 57, setembro de 2018, Disponível em: https://documents1.worldbank.org/curated/en/636421540530725523/pdf/131343-BRI-EMCompass-Note-57-Blockchain-Governance-v1-PUBLIC.pdf.

NAIK, N.; GRACE, P.; JENKINS, P. An attack tree based risk analysis method for investigating attacks and facilitating their mitigations in self-sovereign identity. In: IEEE Symposium Series on Computational Intelligence. IEEE, 2021. P. 1–8.

NAIK, Nitin; JENKINS, Paul. Does Sovrin Network offer sovereign identity? In: IEEE. 2021 IEEE International Symposium on Systems Engineering (ISSE). 2021. P. 1–6.

NEVES, Rebeca de Aguilar Pereira. GDPR e LGPD: estudo comparativo, 2021.

OCDE. *Blockchain Technology and Corporate Governance*. 2018. DAF/CA/CG/RD(2018)1/REV1, Junho de 2018, Disponível em: https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/CA/CG/RD(2018)1/REV1&docLanguage=En.

OPENID FOUNDATION. *OpenID for Verifiable Credentials - Overview*. 2023. Accessed: 2024-12-02. Disponível em: <https://openid.net/sg/openid4vc/>.

PARTNERSHIP, European Blockchain. *European Blockchain Services Infrastructure (EBSI): Overview*. 2024. https://ec.europa.eu/digital-strategy/ebsi. Accessed: 2024-11-30.

PELT, R. van et al. Defining Blockchain Governance: A Framework for Analysis and Comparison. *Information Systems Management*, v. 38, n. 1, p. 21–41, 2021. DOI: 10.1080/10580530.2020.1720046.

PFEIFFER, Alexander; BUGEJA, Mark. Introducing the Concept of “Digital-Agent Signatures”: How SSI Can Be Expanded for the Needs of Industry 4.0. *Artificial Intelligence in Industry 4.0: A Collection of Innovative Research Case-studies that are Reworking the Way We Look at Industry 4.0 Thanks to Artificial Intelligence*, Springer, p. 213–233, 2021.

REED, Drummond et al. Decentralized identifiers (dids) v1. 0. *Draft Community Group Report*, W3C Cambridge, MA, USA, 2020.

REGULATATION EU. https://digital-strategy.ec.europa.eu/pt/policies/eidas-regulation.

ROSSNAGEL, Heiko et al. Users' willingness to pay for web identity management systems. *European Journal of Information Systems*, Taylor & Francis, v. 23, n. 1, p. 36–50, 2014.

SALAH, Khaled et al. Blockchain for AI: Review and open research challenges. *IEEE access*, IEEE, v. 7, p. 10127–10149, 2019.

SAMI, Hani et al. LearnChain: Transparent and cooperative reinforcement learning on Blockchain. *Future Generation Computer Systems*, Elsevier, v. 150, p. 255–271, 2024.

SANTOS, Flávia Alcassa dos. A lei geral de proteção de dados pessoais (LGPD) e a exposição de dados sensíveis nas relações de trabalho. *Revista do Tribunal Regional do Trabalho da 10ª Região*, v. 24, n. 2, p. 145–151, 2020.

SCHREIBER, Anderson. Civil rights framework of the Internet (BCRFI; Marco Civil da Internet): Advance or setback? Civil liability for damage derived from content generated by Third Party. In: PERSONALITY and Data Protection Rights on the Internet: Brazilian and German Approaches. Springer, 2022. P. 241–266.

SEDLMEIR, Johannes et al. Digital identities and verifiable credentials. *Business & Information Systems Engineering*, Springer, v. 63, n. 5, p. 603–613, 2021.

SHAGUN, Attri et al. Building a New IPv8 Bootstrapper and Network Discovery Strategy for Trusted Chain Identities. *Advances in Science and Technology*, Trans Tech Publ, v. 124, p. 789–793, 2023.

