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

Relatório da Meta Física 5:
A6.3 – Pesquisa e Desenvolvimento em Identidade Digital Descentralizada

Relatório do Processo de Seleção dos Projetos

OBSERVATÓRIO NACIONAL DE BLOCKCHAIN

*De olho na web do **futuro**.*

Maio 2025

PROJETO ILÍADA
FASE 1

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 metassistema 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 o objetivo de identificar novas tecnologias, assim como novos produtos e ferramentas relacionadas com o metassistema IDD. Além da prospecção tecnológica, a atividade prevê a 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

Em um mundo cada vez mais digital, a forma como gerenciamos e comprovamos nossa identidade está passando por uma transformação fundamental. Identidades Digitais Descentralizadas (IDD) são um conceito emergente que visa devolver o controle das identidades digitais aos indivíduos, removendo a necessidade de intermediários centralizados. Para compreender plenamente o potencial da IDD, é essencial explorarmos os atores-chave que a sustentam: o emissor, o titular e o verificador. A seguir, explicamos o papel de cada um desses atores.

- **Emissores (issuers):** são as entidades responsáveis por emitir credenciais verificáveis para os titulares. Esses emissores podem ser instituições governamentais, universidades, empresas ou qualquer organização confiável que tenha a autoridade de emitir um documento ou informação verificada. Por exemplo, um governo pode emitir uma carteira de identidade digital ou uma universidade pode emitir um diploma digital. As credenciais emitidas são armazenadas de forma segura e podem ser apresentadas em várias circunstâncias.

- **Titulares (holders):** o titular é a pessoa que detém e controla suas próprias credenciais. Ao contrário dos sistemas tradicionais, onde as informações pessoais são armazenadas em servidores de terceiros, no modelo descentralizado o titular armazena suas credenciais em sua própria carteira digital (digital wallet). Isso dá ao indivíduo a autonomia para decidir quais informações compartilhar e com quem. Por exemplo, um titular pode escolher mostrar apenas a informação necessária (como a idade, mas não o número completo da identidade) para verificar sua elegibilidade para acessar um serviço.

- **Verificadores (verifiers):** são as entidades ou indivíduos que precisam validar as credenciais fornecidas pelos titulares. Eles podem ser empresas, órgãos governamentais ou qualquer entidade que precise verificar a autenticidade de uma informação fornecida. O verificador recebe uma credencial digital do titular e, com a ajuda de tecnologias descentralizadas (como a *blockchain*), pode confirmar se a credencial é válida e emitida por uma fonte confiável sem a necessidade de acessar uma autoridade central.

A Figura 1 exibe como estes atores estão dispostos em uma arquitetura padrão de IDD.

Estes atores interagem entre si a fim de garantir as características fundamentais e desejáveis para uma solução de identidade digital descentralizada. São elas:

- **Controle:** o titular deve ter controle primário sobre seus dados de identidade. Deve controlar quais dados compartilha, com quem compartilha e com qual finalidade os dados serão utilizados, sem depender de um ente centralizado.

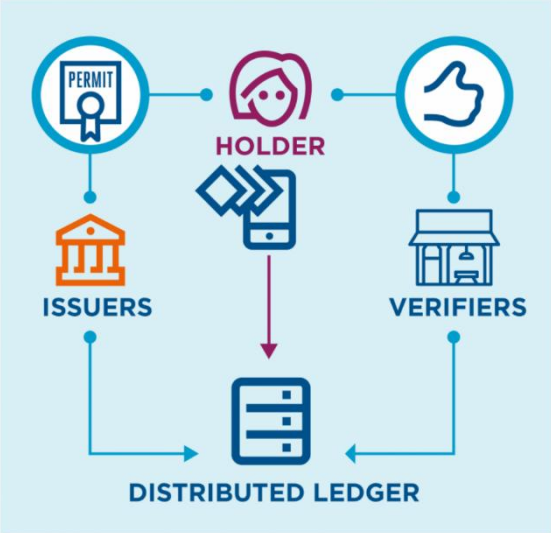
- **Acesso:** o titular deve possui acesso irrestrito aos seus dados de identidade.

- **Portabilidade:** as credenciais de identidade devem ser portáveis e possibilitar o uso em diferentes

contextos e com diferentes verificadores.

• **Transparência:** os sistemas de IDD devem ser transparentes em relação a como os dados são gerenciados e utilizados, desde a emissão até a verificação.

Figura 1 - Arquitetura básica de IDD



Fonte: (GSMA, 2025).

• **Interoperabilidade:** as soluções de IDD devem ser interoperáveis entre diferentes sistemas, plataformas e até mesmo jurisdições, facilitando o reconhecimento mútuo de identidades digitais.

• **Persistência:** As credenciais, uma vez emitidas e armazenadas na carteira digital do titular, persistem independentemente da disponibilidade do emissor.

• **Minimização de Dados:** uma solução de IDD deve garantir a troca do mínimo necessário de informações para cada interação, reduzindo a exposição de dados sensíveis.

• **Consentimento:** o titular deve emitir uma permissão explícita para o compartilhamento dos seus dados de identidade.

Esses fundamentos empoderam o indivíduo e trabalham em conjunto para criar um sistema de identidade digital mais seguro, privado, eficiente e centrado no usuário. A IDD busca construir um ambiente de identidades onde a confiança e a privacidade estão juntas.

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:

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 usuários quanto 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 setores, 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.

Como forma de embasamento das pesquisas e do estado da arte relacionado à 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”, “*Blockchain*”, “*Multiagent*”, “*Self-Sovereign Identity*” e “*Decentralized Digital 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).

A seguir, dissertamos sobre alguns dos temas mais importantes encontrados.

4.1 Especificações e 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. Identificadores Descentralizados (DIDs) 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.

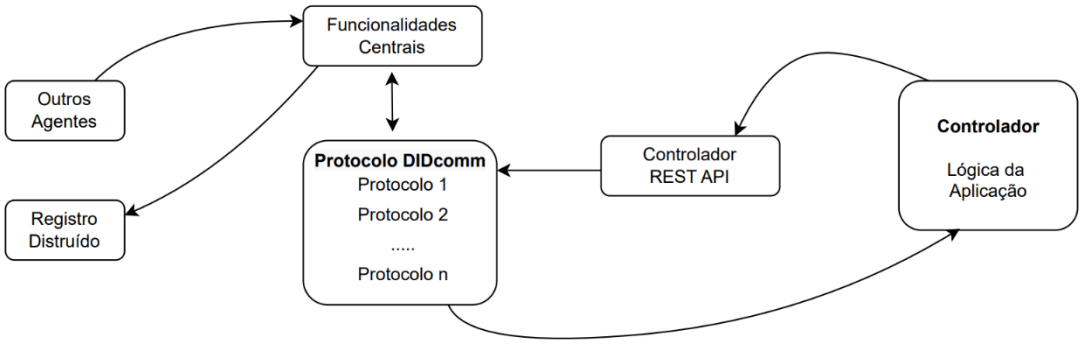
2. Credenciais Verificáveis (VCs) Credenciais Verificáveis são o segundo ponto de discussão. A especificação Verifiable Credentials, fornecida pelo W3C, descreve o processo de geração e utilização de credenciais digitais que podem ser autenticadas sem esforço. Isso facilita a transferência de credenciais 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 das 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. DID Communication (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.

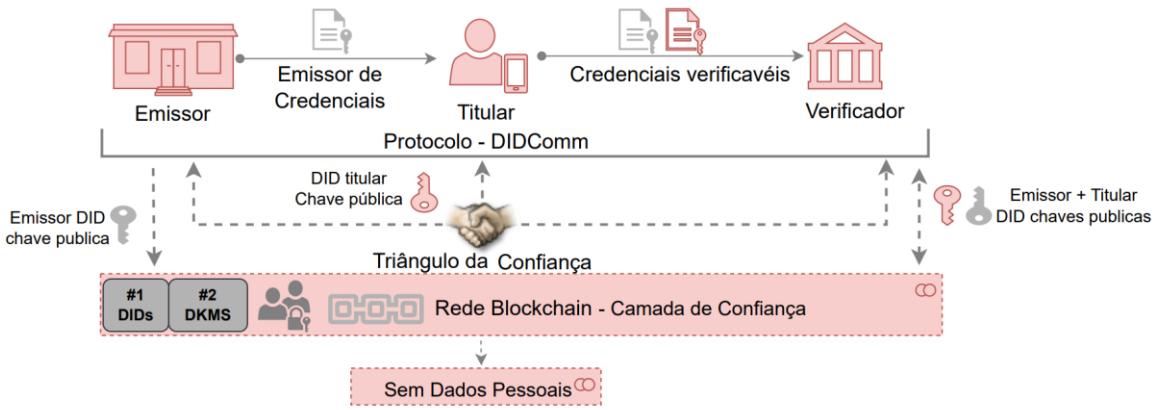
4.2 Tecnologia de Registros Distribuídos para IDD

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

[1] https://sovrin.org/

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 à identidade digital, um exemplo é a fundação *Trust Over IP*[2], que trabalha na padronização de uma arquitetura e na 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 3 - 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 3 (ÁVILA et al., 2023). É válido ressaltar que na *blockchain* não se registra nenhum dado sensível, apenas os schemas de informações que serão atrelados à credencial do usuário.

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.

- Vantagens da estrutura *blockchain Hyperledger Besu*:

  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;

[2] https://trustoverip.org

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.

• Desvantagens da estrutura *blockchain Hyperledger Besu*:

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.

• Vantagens da estrutura *blockchain Hyperledger Indy*:

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.

• Desvantagens da estrutura *blockchain Hyperledger Indy*:

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.

A Tabela 1 exibe uma comparação entre a *Besu* e a *Indy*.

Tabela 1 - Comparação entre *Hyperledger Besu* e *Hyperledger Indy*

Critério	Hyperledger Besu	Hyperledger Indy
Foco da Plataforma	Plataforma *blockchain* geral compatível com EVM	Específica para gerenciamento de IDD
Compatibilidade com EVM	Totalmente compatível	Não compatível
Versatilidade de Rede	Suporta redes públicas e permissionadas	Focado em redes permissionadas
Transações Privadas	Sim, oferece suporte	Limitado ou não nativo
Contratos Inteligentes	Suporta execução de contratos inteligentes, permitindo interoperabilidade	Não foca em contratos inteligentes
Governança Customizável	Sim	Sim
Foco em Identidade Digital	Adaptável, mas requer desenvolvimento adicional	Nativamente projetado para IDD
Segurança e Privacidade em IDD	Oferece transações privadas, mas segurança específica de IDD depende da implementação	Design centrado em privacidade e segurança para identidade
Interoperabilidade de Identidade	Possível com desenvolvimento adicional	Alta interoperabilidade entre redes de identidade
Escalabilidade e Performance	Pode enfrentar limitações, especialmente em redes públicas	Projetado para escalabilidade em redes de identidade
Complexidade Técnica	Exige configuração técnica avançada	Exige conhecimento específico sobre identidade auto-soberana
Aplicabilidade	Geral, podendo ser usado em diversos contextos	Limitado principalmente a aplicações de identidade
Curva de Aprendizado	Moderada, especialmente se já houver experiência com Ethereum	Alta, devido à especificidade dos conceitos de identidade auto-soberana
Comunidade e Ecossistema	Ampla comunidade, com forte base no ecossistema Ethereum	Comunidade menor, menos recursos 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, considerando 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 as 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.

