**Proposta para Grupo de Trabalho Fase 2 – Ciclo 2021-2022**

GT-ChainID - PLATAFORMA PARA GESTÃO DE IDENTIDADES DESCENTRALIZADAS ATRAVÉS DA BLOCKCHAIN

Fabíola Greve

26 de setembro de 2021

## 1. Título

ChainID - Plataforma para gerenciamento de identidades descentralizadas através da blockchain

## 2. Coordenadora Geral

Fabíola Gonçalves Pereira Greve
Profa. titular do Instituto de Computação
Universidade Federal da Bahia (UFBA)
*Lattes: http://lattes.cnpq.br/0120615995402345*
*LinkedIn: https://www.linkedin.com/in/fabiolagreve,*
*fabiola@ufba.br; Cel.: (71) 99302-7775*

## 3. Assistente de Inovação

Patrícia Santiago da Silva.

Analista de Negócios Sênior. Experiência de mais de 15 anos com gestão de pessoas, processos e qualidade voltados para ambientes robustos de infraestrutura, implantando os processos baseados em ITIL como também fazendo a sua gestão. Ampla vivência na implantação de Service Desk e das ferramentas de ITSM (Footprints, GLPI e CA SDM) sempre com vistas às boas práticas e em auditorias para certificação das ISO´s 9000, 14000 e 20000.

*patricia.santiago@gmail.com; Cel.: (71) 988240263*
*LinkedIn: https://www.linkedin.com/in/pssantiago*

## 4. Resumo

A identidade é fundamental para o reconhecimento das entidades (indivíduos, coisas e organizações) e das suas diversas relações. Uma tendência emergente e disruptiva consiste em oferecer identidades descentralizadas, sob controle do próprio usuário, que passa a ter soberania sobre seus dados. O projeto ChainID apresenta uma plataforma para gestão de identidades descentralizadas (IDD) através da blockchain, que contempla atributos e credenciais das IDDs, e é suficientemente genérica para abstrair a complexidade dos padrões e protocolos de comunicação envolvidos. A plataforma proporciona o uso da infraestrutura de IDD em diversos fluxos de oferta de serviços, de forma segura e transparente, facilitando o desenvolvimento de aplicações com IDD por clientes que não dominam necessariamente a tecnologia. Uma gama de aplicações com uso de IDD pode ser oferecida através da ChainID, sendo que um serviço de autenticação está desenvolvido e disponível para integração numa infraestrutura federada, como a CAFe.

## 5. Abstract

Identity is fundamental for the recognition of entities (individuals, things and organizations) and their various relationships. An emerging and disruptive trend is to offer decentralized identities, under the control of the user, who now has sovereignty over their data. The ChainID project presents a platform for managing decentralized identities (IDD) through the blockchain, which includes attributes and IDD credentials, and is generic enough to abstract the complexity of the communication standards and protocols involved. The platform provides the use of IDD infrastructure in various service delivery flows, in a secure and transparent way, facilitating the development of IDD applications by customers who do not necessarily dominate the technology. A range of applications using IDD can be offered through ChainID, and an authentication service is developed and it is available for integration in a federated infrastructure, such as CAFe.

## 6. Parcerias e respectivas contrapartidas

**(1) Universidade Federal da Bahia (UFBA) - grupo de pesquisas Gaudi** do Departamento de Ciência da Computação. O projeto tem coordenação do Gaudi Grupo de Algoritmos e Computação Distribuída, liderado pela Profa. Fabíola Greve, especialista em desenvolvimento de sistemas distribuídos confiáveis, sendo pioneira em pesquisas em blockchain no Brasil. Tem larga experiência na coordenação de projetos

nacionais e internacionais. A equipe proponente irá modelar, projetar, implementar e acompanhar o desenvolvimento da plataforma em todas suas etapas.

**(2) Universidade Federal da Bahia (UFBA) - Superintendência de Tecnologia da Informação (STI)** - Técnicos da STI serão parceiros para carga e manipulação dos dados da comunidade UFBA para prova de conceitos e testes.

**(3) Instituto Federal da Bahia (IFBA)** - A equipe do Prof. Allan Freitas irá auxiliar na construção do ambiente de testes e nos testes da ferramenta.