SHCHERBAKOV, Alexander. Hyperledger Indy Besu as a permissioned ledger in Selfsovereign Identity. In: GESELLSCHAFT FÜR INFORMATIK EV. OPEN Identity Summit 2024. 2024. P. 127–137.

SOLTANI, R; NGUYEN, UT; AN, A. *A survey of self-sovereign identity ecosystem. Secur Commun Netw 2021: 1–26*. 2021.

SOUZA, Fabiani et al. Autenticação segura de pessoas com carteira digital: um estudo no CPQD. In: PROCEEDINGS of IHC Estendido 2022. 2022. P. 48–55. DOI: 10.5753/ihc_estendido.2022.225470.

STODT, Fatemeh et al. Blockchain-Based Privacy-Preserving Shop Floor Auditing Architecture. *IEEE Access*, IEEE, v. 12, p. 26747–26758, 2024.

STOKKINK, Quinten; POUWELSE, Johan. Deployment of a blockchain-based self-sovereign identity. In: IEEE. 2018 IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData). 2018. P. 1336–1342.

SUN, Xiaoqiang et al. A survey on zero-knowledge proof in blockchain. *IEEE network*, IEEE, v. 35, n. 4, p. 198–205, 2021.

THIBAULT, Louis Tremblay; SARRY, Tom; HAFID, Abdelhakim Senhaji. Blockchain scaling using rollups: A comprehensive survey. *IEEE Access*, IEEE, v. 10, p. 93039–93054, 2022.

TOIP - Trust over IP Stack. Disponível em: https://trustoverip.org/toip-model/, Acesso em: março de 2024.

VOLKOV, Andrei. Addressing the Challenges Facing Decentralized Identity Systems. *iS CHANNEL*, v. 15, n. 1, p. 1–10, 2020. Disponível em: <https://www.lse.ac.uk/management/assets/documents/ischannel/Final-Print-iSChannel-Volume-15.pdf#page=10>.

VOS, Martijn de; ISHMAEV, Georgy; POUWELSE, Johan. Match: A decentralized middleware for fair matchmaking in peer-to-peer markets. In: PROCEEDINGS of the 21st International Middleware Conference. 2020. P. 74–88.

WATSONLAW. *Blockchain Governance: What Is It, What Types Are There and How Does It Work in Practice?* 2018. Outubro de 2018, Disponível em: https://watsonlaw.nl/en/blockchain-governance-what-is-it-what-types-are-there-and-how-does-it-work-in-practice/.

WINDLEY, Phillip J. *Learning Digital Identity*. "O'Reilly Media, Inc.", 2023.

YEUNG, Lorraine KC et al. Living with AI personal assistant: an ethical appraisal. *AI & SOCIETY*, Springer, p. 1–16, 2023.

YILDIZ, Hakan et al. A tutorial on the interoperability of self-sovereign identities. *arXiv preprint arXiv:2208.04692*, 2022.

YU, Keping et al. Blockchain-enhanced data sharing with traceable and direct revocation in IIoT. *IEEE transactions on industrial informatics*, IEEE, v. 17, n. 11, p. 7669–7678, 2021.

ZHOU, Lu et al. Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. *Journal of Information Security and Applications*, Elsevier, v. 80, p. 103678, 2024.

9 Histórico de alterações do documento consolidado

Data	Versão	Alterações realizadas
07/08/2024	1.0	Versão inicial do documento
03/12/2024	2.0	Versão 2

10 Execução e aprovação

Executado por:
Antonio Mateus de Sousa
Bruno Evaristo
Raquel Martins
Fernanda Corsini
Ramon Cordeiro
Ismael Ávila
Silvia Marion
Aprovado por:
José Reynaldo Formigoni Filho
Gerente de Solução
Gerência de Soluções Blockchain

A Anexo 1 - Registros do Workshop RNP - Desafio IDD


GT-CampusEdge
Ilíada: a nova
Internet da Confiança
GT-SmartMed