Devido ao contexto no qual o projeto Ilíada está inserido e, considerando as vantagens e a aplicabilidade fornecidas pelo Hyperledger Besu, optou-se por adotá-lo como tecnologia de registro distribuído no Ilíada.

4.3 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 Credenciais Verificáveis (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, podemos citar alguns dos benefícios da interoperabilidade DID: (i) Fornecem 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); (ii) 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; (iii) Adoção mais ampla de identidades descentralizadas, facilitando o acesso e a integração dos sistemas.

Alguns dos exemplos básicos de interoperabilidade estão relacionados à autenticação entre fronteiras, ou seja, um usuário utiliza sua identidade digital baseada em DID, possibilitando 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).

4.4 eIDAS 2.0

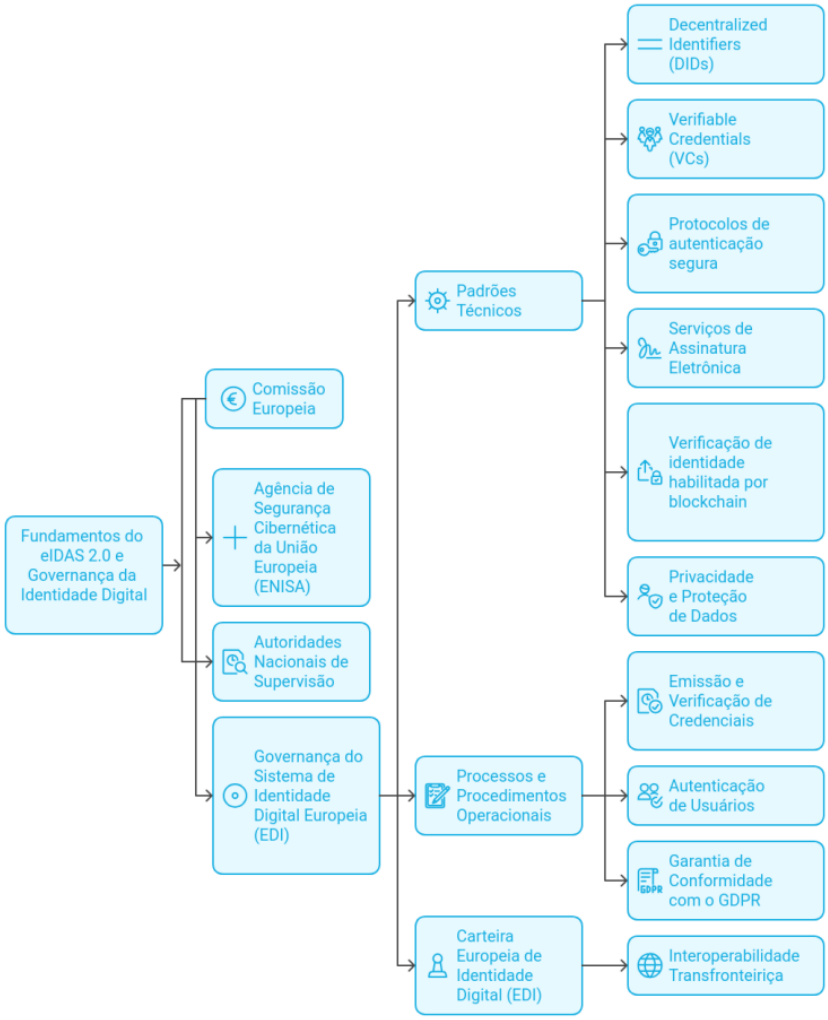
O eIDAS (The European Digital Identity Regulation) 2.0, ou Regulamento Europeu de Identificação Digital,é um regulamento destinado a melhorar a infraestrutura digital da União Europeia, concentrando-se em identidade digital e autenticação, com o objetivo de assegurar a interoperabilidade, segurança e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

4.4.1 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. A Figura 4 exibe os principais elementos da governança técnica do eIDAS 2.0.

Figura 4 - 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. Dentre essas alterações, podemos citar:

• Identificações Descentralizadas (DIDs): 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.; REGULATATION EU. . . , s.d.).

A EDI 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 tem um papel crucial na determinação do futuro da gestão de identidade digital.

4.5 EBSI

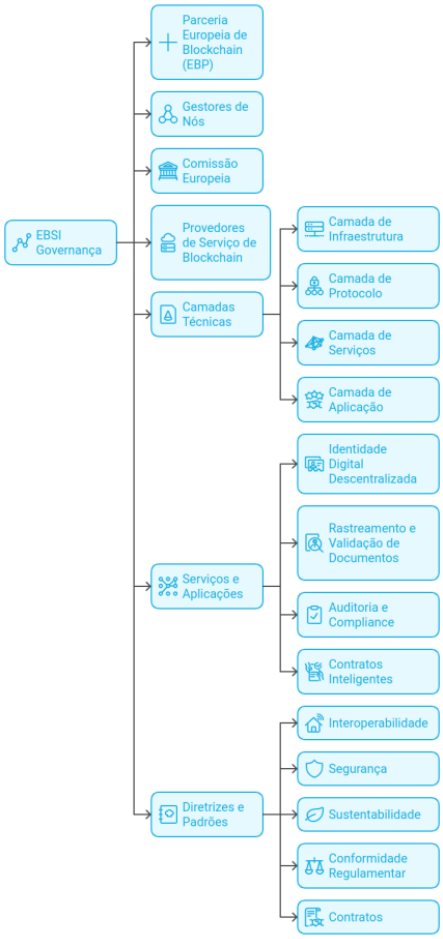
A *European Blockchain Services Infrastructure* (EBSI) é um projeto da União Europeia criado para oferecer uma infraestrutura *blockchain* segura, confiável e interoperável, com o objetivo de apoiar serviços públicos digitais e fomentar a inovação. EBSI possui uma rede *blockchain* autorizada e descentralizada 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; MALHOTRA, 2023).

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). É baseada 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; FERNANDES, 2024). A Figura 5 mostra a estrutura de governança técnica da EBSI.

Figura 5 - Estrutura de Governança Técnica da EBSI



Com a evolução da estrutura de governança técnica da EBSI, naturalmente pode-se elencar 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 natural também, 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.

4.6 OpenID Foundation

A *OpenID Foundation* é uma organização sem fins lucrativos de padrões que desenvolve especificações de identidade digital, autenticação e segurança. Suas especificações técnicas estão presentes em muitos projetos de identidade digital descentralizada, e possui membros notáveis, como Google e Microsoft (OPENID FOUNDATION, 2025).

A *OpenID Connect* é a principal especificação criada pela *OpenID Foundation*. É um protocolo de autenticação interoperável que adiciona uma camada de identidade sobre o *framework* de autorização *OAuth 2.0*. Ele promove uma verificação da identidade dos usuários simplificada, através da autenticação realizada por um Servidor de Autorização e da obtenção de dados de perfil do usuário de forma interoperável, semelhante ao *REST*.

Com base no *OpenID Connect* ou em adaptações dele, a *OpenID Foundation* desenvolveu outras especificações. Algumas delas são descritas a seguir.

4.6.1 OpenID4VC

O OpenID4VC (OpenID para Credenciais Verificáveis) (OPENID FOUNDATION, 2023; GITHUB, 2024) 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. 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.
- Self-Issued OpenID Provider v2 (SIOPv2): permite que usuários finais usem Provedores OpenID (OPs) que eles controlam.

Além disso, podemos citar os principais aspectos do OpenID4VC:

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.

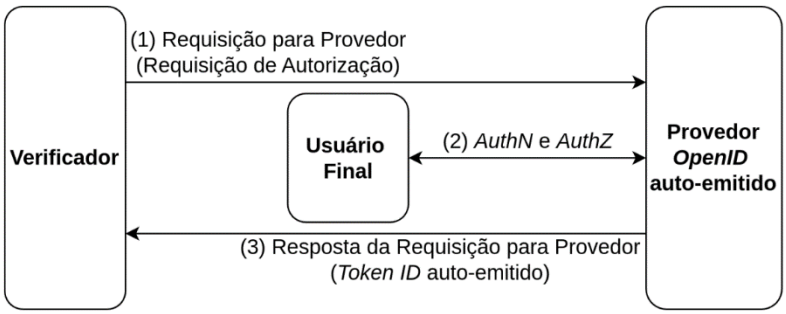
A adoção do OpenID4VC vem crescendo, com destaque para iniciativas como a Estrutura Europeia de Identidade Digital ou sua menção em normas que vêm sendo elaboradas pela ISO. A título de exemplo, em abril de 2023, 18 carteiras no projeto EBSI da Comissão Europeia já davam suporte às especificações OID4VCI 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.

4.6.2 Self-Issued OpenID Provider v2

O *OpenID Connect* limita o usuário final a utilizar um provedor *OpenID* terceirizado para autenticar seus dados. O *Self-Issued OpenID Provider v2* (SIOPv2) remove essa limitação, concedendo ao usuário a possibilidade de agir como seu próprio provedor *OpenID*. Dessa forma, o usuário final assume o papel de emissor de suas informações de identidade. Isso elimina a necessidade de depender de terceiros para autenticação, promovendo maior privacidade e controle sobre os dados pessoais, como em outras propostas descritas neste texto, porém utilizando o protocolo *OpenID Connect* (KRISTINA YASUDA; LODDERSTEDT, 2023).

O termo "*self-issued*" ("auto-emitido") vem do fato de que os usuários finais emitem *tokens* de identificação autoassinados para comprovar a validade dos seus identificadores e das suas declarações (SPHEREON, 2020). A Figura 6 exibe o fluxo até a emissão desses *tokens*.

Figura 6 - Fluxo de Protocolo do SIOPv2



Fonte: (Kristina Yasuda; Lodderstedt, 2023).

Em comparação com o uso de um provedor OpenID terceirizado, podemos exemplificar vantagens do SIOPv2 em alguns casos de uso:

• Resiliência a indisponibilidades de provedores *OpenID* terceirizados: provedores auto-emitidos operam localmente, reduzindo a dependência de disponibilidade de terceiros;

• Autenticação e apresentações de reivindicações do usuário sem o envolvimento do emissor: permite o envio de declarações assinadas sobre o usuário diretamente do provedor auto-emitido, preservando a privacidade, evitando o intermédio do emissor;

• Compartilhamento de declarações de múltiplos emissores em uma única transação: facilita a agregação de informações de diferentes fontes (como credenciais verificáveis) em uma única apresentação ao verificador;

• Agregação de múltiplas identidades sob um único provedor auto-emitido: usuários podem gerenciar diferentes personas - como persona profissional e persona pessoal, por exemplo - em um único provedor auto-emitido, simplificando a gestão de identidades.