## 7. Descrição da evolução do MVP com destaque para a entrada no NasNuvens da RNP

### 7.1 Contextualização

A identidade é fundamental para o reconhecimento das entidades (indivíduos, coisas e organizações) e das suas diversas relações no contexto em que estão inseridas. Prover Gestão de Identidade (GId), conjunto de processos e tecnologias utilizados para garantir a identidade de um usuário ou dispositivo, garantir a qualidade das informações de uma identidade e prover autenticação, autorização e auditoria, é um ponto chave para possibilitar a criação e manutenção das Organizações Virtuais (OVs).

Para realizar interoperabilidade entre topologias mais complexas, onde os círculos de confiança incluem várias autoridades e provedores de serviço, é interessante que a responsabilidade pelos processos de interoperabilidade seja realizada por uma terceira parte confiável que atue em ambas as federações e que implemente os padrões a serem interoperáveis. Por outro lado, os próprios usuários convivem com diversas formas de identificação, e.g., matrículas, CPF, RG, diversos logins/senhas para acesso aos serviços, que se faz de forma ad-hoc, em alguns casos, estão sujeitos a fragilidades de segurança e usos indevidos dos seus dados, e sem o devido consentimento.

Os ambientes federados destacam-se como modelo de GId no qual as instituições parceiras são associadas como federações utilizando um conjunto de atributos, práticas e políticas para troca de informações e serviços. Apesar de proverem uma solução simples para o usuário, apresentam problemas ao gerir usuários que precisam colaborar em mais de uma federação. Até então centralizados ou federados, os sistemas de GId podem evoluir para um modelo descentralizado e autossoberano, no qual, com identidade digital descentralizada (IDD) e autossoberana, o próprio usuário passa a ser o administrador das informações sobre sua identidade [Kubach et al. 2020], e esta, inclusive, possibilita a criação de um identificador global único e compartilhável em todo o ecossistema.

### 7.2 O Desafio

A IDD consolida então os frutos dos modelos anteriores e avança no estabelecimento de uma autossoberania do usuário no controle da sua identidade, que se faz de forma segura e universal. Tal quebra de paradigma, do centralizado para o descentralizado, inverte o fluxo dos modelos tradicionais e provoca uma mudança estrutural nas arquiteturas e sistemas de GId.

Contudo, as especificações de IDD são recentes e sem maturidade, alguns poucos sistemas começam a despontar no sentido de propor uma implementação desse novo

paradigma de identidade descentralizada [Liu et al. 2020] sem estabelecer padrões comerciais. Os principais exemplos são o da rede *SOVRIN* [Tobin and Reed 2017] para blockchains permissionadas, e utiliza o arcabouço *Hyperledger Indy* (HLI) e *Aries* (HLA), e UPORT [Naik and Jenkins 2020], que atende ao padrão de blockchain aberta da *Ethereum*. Entretanto, resta o provimento de diversos componentes, arcabouços e plataformas capazes de construir tal ecossistema IDD para desenvolvimento de aplicações de maneira segura, transparente, extensível e confiável.

### 7.3 A Plataforma ChainID

A **ChainID** consiste numa plataforma para gestão de identidades descentralizadas que fornece uma arquitetura baseada em serviços com o objetivo de facilitar a criação de aplicações e serviços utilizando Identidades Digitais Descentralizadas (IDDs) com agilidade, rapidez e transparência. Estas características são proporcionadas ao incorporar a complexidade de um ecossistema descentralizado e assíncrono (infraestrutura, protocolos de comunicação, padrões e demais componentes próprios de soluções com IDD) em uma plataforma de serviços com baixo acoplamento e baixo esforço de integração.

O projeto **ChainID** utiliza as especificações W3C de IDD[1] e Credenciais Verificáveis[2] como *core* da plataforma para gestão de identidades descentralizadas (IDD) através da blockchain, contempla atributos e credenciais de forma suficientemente genérica para abstrair a complexidade dos padrões e protocolos de comunicação envolvidos.

