SISTEMA DE IDENTIDADES DIGITAIS AUTOSSOBERANAS: TRANSIÇÃO DA BIBLIOTECA INDY SDK PARA NOVAS TECNOLOGIAS[1]

Gabriel Felipe Cordeiro Da Silva[2], Mauricio Aronne Pillon[3].

[1] Vinculado ao projeto "Técnicas de escalonamento, precificação e impacto energético em plataformas distribuídas"
[2]Acadêmico do Curso de Tecnologia em Análise e Desenvolvimento de Sistema – CCT – Bolsista PROBIC.
[3] Orientador(a), Departamento de Ciência da computação – CCT mauricio.pillon@udesc.br

No cenário atual, as identidades digitais autossoberanas são essenciais para garantir a privacidade e a segurança dos dados dos usuários. Com esse objetivo, o Hyperledger Indy é uma plataforma de código aberto, destinada a oferecer uma solução segura e descentralizada para a identidade digital. Seu propósito é possibilitar que indivíduos e organizações administrem suas identidades digitais de maneira privada, tornando-as independentes. A plataforma disponibiliza ferramentas, bibliotecas e componentes reutilizáveis, para fornecer identidades digitais enraizadas em blockchains, ou outros livros-razão distribuídos, para que sejam interoperáveis em domínios administrativos, aplicativos e quaisquer outros silos de dados, potencializando sua descentralização.

O Hyperledger Indy Software Development Kit (**Indy SDK**), é uma das principais bibliotecas integrantes do Hyperledger Indy, e fornece as principais ferramentas para a criação de sistemas de identidades digitais descentralizadas, oferecendo uma estrutura confiável para a criação, emissão, armazenamento e verificação de identidades digitais autossoberanas. No entanto, foi descontinuada em favor das bibliotecas compartilhadas **Indy-VDR** e **Aries,** por razões relacionadas à evolução da tecnologia e a simplificação do desenvolvimento de soluções de identidade descentralizada, como:

1. **Modularidade e Flexibilidade**: Indy SDK era um pacote monolítico, combinando várias funcionalidades em uma única biblioteca. Porém, a modularidade mostrou-se mais vantajosa, permitindo o desenvolvimento independente de diferentes componentes.
2. **Foco em Interoperabilidade**: A biblioteca **Aries** foi projetada para promover a interoperabilidade entre diferentes redes e implementações de identidade descentralizada, facilitando a comunicação entre diferentes sistemas, permitindo uma integração mais fácil e um suporte mais amplo a padrões abertos.
3. **Simplificação e Manutenção**: Ao desmembrar a **Indy SDK** em componentes especializados, a manutenção e a atualização do código se tornaram mais simples e eficientes.
4. **Adoção de Novos Padrões**: As novas bibliotecas também permitem a adoção mais fácil de novos padrões e tecnologias emergentes. O foco no **Aries**, exemplificadamente, está alinhado com a adoção de protocolos de comunicação seguros e descentralizados que são essenciais para a evolução das redes de identidade descentralizada. Em resumo, com o aumento expressivo do desenvolvimento de soluções de identidade descentralizada, a transição para as bibliotecas **Indy** e **Aries** reflete uma estratégia de longo prazo da Hyperledger, para melhorar a escalabilidade, modularidade, interoperabilidade e eficiência no desenvolvimento dessas soluções.

Conforme o artigo “Hyperledger Indy: revolucionando a identidade digital”, o desenvolvimento do protótipo CottonTrust – UBA foi baseado na **Indy SDK**, como principal fonte de tecnologias para desenvolver e administrar identidades descentralizadas (DIDs). Desta forma, o principal objetivo desta IC foi analisar e compreender os métodos, para migrar o protótipo e todas as suas características, para as bibliotecas e tecnologias modernas e atualizadas. Para isso, foi necessário utilizar as seguintes tecnologias e ferramentas:

1. **Indy-VDR (Verifiable Data Registry):** módulo crucial para interação com o Indy Node Ledger, o livro-razão da rede Hyperledger Indy. Ele facilita a comunicação entre o usuário e a blockchain, permitindo a execução de operações como leitura e escrita de dados. Fornece também uma interface para que aplicativos possam realizar transações no livro-razão, como a criação de identidades digitais descentralizadas, a publicação de chaves públicas, ou a verificação de credenciais.
2. **Aries-Askar:** serviço de gerenciamento de chaves criptográficas e armazenamento seguro, projetado para funcionar com agentes do Hyperledger Aries e outros agentes de confiança digital. No contexto do Hyperledger, um "agente" é um software que gerencia identidades descentralizadas e interage com outros agentes para realizar transações seguras. O Aries Askar fornece uma camada de segurança ao armazenar dados criptográficos sensíveis, como chaves privadas, credenciais, e outros segredos criptográficos, em um formato criptografado.
3. **Anoncreds (Anonymous Credentials):** refere-se a um sistema de credenciais criptográficas anônimas, projetado para proteger a privacidade dos usuários enquanto fornece verificação confiável de credenciais em redes blockchain. No contexto do Hyperledger Indy, o Anoncreds permite que um usuário prove que possui uma credencial sem revelar informações pessoais subjacentes. Por exemplo, um usuário pode provar que tem mais de 18 anos sem divulgar sua data de nascimento exata.
4. **Hyperledger Aries Cloud Agent Python (ACA-Py):** Implementação em Python de um agente baseado no Hyperledger Aries para operar em ambiente de nuvem. O agente gerencia carteiras digitais e identidades descentralizadas, armazenando credenciais verificáveis, chaves criptográficas e informações de identidade digital. Além disso, o ACA-Py facilita a comunicação entre agentes por meio de protocolos padronizados, permitindo transações seguras em uma rede blockchain.

Em suma, essas novas bibliotecas, individualmente, proporcionam uma gestão eficiente das identidades digitais, cada uma com um propósito específico, mantendo a privacidade dos dados. No entanto, um sistema complexo depende da combinação entre as tecnologias e essa migração exige que a arquitetura dos sistemas baseados na **Indy SDK** seja completamente reestruturada para integrar novas tecnologias.Durante a execução desta bolsa de pesquisa, foram observadas e estudadas as barreiras na atualização dos algoritmos, devido a fatores como a falta de compatibilidade entre as bibliotecas recomendadas. Como resultados operacionais, tem-se a atualização do protótipo operacional do CottonTrust - UBA, entretanto, não foi possível durante o escopo da IC, converter todas as funções e operações que caracterizam o sistema. Como trabalhos futuros a curto prazo estão: (i) verificação de erros do ambiente; (ii) atualização total do protótipo para tecnologias modernas; (iii) comparação de desempenho dos sistemas.

Palavras-chave: Indy SDK, identidade digital autossoberana, CottonTrust.