4.6.3 OpenIDIDComm

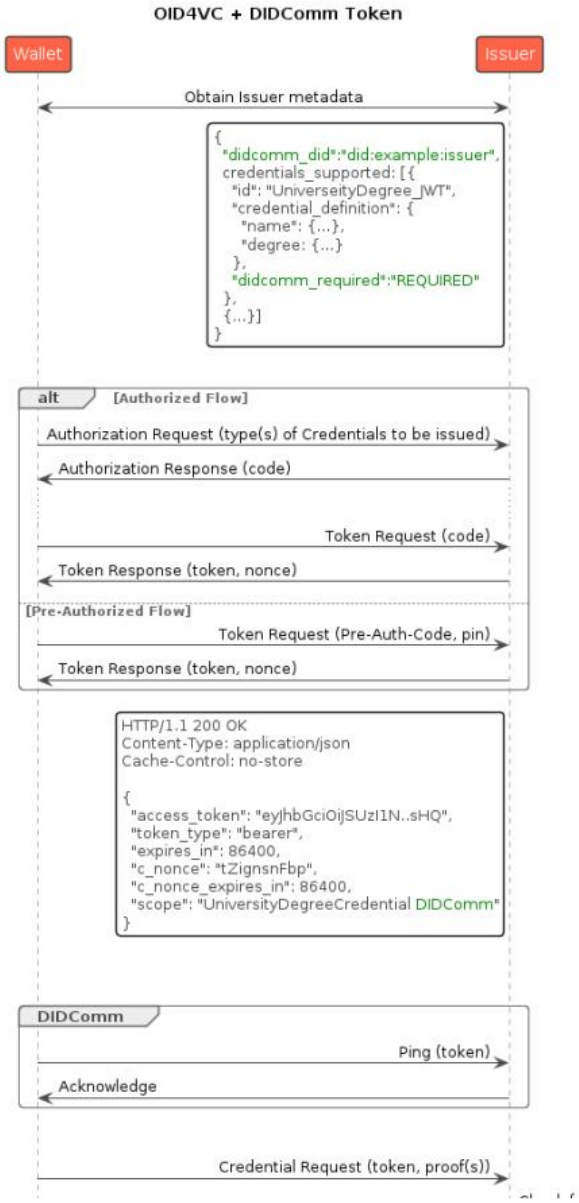
O objetivo do projeto OpenIDIDComm foi criar uma extensão para os protocolos OpenID4VCI e OpenID4VP com vistas a criar um canal DIDComm para comunicação. São elencados diversos casos de uso nos quais a combinação dos protocolos OpenID4VCI e OpenID4VP com o DIDComm traz vantagens. De modo geral, qualquer 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 várias outras 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 (IDUNION, 2024), o projeto OpenIDIDComm 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 7, 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 7 - Requisição e autorização utilizando OpenIDIDComm



Fonte: (IDUNION, 2024).

Por fim, os responsáveis pelo projeto OpenIDIDComm 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

4.6.4 EU Digital Identity Wallet

Sob o Regulamento de Identificação Eletrônica, Autenticação e Serviços de Confiança (eIDAS), os Estados-Membros da União Europeia podem, de forma voluntária, notificar e reconhecer esquemas nacionais de identificação eletrônica em seus países. O reconhecimento das identificações eletrônicas notificadas tornou-se obrigatório em 2018. No entanto, não há exigência para que os Estados-Membros desenvolvam uma identificação eletrônica nacional nem que a tornem interoperável com as

de outros Estados-Membros. Isso levou a discrepâncias entre os países. O novo Regulamento sobre identidade digital visa corrigir as deficiências do eIDAS, aprimorando a eficácia do seu arcabouço legal e ampliando seus benefícios para o setor privado. Os Estados-Membros oferecerão aos cidadãos e empresas carteiras digitais que poderão vincular diversos aspectos de suas identidades digitais nacionais. Essas carteiras poderão ser fornecidas por autoridades públicas ou pelo setor privado, desde que reconhecidas pelos Estados-Membros.

A Carteira de Identidade Digital da UE será:

• disponível para todos os que quiserem usá-la: Qualquer cidadão, residente ou empresa da UE que deseje utilizar a Identidade Digital da UE poderá fazê-lo.

• amplamente utilizada: As Carteiras de Identidade Digital da UE serão usadas como meio de identificação para acesso a serviços digitais públicos e privados em toda a União Europeia.

• controlada pelos usuários: As Carteiras de Identidade Digital da UE permitirão que as pessoas escolham e acompanhem quais dados de identidade e certificados compartilham com terceiros. Nada que não seja necessário será compartilhado.

Os consumidores também deverão ser capazes de acessar serviços online sem depender de plataformas privadas ou compartilhar dados pessoais desnecessariamente. Eles terão controle total sobre os dados que compartilham.

4.7 Linux Foundation Decentralized Trust

A *Linux Foundation Decentralized* Trust é uma organização sem fins lucrativos que adota os princípios de código livre estabelecidos pela *Linux Foundation* para fomentar um ecossistema crescente de *ledgers*, identidades digitais e tecnologias relacionadas (LF DECENTRALIZED TRUST, 2025c).

Seu escopo de atuação inclui o fortalecimento e financiamento de desenvolvedores, pesquisadores e empreendedores que compõem a comunidade global de tecnologias voltadas para confiança digital, além de oferecer suporte e manutenção a uma infraestrutura técnica neutra e colaborativa que viabiliza o desenvolvimento de projetos abertos, eventos comunitários e iniciativas educacionais.

A *LF Decentralized Trust* possui uma forte frente de atuação na área de Identidade Digital Descentralizada e Credenciais Verificáveis. As Subseções 4.7.2, 4.7.4 e 4.7.5 descrevem alguns projetos neste escopo.

4.7.1 Hyperledger Aries

O *Hyperledger Aries* é um conjunto de ferramentas de código aberto para soluções de identidade digital descentralizada e confiança digital. Ele inclui uma definição de protocolo, ferramentas e implementações de referência, como o ACA-Py.

Utilizando os princípios de credenciais verificáveis e de identidade digital descentralizada, o Aries fornece uma infraestrutura para comunicação segura e troca de credenciais verificáveis entre agentes. Com suporte a múltiplos protocolos, tipos de credenciais e *ledgers*, ele permite a emissão, o armazenamento e a apresentação de credenciais verificáveis com alto grau de privacidade (LF DECENTRALIZED TRUST, 2025a).

4.7.2 Hyperledger AnonCreds

O *Hyperledger AnonCreds* é um projeto 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 consumir bebidas alcoólicas 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. Ele 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.

No projeto Ilíada, juntamente do Besu, o *Hyperledger AnonCreds* foi escolhido como padrão a ser adotado para as aplicações de identidade digital e credenciais verificáveis.

4.7.2.1 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*.

O *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* apoia 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.

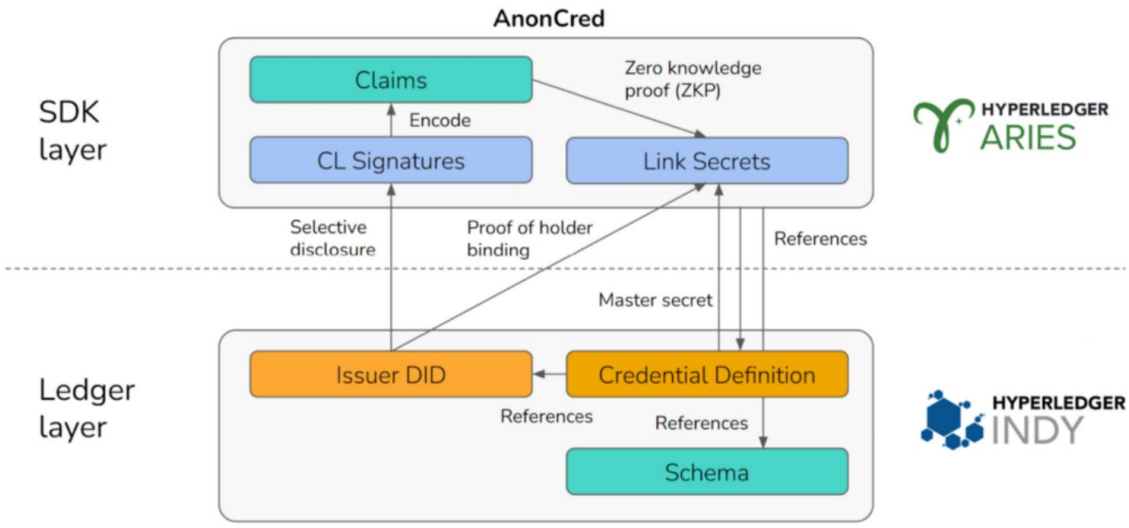
As principais características que fazem o sistema *AnonCreds* existir podem ser definidas em dois níveis distintos:

- 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 8.

Figura 8 - Pilha do AnonCreds



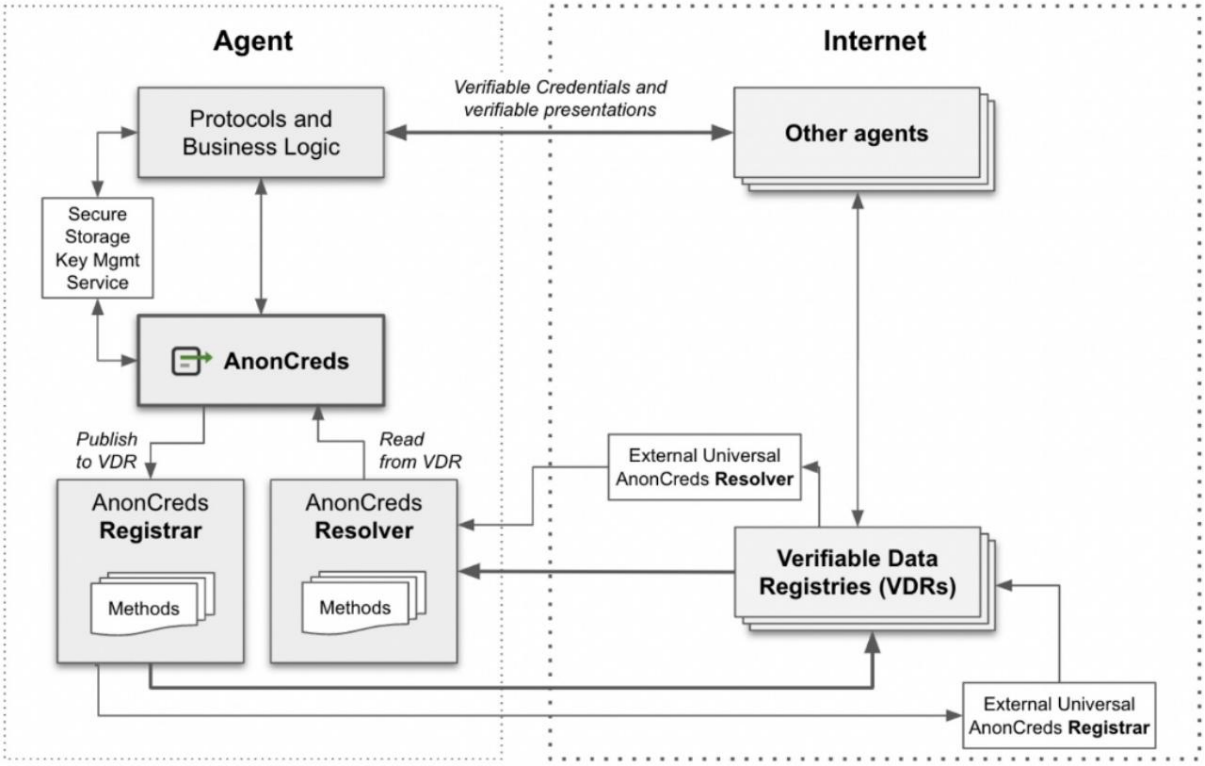
O *Hyperledger Indy* é importante para oferecer suporte a *AnonCreds*, pois até o momento é o único *blockchain* de identidade que pode oferecer suporte nativo a transações de DIDs, esquemas, definições de credenciais (e registro de revogação opcional) gravadas no livro-razão.