A **ChainID** oferece uma *API* (*Application Programming Interface*) e suporte a tratamento de eventos, que permitem que aplicações externas possam ser integradas à solução de forma facilitada, abstraindo a complexidade de protocolos e infraestrutura. Desta forma, tanto aplicações legadas, quanto novas aplicações, podem ser beneficiadas com a privacidade, a soberania e a segurança no compartilhamento de informações proporcionada por soluções utilizando IDD.

A orquestração provida pelo **ChainID *Workflow*** é outro ponto de destaque da plataforma. Este componente ajuda a gerenciar fluxos de trabalho e tarefas complexas com mais facilidade, dando oportunidade a abordagens que facilitem implantar aplicações mais rapidamente. As operações entre os agentes utilizados em um ecossistema de IDD são complexas, assíncronas, repetitivas e padronizadas pelas especificações das infraestruturas de base para IDD, como o *Hyperledger Aries*. Desta forma, as operações com IDD foram mapeadas em fluxos contendo chamadas orquestradas a serviços de forma a automatizar o processo.

Buscando facilitar o gerenciamento das identidades de forma flexível, ágil e com baixa complexidade, a plataforma **ChainID** disponibiliza uma aplicação cliente chamada **ChainID Console**. Esta aplicação funciona como um configurador e possui uma interface com fluxos simplificados para a criação de credenciais, requisições de prova e revogações de credenciais. Para um serviço de autenticação, a console é um facilitador na administração das credenciais possibilitando a construção da estrutura da credencial através da definição dos atributos que a compõem, com a facilidade de uma interface web e a publicação na blockchain com apenas alguns cliques.

### 7.4 Benefícios

Como proposta de valor da plataforma **ChainID** é possível elencar: **(i) Maior privacidade dos dados.** A plataforma oferece uma solução essencialmente autossoberana com a utilização de uma blockchain especializada em identidade; **(ii) Maior segurança no compartilhamento.** O protocolo de compartilhamento de credenciais verificáveis associado às características da blockchain fornece um arcabouço seguro para identificação de pares no compartilhamento de informações, além de verificação de conteúdo, emissores e titulares das credenciais; **(iii) Flexibilidade.** A plataforma **ChainID** fornece suporte para a criação de soluções flexíveis com a criação da estrutura, emissão e prova de credenciais verificáveis; **(iv) Adequação à LGPD.** A exigência da privacidade e proteção de dados de usuários é real e pode ocasionar multas ou sanções. A **ChainID** oferece soluções *by design* com interoperabilidade e escalabilidade como um software como serviço; **(v) Interoperabilidade e escalabilidade.** As organizações possuem diversas aplicações legadas desenvolvidas em várias tecnologias e protocolos. A **ChainID** fornece interoperabilidade com diversos protocolos e tecnologias de mercado através do uso de serviços e eventos; **(vi) Solução com baixo acoplamento e integração facilitada.** Além dos custos de aquisições de soluções, os gestores se preocupam com o esforço de integração da solução com suas aplicações. A **ChainID** através de suas arquitetura baseada em eventos beneficia seus clientes com várias possibilidades de integração e a possibilidade de desenvolvimento de tantas outras; **(vii) Alinhamento com aplicações descentralizadas via blockchain.** A plataforma **ChainID** utiliza a tecnologia blockchain como infraestrutura para armazenamento de chaves públicas, identificadores descentralizados e estruturas de credenciais de forma a possibilitar o compartilhamento e a validação de credenciais pelos utilizadores da rede. Desta forma, garantindo a escalabilidade, replicação e failover da solução e das aplicações que utilizem a plataforma.

### 7.5 Aplicabilidade e Instituições interessadas

A plataforma **ChainID** proporciona o uso da infraestrutura de IDD em diversos fluxos de oferta de serviços, de forma segura e transparente, facilitando o desenvolvimento de aplicações com IDD por clientes que não dominam necessariamente a tecnologia.

Diantes das potencialidades do uso da plataforma **ChainID** na criação de aplicações com IDD incorporando privacidade, soberania, identificação do usuário, compartilhamento seguro e verificável de informações, identificamos algumas aplicações que podem ser desenvolvidas com o objetivo em atender a esses propósitos acima, tais como: Passaporte de Vacinação COVID, Controle de Acesso,
Votação Eletrônica, Diploma Digital e Prontuários Eletrônicos.