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).

4.7.2.2 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 9.

Figura 9 - Agentes e Registros de Dados Verificáveis (VDRs)



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 uso somente de resolvedor (titular e verificador) (SHCHERBAKOV, 2024). Além de uma mudança nas dependências dentro do *Aries Framework*, 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*.

4.7.3 Indy-Besu

O projeto Indy-Besu tem como objetivo substituir o ecossistema Hyperledger Indy por uma nova solução baseada em *blockchain* compatível com EVM, mantendo o suporte a credenciais verificáveis. Ele propõe substituir os componentes Indy Node, Indy Plenum e Indy SDK, além de permitir a migração de dados do ledger original.

4.7.3.1 Principais requisitos

• Ledger público permissionado com controle sobre validadores e usuários.
• Compatibilidade com a Ethereum Virtual Machine (EVM).
• Base em um framework *open-source* com bom desempenho e ampla adoção.
• Funcionamento sem tokens ou taxas.
• Protocolo de consenso estável.

4.7.3.2 Funcionalidades

• Interoperabilidade com métodos de identidade descentralizada (DID), incluindo indy, sov e ethr.
• Uso como registro de credenciais AnonCreds.
• Compatibilidade com a especificação mais recente de AnonCreds.
• Extensibilidade para integração de novas funcionalidades.
• Validação apenas da consistência básica do estado.

O projeto também disponibiliza documentação para execução local com Docker, biblioteca cliente em Rust e diretrizes para contribuição.

4.7.4 CREDEBL

A CREDEBL é uma plataforma de código aberto para o gerenciamento de Identidades Digitais Descentralizadas (IDDs) e Credenciais Verificáveis (VCs). É reconhecida pela *DPG Alliance* como um Bem Público Digital (DIGITAL PUBLIC GOODS ALLIANCE, 2024) e é usada em dois programas nacionais de Identidade Digital, o NDI do Butão e o *SevisPass Digital ID* da Papua-Nova Guiné (CREDEBL, 2025).

Originalmente, foi desenvolvida pela AYANWORKS, mas em 2025, tornou-se um projeto da *LF Decentralized Trust*. Assim, a CREDEBL passou a ter um modelo de governança estruturado e uma base diversificada de colaboradores globais, acelerando sua adoção e garantindo que sua direção seja orientada pela comunidade e que as decisões sejam tomadas de forma transparente, apoiando a estabilidade do projeto a longo prazo (AJAY JADHAV, 2025).

A CREDEBL permite que organizações emitam, verifiquem e gerenciem credenciais digitais de maneira escalável e otimizada, podendo suportar projetos em escala populacional. A CREDEBL ajuda governos e entidades privadas a implementar uma solução de emissão e verificação de identidade digital de forma econômica, aproveitando os padrões W3C (MASHA BORAK, 2025).

A plataforma CREDEBL possui algumas características desejáveis no contexto de DIDs e VCs, algumas delas são:

• Padrões abertos: é construída utilizando padrões abertos da W3C para DIDs e VCs;

• Escalabilidade: suporta desde provas de conceito até projetos a nível populacional;

• Privacidade desde a concepção: adota os princípios de *Privacy-by-Design*, garantindo a soberania dos usuários os concedendo total controle sobre seus dados;

• Agnótico à *ledger*: suporta múltiplas ledgers, como *Indy, Polygon e Cheqd* (em breve), além de fornecer suporte também a emissão de credenciais sem utilizar *ledger*, com métodos *did:web*, *did:peer* e *did:key*, por exemplo.

Para permitir que administradores e usuários tenham um acesso mais simples e facilitado para interagir com as ferramentas disponibilizadas pela CREDEBL, é fornecido o *CREDEBL Studio*, uma aplicação web de interface amigável. O utilizando, podemos:

• Registrar usuários: a plataforma oferece um processo de registro de usuários seguro com verificação por e-mail e autenticação;

• Integrar uma organização: possui um processo de inscrição de novas organizações facilitado;

• Integrar um equipe: oferece convites por e-mail para integração de membros de uma equipe de maneira eficiente;

• Gerenciar carteiras da organização: fornece suporte para carteiras web SSI, utilizando agentes *Aries*;

• Definir esquemas de credenciais: permite a criação de esquemas de credencias e registro na *ledger*;

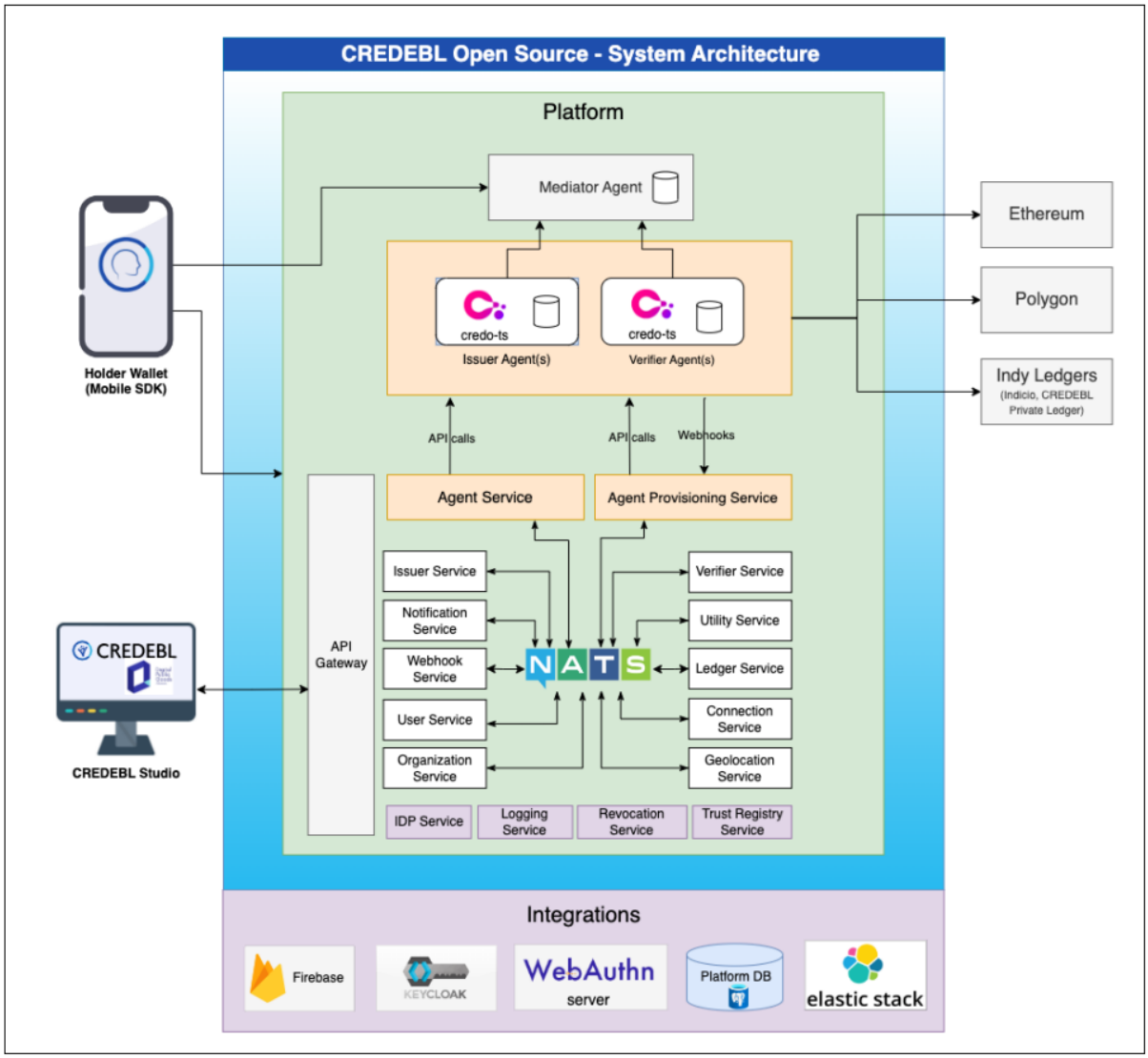
• Gerenciar ciclo de vida de VCs: oferece um processo consistente para criar e gerenciar o ciclo de vida dos VCs. Emissores confiáveis podem emitir e revogar credenciais de forma integrada (CREDEBL, 2025).

Além disso, pensando nos desenvolvedores mobile, também é fornecido o *CREDEBL Mobile SDK*, uma ferramenta *React-Native* que ajuda no desenvolvimento de recursos de SSI em aplicativos móveis, enquanto permite interoperabilidade e comunicação segura.

Para facilitar interações peer-to-peer e transações de dados seguras, a CREDEBL fornece suporte a implementações do protocolo *Aries*, como *Credo* e *ACA-Py*. Assim, a depender de suas necessidades, uma organização pode usar Agentes Compartilhados e/ou Agentes Dedicados.

A Figura 10 exibe a arquitetura da plataforma CREDEBL.

Figura 10 - Arquitetura CREDEBL



Fonte: (CREDEBL, 2025).

4.7.5 Hyperledger Identus

O *Hyperledger Identus* é um conjunto de ferramentas projetado para permitir o uso de soluções de identidade digital descentralizada (IDD). Essas ferramentas trabalham juntas para estabelecer uma estrutura para a implementação de soluções de identidade descentralizada. Ele atua como uma solução de *blockchain layer-2* da *Cardano* (CARDANO, 2025) e fornece funcionalidade completa de DID e credenciais verificáveis, simplificando as complexidades da adoção de uma solução de identidade descentralizada (HYPERLEDGER IDENTUS, 2025).

O *Hyperledger Identus* utiliza padrões e protocolos abertos, como a especificação W3C de Identificadores Descentralizados (DIDs), o W3C JWT, o *Hyperledger AnonCreds* e o *DIDComm v2*. Os padrões abertos visam promover a colaboração, a inovação, a portabilidade e a interoperabilidade, facilitando assim o funcionamento integrado das tecnologias. Isso promove uma experiência do usuário que permite a movimentação de dados e aplicativos entre diferentes plataformas e dispositivos com uma experiência semelhante (LF DECENTRALIZED TRUST, 2025b).

Podemos dividir o *Hyperledger Identus* em quatro principais componentes. São eles:

• **Agente de nuvem:** fornece serviços de identidade autossoberana e é baseado nos padrões W3C, DIDComm e nos protocolos *Hyperledger* Aries. Além disso, expõe uma *API REST* para integração com qualquer linguagem de programação, permitindo o desenvolvimento de soluções baseadas na tecnologia SSI;

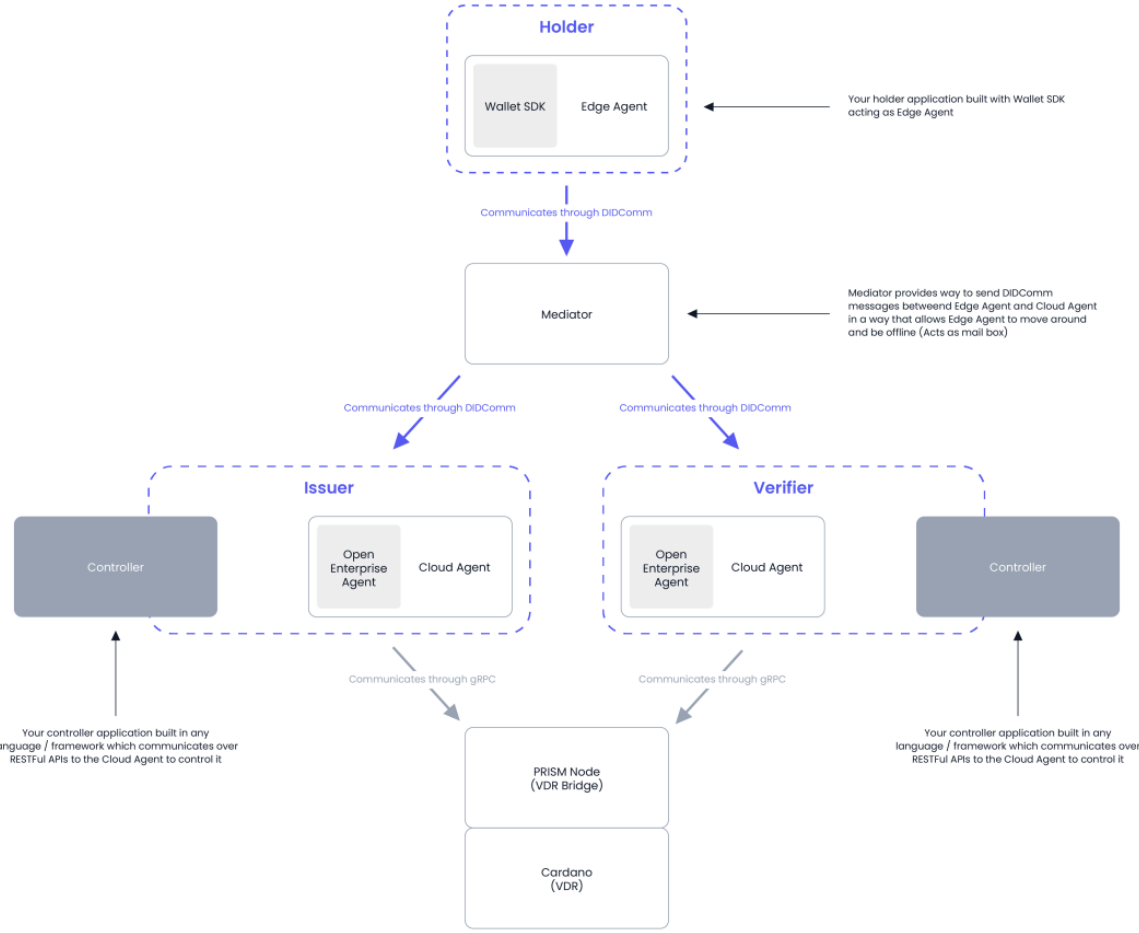
• **Nó *PRISM*:** serve como um registro de dados verificável (VDR). O nó *PRISM* armazena e recupera dados com segurança, é à prova de violação e é responsável por publicar as transações de protocolo do *Identus* na *ledger*. Opera em segunda camada e em conjunto com a *blockchain*, mantendo seu estado interno sincronizado com a rede, fornece operações de pesquisa de forma eficiente. Ele também desempenha um papel crítico na resolução eficiente de DIDs sem a necessidade de acesso à *blockchain* subjacente;

• **Mediador:** atua na entrega de mensagens de agente para agente, como uma ponte entre o dispositivo do titular e outros atores, como emissores e verificadores, garantindo uma comunicação segura e confiável sem gerenciamento centralizado. Especialmente, quando os agentes estão implantados em dispositivos móveis, sem IP estático e/ou com baixa disponibilidade, o mediador se torna indispensável, garantindo a entrega da mensagem.

• **Kits de desenvolvimento de software (SDKs) de agentes de borda:** permitem o desenvolvimento de agentes de borda de identidade digital, como aplicativos móveis e extensões para navegadores. Os SDKs estão disponíveis em Swift (iOS e outros sistemas operacionais da *Apple*), *Typescript* (navegador e *Node.js*) e *Kotlin Multiplatform* (*Java Virtual Machine e Android*) (HYPERLEDGER IDENTUS, 2025).

A Figura 11 ilustra uma iteração típica desses componentes.

Figura 11 - Iteração entre componentes do Hyperledger Identus



Fonte: (HYPERLEDGER IDENTUS, 2025).

4.8 OpenWallet Foundation

A *OpenWallet Foundation* é mais uma iniciativa internacional de código aberto, mantida pela *Linux Foundation*, que promove o desenvolvimento de carteiras digitais interoperáveis, seguras e confiáveis.

Ela incentiva o desenvolvimento colaborativo de tecnologias de carteira digital para facilitar a interoperabilidade global de credenciais verificáveis, estabelecer melhores práticas e, por meio do desenvolvimento colaborativo de tecnologia de carteira digital, promover softwares de código aberto e baseados em padrões abertos, nos quais os emissores e fornecedores de carteiras possam confiar (OPENWALLET FOUNDATION, 2025c). É uma organização sem fins lucrativos e gerida de forma colaborativa e conta com alguns membros notáveis, como: *Google, Mastercard e Visa.*

As Subseções 4.8.1, 4.8.2 descrevem alguns dos projetos da *OpenWallet Foundation* relacionados com identidade digital descentralizada.

4.8.1 Credo

O Credo é um *framework Typescript* para o desenvolvimento de soluções de identidade digital descentralizada. Ele é independente de qualquer protocolo de troca de dados, formato de credencial, conjunto de assinaturas ou método DID específico, mas atualmente se concentra principalmente no alinhamento com OpenID4VC, DIDComm e *Hyperledger Aries*. Dessa forma, mantém-se compatível e interoperável com diversos padrões de identidade em todo o mundo.

Foi concebido, inicialmente, pela Hyperledger Foundation e nomeado como *Aries Framework JavaScript*. Posteriormente, foi migrado para a *OpenWallet* Foundation e renomeado para *Credo*, porém mantendo uma parte significativa da comunidade de desenvolvedores da Hyperledger. Dessa forma, é comum encontrá-lo em aplicações deste ecossistema de identidade digital descentralizada (OPENWALLET FOUNDATION, 2025b).

4.8.2 Bifold

O Bifold é um projeto React Native desenvolvido para melhorar a interação com identidades digitais de maneira intuitiva e segura. É uma carteira *mobile*, disponível como *Android e iOS*, que faz o gerenciamento de identidades digitais em diversos padrões, como *AnonCreds e W3C VC Data Model*.

Tem como foco principal simplificar e tornar conveniente o uso de credenciais verificáveis (VCs). Enquanto o *Credo* trata da verificação e processamento das credenciais verificáveis, o *Bifold* trata da experiência do usuário e como é feita a interação com as credenciais (OPENWALLET FOUNDATION, 2025a).

Sua crescente adoção internacional, incluindo entidades governamentais no Canadá e equipes no Brasil, evidencia sua confiabilidade e capacidade de adaptação a diferentes contextos. Sua participação no Canadá inclui a *BC Wallet*, uma carteira mobile do governo de *British Columbia* para o armazenamento e gerenciamento de credenciais verificáveis para as empresas e cidadãos da província.

4.9 Privacidade e Segurança de Dados

Privacidade e segurança de dados são aspectos de alta importância em sistemas computacionais, e se tornaram 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, à 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 à carteira, ao *issuer* ou *verifier* comprometendo a segurança e privacidade do usuário (STODT et al., 2024).

4.9.1 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 a 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 consiste na garantia de 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).

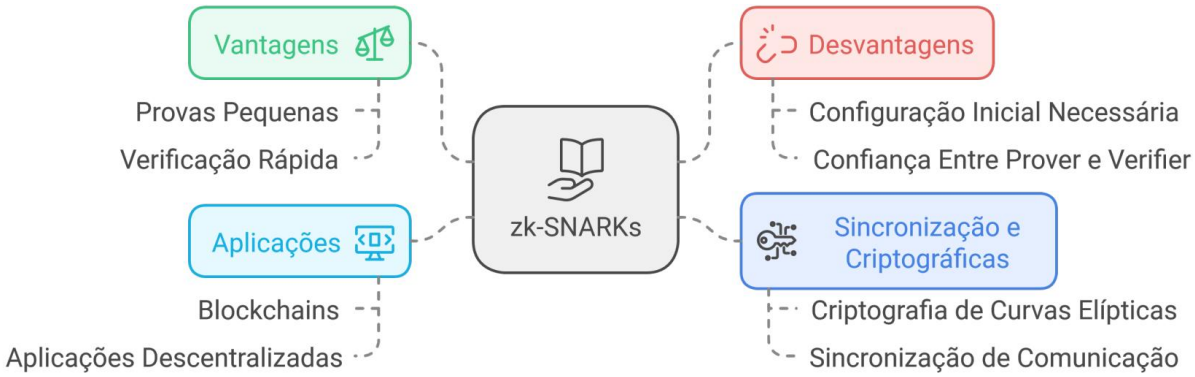
Em termos gerais, existem dois tipos de provas de conhecimento, as interativas e não-interativas. Em ZKPs interativas, o provador e o verificador comprometem-se mutuamente num protocolo de troca de mensagens na forma de requisições desafio-resposta em múltiplas rodadas de interação para atestar a validade 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 de que sua declaração é verdadeira sem revelar informações sensíveis (ZHOU et al., 2024). Por outro lado, 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 12 apresenta as etapas de uma prova de conhecimento zero.