Instituições, incluindo **UFBA, IFBA, UFPB(LedgerTec)** demonstraram interesse em utilizar a plataforma e seus serviços para implementar as seguintes soluções:

**I - *Chain Moodle*: Autenticação do Moodle utilizando o serviço de autenticação IdP Blockchain.**

Alguns cursos oferecidos pela universidade possuem como público alunos da própria instituição, de instituições parceiras ou de pessoas sem vínculos com instituições de ensino. Suportar esta necessidade requer a configuração de mecanismos de

autenticação alternativos, configurações na Active Directory e/ou criação de novas instâncias do moodle.

Com a adoção da autenticação com credenciais verificáveis, apenas usuários detentores da credencial para determinado semestre ou cursos podem acessar o Moodle, facilitando o gerenciamento de identidade e reduzindo o *overhead* da equipe.

**II - *Chain 2FA*: Adição de segundo fator de autenticação a aplicações legadas.** Apesar da autenticação utilizando o **IdP Blockchain** promover uma identificação sem a necessidade de um segundo fator de autenticação, existem aplicações legadas que utilizam autenticação local e necessitam adicionar um novo fator de autenticação para garantir o acesso. Como requisito não funcional, a instituição indicou: (i) facilidade de integração, (ii) pouca modificação do atual comportamento da aplicação, (iii) tratar vulnerabilidade das soluções atuais a ataques utilizando engenharia social. A solução proposta é a utilização de credenciais verificáveis para a identificação do usuário e realizar a integração com a plataforma **ChainID** através da transferência dos dados do usuário utilizando um token JWT (*Jason Web Token)*.

**III - *Chain Diploma*: Carteira com credencial de diploma digital.**

A **LedgerTech**, Startup do projeto V4H, tendo como coordenador acadêmico o Prof. Guido Lemos, demonstrou interesse na solução de autenticação utilizando o **IdP Blockchain** como mais um método de autenticação do usuário em sua plataforma. Nesse sentido, podemos desenvolver uma carteira para oferecer IDD para os estudantes, e de forma a representar o diploma como um de seus atributos. Tal solução pode agregar valor ao V4H, bem como a outros projetos de diplomas digitais em curso.

O ponto em comum destas soluções é a necessidade em obter informações sobre usuários que, em sua grande maioria, são informações sensíveis, de maneira a identificá-los para uma tomada de decisão. Assim, estas aplicações atuam essencialmente como verificadores de credenciais e são beneficiadas pelo baixo acoplamento e facilidade de integração da **ChainID**.

Os clientes, emissores das credenciais, são beneficiados com a facilidade em modelar, publicar e emitir credenciais com uso dos serviços básicos e do console da plataforma **ChainID**, sem a necessidade de preocupação com o ciclo de vida oriundo da tecnologia de identidades descentralizadas, tais como: mudanças de especificações e fornecedores de tecnologias

Além dos benefícios imediatos na construção das aplicações, a utilização de credenciais verificáveis dispensa o uso de barramentos de comunicação ou serviços de consulta de dados pelo emissor. As informações são armazenadas e trafegadas na *wallet* do usuário, tendo sua comunicação realizada entre o usuário e a aplicação por intermédio da **ChainID**, de forma assíncrona e reduzindo consideravelmente a infraestrutura necessária para o desenvolvimento desta natureza. Desta forma, proporciona-se o compartilhamento de informações entre organizações de maneira elegante e com baixo acoplamento.

Fechando a tríade de confiança (Emissor + Titular + Verificador), pilar da especificação das credenciais verificáveis da *W3C*, os titulares, usuários finais das credenciais e aplicações das mesmas, serão beneficiados com a extensão de serviços com maior segurança, experiência e soberania sobre seus dados.

### 7.6 GT FASE 1

O desenvolvimento no primeiro ano do **GT-ChainID** permitiu identificar a viabilidade de uso da plataforma em diferentes cenários de autenticação, tornando-a um método viável de autenticação e autorização de diversas instituições brasileiras, públicas e privadas.