Figura 12 - Fazes de prova de conhecimento zero

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

Os zk-SNARKs são mecanismos de prova de conhecimento zero utilizados em contextos de comunicação síncrona entre *prover* e *verifier*. Os 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 uma configuração 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 configuração seja realizado entre atores não confiáveis (CAPKO; VUKMIROVIC´; NEDIC´, 2022; THIBAULT; SARRY; HAFID, 2022). A Figura 13 apresenta uma visão geral de zk-SNARKs.

Figura 13 - Visão geral zk-SNARKs

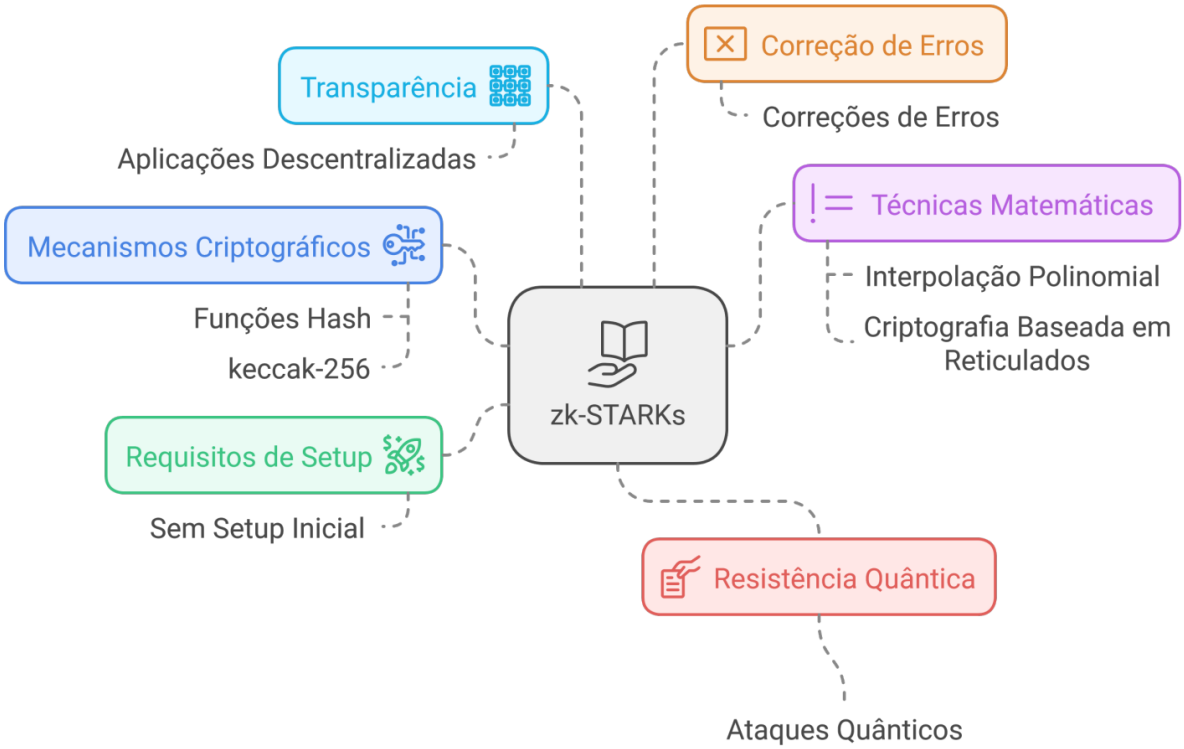


b) Zero-Knowledge Scalable Transparent Argument of Knowledge (zk-STARKs)

Os 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 configuração 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; VUKMIROVIC´; NEDIC´, 2022). A Figura 14 apresenta os principais aspectos de provas de conhecimento zero STARKs.

Figura 14 - Visão geral de zk-STARKs



4.9.2 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 esses 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, possibilitando 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.

4.9.3 Ataques em IDD

Ataques de segurança em Identidades Digitais Descentralizadas (IDD) representam um desafio crescente na era digital. Alguns dos principais tipos de ataques estão descritos nas seções a seguir.

4.9.3.1 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 revogação 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 garantindo 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 à 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 o intuito de obter dados suficientes para encontrar o usuário alvo com base nas informações fornecidas. A Tabela 2 apresenta os vetores de ataque e como funcionam (NAIK; GRACE; JENKINS, 2021).

Tabela 2 - Ataque de roubo de dados e identidade

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.

Fonte: (NAIK; GRACE; JENKINS, 2021).

4.9.3.2 Técnicas de ataque de credenciais falsas

Existem diversos vetores de ataque que exploram vulnerabilidades com o 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 à 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 os 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 3 apresenta os ataques de credenciais falsas.

Tabela 3 - Técnicas de ataque de credenciais falsas

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.

Fonte: (NAIK; GRACE; JENKINS, 2021).

4.9.3.3 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 o intuito de esgotar os recursos de processamento de um ou mais participantes 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 4 apresenta os vetores de ataque de negação de serviço.

Tabela 4 - Ataques de negação de serviço

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.

Fonte: (NAIK; GRACE; JENKINS, 2021).

4.9.4 Avaliação de Risco e Mitigação

Tabela 5 - Avaliação e mitigação de risco para ataque de roubo de dados e identidade

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.

Fonte: (NAIK; GRACE; JENKINS, 2021).

Tabela 6 - Avaliação e mitigação de risco para ataque de credenciais falsas

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.

Fonte: (NAIK; GRACE; JENKINS, 2021).

Tabela 7 - Avaliação e mitigação de risco para ataque de negação de serviço

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 provedor, implementar políticas estritas de autorização e acesso.

Fonte: (NAIK; GRACE; JENKINS, 2021).

4.9.5 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 os descritos nas Subseções 4.9.5.1, 4.9.5.2 e 4.9.5.3.

4.9.5.1 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, usar 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).

4.9.5.2 IDD e segurança em *Personal Agents*

Agentes pessoais podem executar tarefas de maneira autônoma que antes exigiam a presença ou execução pessoal, a ação dos agentes permite ganho de tempo, velocidade de execução e autonomia. Embora a utilização de agentes pessoais apresente vantagens, existem aspectos de segurança e privacidade que precisam ser abordados. Um dos primeiros aspectos está relacionado à privacidade dos dados de usuário, os agentes necessitam de contexto e uma quantidade significativa de dados de 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).

4.9.5.3 IDD e *Personal Agents for People*

A combinação de identidade digital descentralizada (IDD) e *agents* People fornece 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.

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.

1. Autonomia e Controle:

(a) IDD: proporciona aos usuários controle total sobre suas identidades e dados associados.
(b) *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.

2. Privacidade e Segurança:

(a) IDD: assegura que os dados pessoais são armazenados de forma segura e compartilhados apenas sob consentimento explícito do usuário.
(b) *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.

3. Interoperabilidade e Integração:

(a) IDD: facilita a interoperabilidade entre diferentes plataformas e serviços, utilizando padrões abertos e descentralizados para a gestão de identidades.
(b) *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.

4. Automatização de Processos:

(a) IDD: fornece a infraestrutura segura e confiável necessária para que essas automações ocorram sem riscos para a privacidade ou segurança do usuário.
(b) *Personal Agents*: podem automatizar rotinas e decisões com base nas preferências do usuário e nas informações acessíveis através da IDD.

5. Serviços Personalizados:

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

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.

4.10 Mobile Documents

Os *Mobile Documents* (*mDocs*) são documentos de identidade digitais projetados para serem armazenados no dispositivo móvel do titular e podem ser verificados tanto presencialmente quanto remotamente. Eles são baseados no padrão ISO/IEC 18013-5 e na especificação técnica 18013-7 (MATTR, 2024).

A principal vantagem dos *mDocs* em relação a outras tecnologias de credenciais digitais está na sua capacidade de fornecer autenticação e identificação robustas, possibilitando interações digitais que antes eram inviáveis devido a altos riscos de segurança. Ao oferecer níveis elevados de segurança para fluxos de verificação tanto offline quanto online, os *mDocs* permitem uma integração perfeita em diversos casos de uso em diferentes setores. Eles são particularmente ideais para credenciais de identidade de alta garantia, como passaportes e carteiras de identidade nacionais, pois oferecem proteção adicional contra falsificação, clonagem, interceptação e personificação.

Projetados para serem armazenados em uma carteira digital em um dispositivo móvel, os *mDocs* possibilitam uma vinculação segura entre o dispositivo móvel e a credencial, além de uma integração nativa mais estreita com *iOS* e *Android.* Isso significa que os fluxos de verificação de credenciais podem utilizar tecnologias de proximidade, como *Bluetooth Low Energy* (BLE).

Os *Mobiles Documents* têm foco em duas principais categorias: segurança e experiência do usuário. As funcionalidades de segurança são projetadas para garantir a integridade e a autenticidade das credenciais digitais. A autenticação dos dados do emissor permite que as partes confiáveis verifiquem a origem e o emissor de uma credencial apresentada, utilizando estruturas de dados e algoritmos criptográficos definidos no padrão ISO 18013-5. A autenticação do dispositivo assegura que a credencial foi emitida para o dispositivo específico que a apresenta, protegendo contra clonagens maliciosas. A autenticação do titular permite validar que a pessoa que apresenta a credencial é a mesma para quem ela foi emitida, podendo incluir uma foto do titular para comparação. Além disso, a criptografia de sessão estabelece um canal criptografado de ponta a ponta durante as interações, garantindo a confidencialidade dos dados transmitidos.

Com relação à experiência do usuário, os *mDocs* oferecem múltiplos fluxos de verificação, suportando interações tanto presenciais quanto remotas. Em interações remotas, os *mDocs* podem ser utilizados em fluxos de trabalho no mesmo dispositivo ou em dispositivos diferentes, conforme o padrão ISO/IEC 18013-7. Para interações presenciais, os *mDocs* permitem verificações em tempo real, mesmo offline, utilizando tecnologias como BLE para comunicação entre dispositivos. A funcionalidade de divulgação seletiva permite que os titulares compartilhem apenas as informações necessárias, preservando sua privacidade. Além disso, os *mDocs* oferecem mecanismos de revogação, permitindo que credenciais comprometidas ou inválidas sejam revogadas, mantendo a confiança no ecossistema (MATTR, 2024).

4.11 Mobile Drive Licences

As *Mobile Driver's License* (MDLs), padronizadas sob a norma ISO/IEC 18013-5, são credenciais digitais seguras que representam as informações da carteira de motorista de uma pessoa em um *smartphone* ou em outros dispositivos digitais. Oferecendo maior segurança e conveniência, as MDLs permitem que os usuários compartilhem apenas as informações necessárias para diversas interações, facilitam o acesso a serviços e reduzem o risco de roubo de identidade por meio de assinaturas digitais.

O uso de MDLs está sendo considerado devido à gama de benefícios nativos, tais como:

• **Conveniência:** reduz a necessidade de cartões físicos, diminui o risco de perda e oferece maior privacidade;

• **Privacidade:** os usuários controlam as informações compartilhadas, ao contrário dos documentos físicos, que expõem todos os detalhes;

• **Segurança:** utiliza criptografia e biometria para prevenir fraudes e acessos não autorizados;

• **Utilidade:** facilita a autenticação perfeita para atividades offline e online;

• **Eficiência:** agiliza processos e o acesso a serviços;

• **Prevenção de Fraudes:** reduz o roubo de identidade e atividades fraudulentas por meio de credenciais verificáveis;

• **Interoperabilidade:** segue padrões globais, garantindo compatibilidade entre diversas regiões e serviços.

5 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. Além disso, 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.

5.1 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)

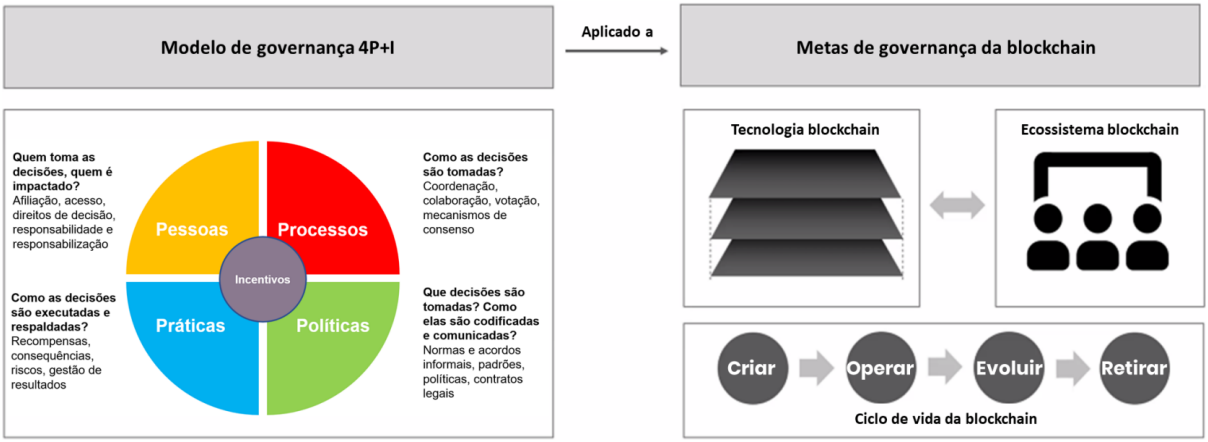
> "a governança possibilita a uma plataforma lidar com o imprevisto e o inesperado" (BARRERA, 2019)

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 15.

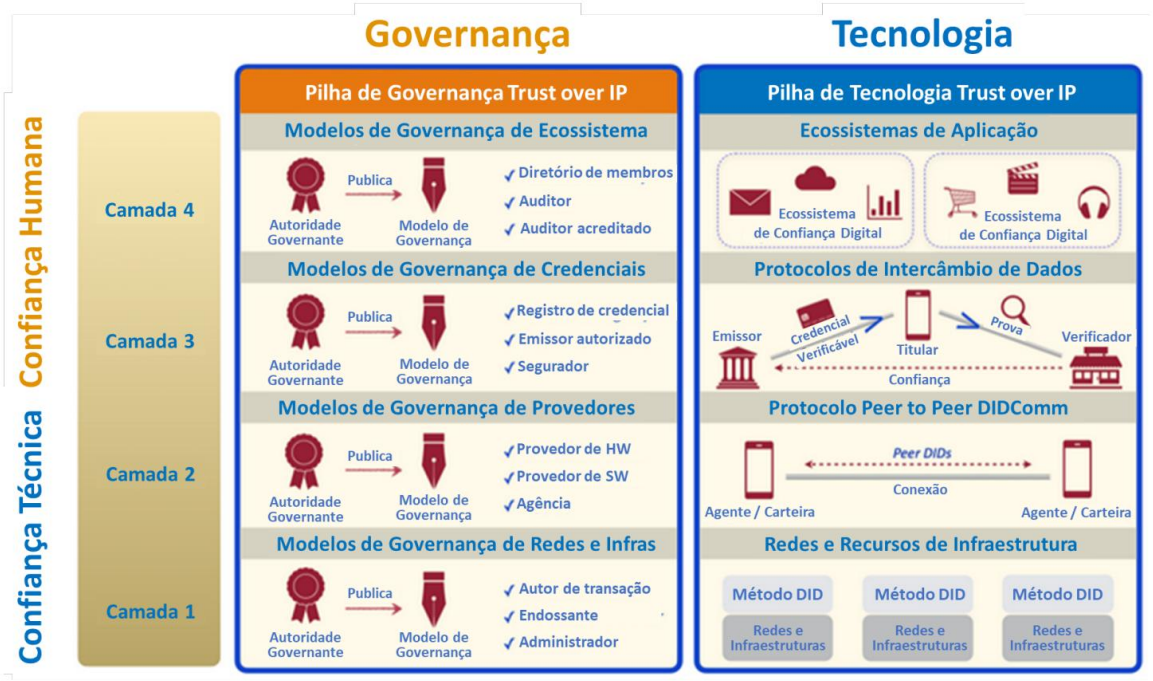
Figura 15 - Cinco dimensões do modelo aplicadas às metas de governança



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 16. 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 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 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 16 - 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 sejam 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 16, 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 8. 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.

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.

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.

5.2 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 17, 18, 19 ilustram essas respectivas fases na perspectiva da “confiança humana” da solução, ao passo que as Figuras 20, 21 e 22 o fazem na visão da “confiança técnica”.

Figura 18 - Tópicos de governança da fase de criação da camada de confiança humana

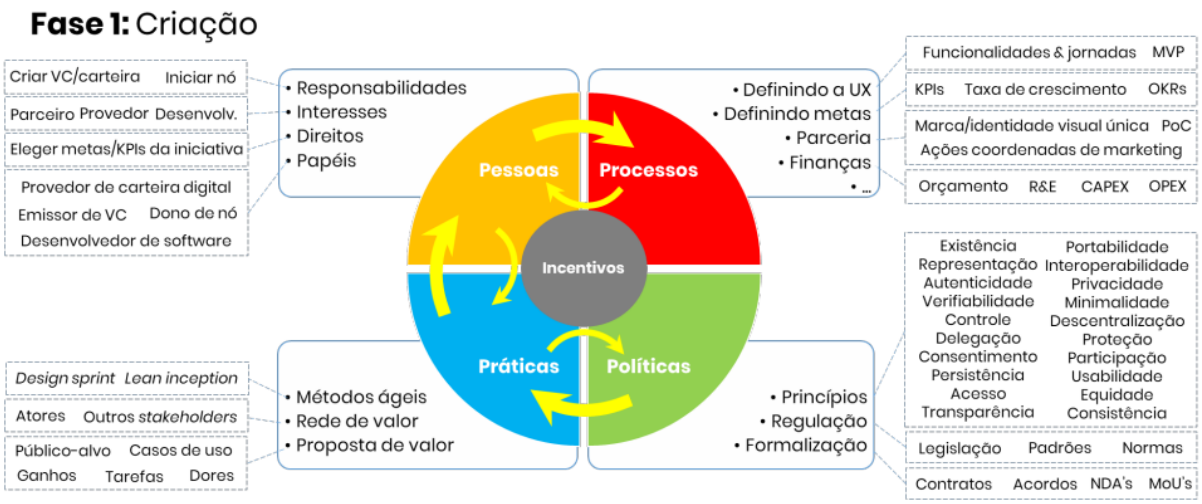


Figura 17: Tópicos de governança da fase de criação da camada de confiança humana

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.

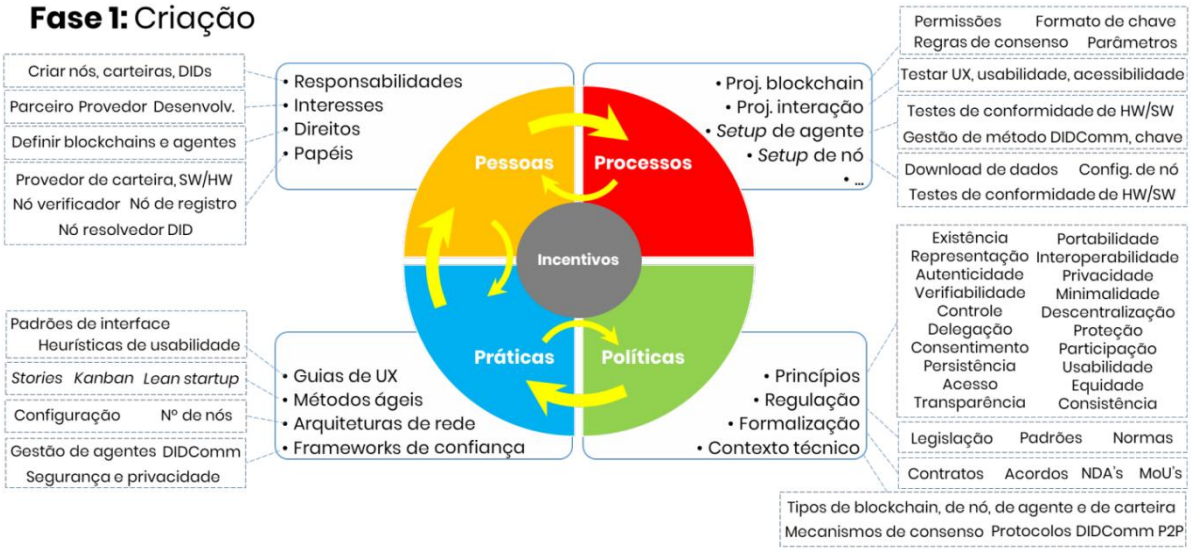
Como sugerido pelas setas amarelas mais grossas (apontando no sentido horário), há uma precedência típica entre as dimensões da governança. Parte-se das políticas, que englobam princípios fundamentais de IDD, a legislação vigente no contexto em que a solução será implementada e os contratos e acordos 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 às reiterações (indicadas pelas setas mais finas, que apontam no sentido anti-horário). Assim, por exemplo, pode ocorrer

Figura 19 - Tópicos de governança da fase de criação da camada de confiança humana

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 20 - 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 20, 21 e 22. 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 21 - Tópicos de governança da fase de Crescimento.