A Fase 1 do projeto **ChainID** foi constituído das seguintes atividades chave: (i) Concepção e desenvolvimento da arquitetura de referência do projeto; (ii) Concepção e desenvolvimento dos serviços básicos de gerenciamento das IDDs: emissão, revogação e prova; (iii) Concepção e desenvolvimento do serviço de autenticação baseado, IdP SAML compatível com os padrões de atributos da federação CAFe, utilizando credenciais verificáveis e os serviços básicos da plataforma; (iv) Construção de aplicação **ChainID Console** com uma aplicação cliente para facilitar o gerenciamento das identidades: Modelagem de atributos, implantação e revogação; (v) Elaboração e criação da página principal do projeto; (vi) Elaboração e criação do modelo de negócio inicial do projeto; (vii) Elaboração e criação da *landing page*; (vii) Identificar e validar a proposta de valor do projeto com a realização de entrevistas.

Os principais serviços da plataforma **ChainID** são: **(i) Emissão de credenciais** é um processo pelo qual uma credencial verificável é atribuída ao titular. No serviço de emissão na plataforma **ChainID** o emissor, organização cliente, possui os dados do titular, emite a credencial informando os valores para os atributos. A emissão de credenciais a titulares pelas organizações, além de registrar os dados, encaminha a solicitação de credencial ao titular; **(ii) Solicitação de prova** é o processo pelo qual uma credencial verificável pode ser apresentada e validada. Neste processo existem dois atores: o titular e o verificador. O titular é o ator que realiza a prova apresentando sua credencial; **(iii) Revogação de credenciais** é o processo pelo qual um emissor invalida uma credencial emitida a um titular. Uma credencial revogada não pode ser utilizada para apresentação de provas.

O serviço de autenticação é o primeiro serviço de negócio disponibilizado pela plataforma **ChainID**, sendo implementado a partir da orquestração de serviços básicos associado a capacidade da plataforma em interoperar com diversos padrões e aplicações, além do desenvolvimento de um IDP (denominado aqui por **IDP Blockchain**) para uma rede federada, tal como a rede CAFe (Comunidade Acadêmica Federada) da Rede Nacional de Ensino e Pesquisa (RNP).

Como resultado, é possível autenticar e identificar usuários utilizando credenciais verificáveis, sem a utilização de bases centralizadas, respeitando a privacidade e a soberania do usuário sobre seus dados, além de mitigar o risco de acessos não autorizados a dados pessoais armazenados em bases centralizadas. Desta forma, o **IDP Blockchain** se apresentou uma solução elegante e não intrusiva que funciona com um broker. Não persiste dados de usuários, apenas processa e encaminha as informações necessárias às aplicações com uso do protocolo *SAML2*. A compatibilidade com outros protocolos, como Oauth e CAS, serão disponibilizados em breve

### 7.7 Modelo de Negócio

O modelo de negócio da plataforma **ChainID** foi desenvolvido, inicialmente, utilizando a metodologia proposta por Steve Blank, na qual os principais aspectos de um novo negócio são mapeados de forma visual através do Canvas e refinados com o uso de

entrevistas e análises de mercado. O resultado desta metodologia é apresentado nas próximas seções, as quais apresentam as principais características da plataforma como um negócio detentor de um produto com mercado consumidor identificado.

### 7.7.1 Segmento de Clientes

O segmento de clientes da plataforma **ChainID** é formado por ***early adopters*** que precisam de uma solução *by design* com IDD para atender às necessidades exigidas pela LGPD/GDPR, promover maior privacidade e segurança dos dados e oferecer compartilhamento seguro de informações seguindo o modelo ***Business to business* (B2B) institucional**, inicialmente, sem a possibilidade de revenda. Enumeradamente são instituições de ensino e pesquisa e empresas parceiras da RNP, como por exemplo a Universidade Federal da Bahia (UFBA) que demonstrou interesse na solução.

Os usuários da plataforma **ChainID** são formados, em ordem de grandeza: alunos, servidores, terceirizados e colaboradores/clientes das organizações parceiras.

### 7.7.2 Canais

Os canais de distribuição escolhidos pelo projeto **ChainID** para alcançar e se comunicar com seus consumidores estão segmentados da seguinte maneira: **(i) Conscientização.** Voltado a publicidade do projeto e seus serviços, tem objetivo em apresentar a proposta de valor da plataforma. A natureza do serviço, assim como o seu segmento de clientes, faz dos eventos científicos e de inovação um canal natural no alcance de novos clientes. A RNP já promove ou apóia diversos eventos científicos no Brasil, assim como tem uma presença destacada na comunidade científica brasileira. Através das suas ações, a RNP auxiliará o **ChainID** ampliar o seu conjunto de usuários em tais oportunidades; **(ii) Avaliação.** Voltado a avaliação e fonte de informações do projeto e produto, possuem como objetivo obter as opiniões do cliente sobre a proposta de valor e a sua perspectiva em relação aos concorrentes do projeto. A página principal e a *landing page* do projeto serão atualizados, incluindo informações complementares, documentações do projeto, *white paper*, atualização do formulário de pesquisa e contato; **(iii) Compra, entrega e pós venda.** Voltado para o processo de compra, venda, entrega e atendimento do serviço ao cliente. A plataforma de *marketplace* computacional (serviços e infraestrutura) criado pela RNP, com a parceria da CAPES, une em um mesmo local, a consultoria, a gestão, a contratação de soluções e infraestrutura em um modelo totalmente pensado para o setor público, fornece um broker de serviços completo, com *IaaS*, *SaaS*, *PaaS*, aplicativos e serviços. É o canal escolhido para o projeto **ChainID.** Atende aos principais requisitos e modelos de contratação para instituições públicas. Para cada tipo de serviço ofertado existe o modelo certo que reduz tempo e facilita a contratação e a implantação das soluções. Com a adoção do NasNuvens, critérios de padronização do produto, conhecimento e credibilidade do canal são atendidos, além do excelente relacionamento da RNP com o público alvo. Além de critérios negociais, a plataforma fornece características técnicas interessantes para a evolução, aprovisionamento e melhorias necessárias ao projeto: a existência de soluções padronizadas e efetivas, tais como a utilização de scripts de automação com ansible, possibilida escalar a solução de maneira rápida e sustentável.

### 7.7.3 Fonte de Receita

A fonte de receita para o projeto **ChainID** foi elaborada a partir de previsões, levando em consideração a situação atual do segmento de mercado, a atratividade financeira, possibilitar e flexibilidade em atender organizações de diversos tamanhos, aumentar a receita com o aumento do valor da organização, além de ser compatível com o canal de compra, entrega e pós venda escolhido, o NasNuvens. Desta forma, a principal forma é a comercialização dos produtos e serviços da plataforma será via venda de pacotes e serviços com a cobrança de taxa de uso de transações. Uma transação é definida pela menor operação executada na plataforma. Exemplos de transações são: Criação, emissão e revogação de credenciais. Este modelo de comercialização é chamado *SaaS*, do inglês *Software as a Service,*

Além do pagamento pela utilização da plataforma, outra fonte de receita provida pela capacidade da plataforma em oferecer um framework para a construção de aplicações descentralizadas, é o desenvolvimento de aplicações e serviços, projeto de integração com sistemas legados e implantação da solução nas organizações cliente, através da contratação de consultoria e mão de obra especializada do projeto.

### 7.7.4 Parceiros

A **RNP** é o principal parceiro da plataforma **ChainID**, sobretudo em função do seu protagonismo frente às instituições acadêmicas no Brasil através da federação CAFe. Os usuários que fazem acesso aos serviços do atual marketplace nasnuvens.rnp.br são os usuários iniciais da solução.

A **Universidade Federal da Bahia (UFBA) e o Instituto Federal da Bahia (IFBA)** são parceiros do projeto ao demonstrarem interesse em utilizar os serviços da plataforma **ChainID**, fornecerão dados para execução dos experimentos de validação e melhoria contínua, e apoio no desenvolvimento do ambiente de testes na rede de identidade orquestrada pelo CT-Blockchain, com a implementação de um nó validador, e na realização dos testes da ferramenta neste ambiente. Desta forma, o projeto se beneficia com a possibilidade de realizar simulações e pilotos dos serviços oferecidos para essas comunidades acadêmicas e promove novas parcerias e clientes parceiros do CT-Blockchain.