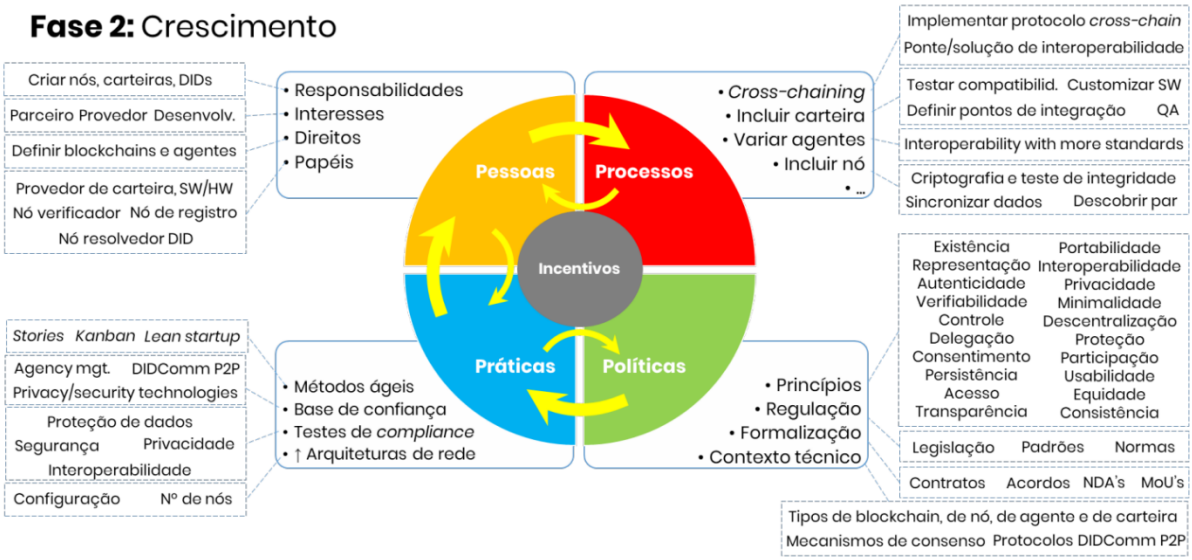
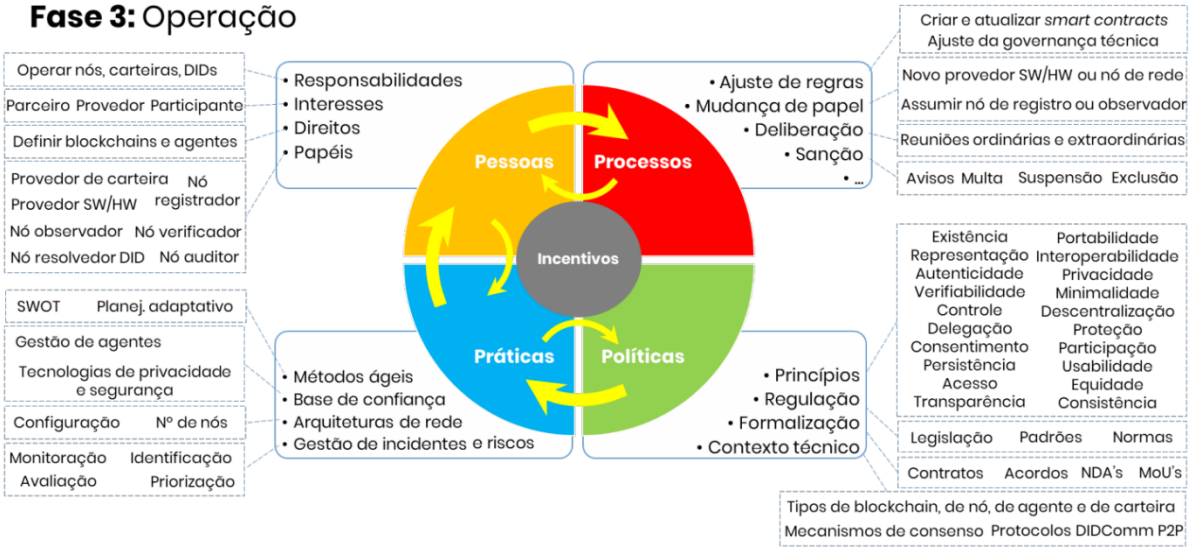


Figura 22 - Tópicos de governança da fase Operação.



5.3 Aspectos legais e regulatórios

Marcos regulatórios como a Lei Geral de Proteção de Dados Pessoais (LGPD) estabelecem diretrizes rigorosas para o tratamento de dados, promovendo a proteção da privacidade dos usuários. A interação entre a IDD e a legislação destaca um futuro promissor para o fortalecimento da segurança

digital, especialmente quando alinhada a normas internacionais como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. Esta união entre tecnologia e regulação representa um desafio, mas também uma oportunidade de desenvolver soluções robustas e confiáveis de identidade digital.

5.3.1 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).

2. 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.).

3. 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).

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.

5.3.2 A IDD e a LGPD

A relação entre a Identidade Digital Descentralizada (IDD) 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, foram definidos alguns pontos de relação importantes e como IDD suporta os princípios da LGPD, são eles:

- 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 as práticas regulatórias evoluam juntas para garantir que as promessas de ambas as abordagens sejam plenamente realizadas.

6. Conclusões

Neste relatório foi apresentado um estudo detalhado sobre identidade digital descentralizada, com uma prospecção tecnológica, passando por padronização, aspectos legais e os principais desafios referentes à IDD, conforme definido na Meta 5.1 do Projeto Ilíada.

Após uma busca na literatura e no mercado por soluções ligadas a identidades digitais descentralizadas, foram elencados os principais tópicos encontrados relacionados a este novo paradigma. O levantamento mostrou a crescente sofisticação e complexidade das soluções voltadas para IDD, revelando um cenário dinâmico e em construção. Com destaque para as iniciativas apoiadas pela União Europeia, eIDAS 2.0 e EBSI. Além disso, projetos em andamento, modelos de padronização

e interoperabilidade, frameworks, governança, mecanismos de segurança e privacidade, e LGPD também estão dentre os temas discutidos.

No ponto de vista tecnológico, pode-se destacar os avanços quanto a Zero-Knowledge Proofs, integração de HSMs com *blockchains* e soluções voltadas para escalabilidade, como o CREDEBL. Tais avanços fomentam a confiança dos usuários e podem garantir um ambiente seguro e escalável, garantindo a soberania do usuário sobre os seus dados.

Com respeito à jurisdição e aspectos legais, os desafios permanecem significativos. A conformidade com leis de proteção de dados, como a LGPD e o GDPR, exige que as soluções estejam de acordo com seus princípios legais, como minimização de dados, transparência e consentimento informado.

A governança em IDD se mostra como um fator determinante, especialmente em ambientes descentralizados, onde a ausência de uma autoridade central exige estruturas inovadoras de coordenação e responsabilização. A modelagem da governança conforme as fases do ciclo de vida das credenciais (desde a emissão até a revogação) e o desenvolvimento conceitual de modelos adaptados à realidade brasileira foram aspectos centrais abordados neste trabalho. Nesse sentido, a discussão sobre a compatibilidade com marcos legais reforça a necessidade de alinhamento entre tecnologia e regulação.

Nota-se também que há um esforço coletivo e crescente para a adoção e interoperabilidade global da IDD, por meio das iniciativas de padronização globais, discutidas aqui, como DIF e ToIP. Tais iniciativas possuem grande importância para evitar fragmentações técnicas e garantir que as soluções desenvolvidas sejam reconhecidas internacionalmente.

Assim, conclui-se que a convergência entre tecnologia, padronização e regulação é essencial para garantir que a IDD cumpra seu papel como instrumento de cidadania digital, promovendo inclusão, segurança e soberania em escala global.

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.

AJAY JADHAV. *CREDEBL Becomes an LF Decentralized Trust Project, Advancing Decentralized Identity and Verifiable Credentials for a Secure Digital Future.* 2025. Disponível em: https://www.lfdecentralizedtrust.org/blog/credebl-becomes-an-lf-decentralized-trust-project-advancing-decentralized-identity-and-verifiable-credentials-for-a-secure-digital-future. Acesso em: 22 abr. 2025.

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.

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.

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; VUKMIROVIC´, Srdan; ¯ NEDIC´, Nemanja. *State of the art of zero-knowledge proofs in blockchain. 2022 30th Telecommunications Forum (TELFOR)*. IEEE, 2022.

CARDANO. *Cardano.* 2025. Disponível em: https://cardano.org/. Acesso em: 22 abr. 2025.

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. Acesso em: 30 nov. 2024.

CREDEBL. *CREDEBL Docs.* 2025. Acessado em: 17/04/2025. Disponível em: https://docs.credebl.id/docs.

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

DIGITAL PUBLIC GOODS ALLIANCE. *CREDEBL.* 2024. Acessado em: 17/04/2025. Disponível em: https://www.digitalpublicgoods.net/r/credebl.

EIDAS 2.0. Disponível em: 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: Disponível em: https://infoscience.epfl.ch/record/296053.

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

GSMA. *Decentralised Identity.* 2025. Disponível em: https://www.gsma. com/solutions-and-impact/technologies/mobile-identity/decentralised-identity/. Acesso em: 05 maio 2025.

HYPERLEDGER IDENTUS. *Getting Started.* 2025. Disponível em: https://hyperledger-identus.github.io/docs/home/. Acesso em: 17 abr. 2025.

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

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

IEEE. *Blockchain governance standards.* 2022. Grupo de Trabalho P2145, Disponível em: https://standards.ieee.org/ieee/2145/10143/, Acessado em: 03/2024.

KRISTINA YASUDA, Michael B. Jones; LODDERSTEDT, Torsten. *Self-Issued OpenID Provider v2 - draft13.* 2023. Disponível em: https://openid.net/specs/openid-connect-self-issued-v2-1_0.html. Acesso em: 22 abr. 2025.

LF DECENTRALIZED TRUST. *Aries.* 2025. Disponível em: https://www.lfdecentralizedtrust.org/projects/aries. Acesso em: 06 maio 2025.

_____. *Hyperledger Identus.* 2025. Acessado em: 22/04/2025. Disponível em: https://www.lfdecentralizedtrust.org/projects/identus.

_____. *The open source foundation for decentralized technology ecosystems.* 2025. Acessado em: 24/04/2025. Disponível em: https://www.lfdecentralizedtrust.org/about.

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.

MASHA BORAK. *CREDEBL comes under Linux Foundation Decentralized Trust.* 2025. Disponível em: https://www.biometricupdate.com/202502/credebl-comes-under-linux-foundation-decentralized-trust. Acesso em: 17 abr. 2025.

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

MATTR. mDocs. 2024. Disponível em: https://learn.mattr.global/docs/mdocs/. Acesso em: 22 abr. 2025.

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.* 2025. Disponível em: https://openid.net/. Acesso em: 24 abr. 2025.

_____. *OpenID for Verifiable Credentials - Overview.* 2023. Disponível em: https://openid.net/sg/openid4vc/. Acesso em: 02 dez. 2024.

OPENWALLET FOUNDATION. Bifold. 2025. Disponível em: https://github.com/openwallet-foundation/bifold-wallet. Acesso em: 29 abr. 2025.

_____. *Credo Docs.* 2025. Disponível em: https://credo.js.org/guides. Acesso em: 29 abr. 2025.

_____. *The Mission.* 2025. Disponível em: https://openwallet.foundation/. Acesso em: 29 abr. 2025.

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

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.

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.

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.

SPHEREON. *Presentation Exchange with SIOP v2*. 2020. Acessado em: 22/04/2025. Disponível em: <https://sphereon.com/solution/dif-presentation-exchange-with-siop-v2/>.

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: mar. 2024.

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.

OBSERVATÓRIO
NACIONAL DE
BLOCKCHAIN