## 7.8. Evolução da ChainID (Atividades Chave Fase 2)

A Fase 1 teve como principal objetivo elaborar e desenvolver a arquitetura da plataforma atribuindo a capacidade de manter-se alinhada com as constantes evoluções da academia e avanços científicos da tecnologia: adicionando/removendo protocolos, fornecedores e componentes; com transparência e resiliência a fim de garantir o funcionamento pleno dos contratos estabelecidos entre os clientes e os serviços oferecidos. Como próximos desenvolvimentos, temos:

**APERFEIÇOAR PLATAFORMA ChainID e IdP**

- Realizar experimentações e laboratórios com as instituições parceiras e interessadas no projeto. O objetivo desta atividade: (i) validar os serviços desenvolvidos na Fase 1, (ii) identificar necessidades ainda não mapeadas, (iii) realizar melhorias e correções nos modelo de negócio modelado tendo como

principal premissa a necessidade das instituições e as limitações/impedimentos do produto que dificultam sua adoção;

- Realizar testes de usabilidade com os usuários finais da instituição UFBA: alunos, professores e técnicos administrativos com a finalidade em orientar o desenvolvimento da *wallet* e melhorar a experiência do usuário final
- Realizar testes de usabilidade do console com os clientes institucionais com a finalidade em orientar as melhorias da interface e o desenvolvimento de novas funcionalidades;
- Realizar testes no ambiente de homologação do CAFe, o Chimarrão, além de avaliações da solução com o GIDLab;
- Adicionar resolução universal de redes, *did methods*, de forma a propiciar a solução de identidades em diferentes redes e tecnologias, aumentando a interoperabilidade e a portabilidade da solução. Como por exemplo, a resolução de IDD na Lacchain ( *did method* did:lac:), promovendo a resolução destes identificadores além da possibilidade de cooperação técnica;
- Adicionar suporte a HUB de atributos de forma a determinar um cache dos mesmos com permissão de acesso e data de expiração, como forma de melhorar a usabilidade do usuário final ao apresentar suas credenciais em fluxos repetitivos e que permitam estabelecer regras claras para o uso deste recurso;
- Adicionar suporte a outros protocolos de autenticação ao IDP, como o Outh2 e CAS;
- Melhorar a arquitetura atual adicionando processamento assíncrono de eventos através da inclusão de filas, proporcionando maior resiliência, baixo acoplamento, tolerância a falhas, melhor manutenibilidade dos componentes e *downtime* do serviço;
- Construir clientes para a plataforma em diversas linguagens de programação: java, python, php e javascript;
- Reformular a *landing page*, site principal e formulário de coleta de dados

**IMPLANTAR Solução no NasNuvens**

- Implementar método de *onboard*, criar o identificador descentralizado para o usuário, utilizando as identidades federadas ou locais, em um modelo semelhante ao utilizado pelo serviço de emissão de certificado digital pessoal do ICP-EDU. Esta atividade também engloba a integração com a interface administrativa *JamCracker* de forma a permitir que os administradores das instituições consigam determinar a forma de identificação do usuário durante o *onboard*: autenticação federada ou usuário local. O fluxo de *onboard* pode ser realizado via aplicação web ou via *wallet* própria do projeto;
- Para proporcionar o mecanismo de *onboard* e a inclusão de alguns serviços específicos a serem disponibilizados pelas instituições clientes do **ChainID**, será necessária a construção do *wallet* próprio do projeto, além de adicionar mecanismos adicionais de segurança e resiliência, tais como: backup/recovery, biometria entre outros identificados durante a experimentação da plataforma e seus serviços;
- Criar mecanismo de tarifação e bilhetagem de acordo com os padrões estabelecidos pela plataforma NasNuvens da RNP;
- Alterar o console para realizar a autenticação utilizando o IDP do CAFe;

- Criar pilhas de aplicações necessárias a implantação da plataforma;
- Criar scripts de automação com ansible para o aprovisionamento e configuração de *assets* do projeto;
- Construir termo de uso;
- Criar loja do ChainID na plataforma Nasnuvens da RNP.

**DESENVOLVER O *Chain Diploma***

- Realizar aproximação com o MEC, LedgerTech e RNP para a criação do serviço *"Diploma na palma da mão"*, na qual será possível compartilhar as informações do diploma utilizando credenciais verificáveis, tornando a validação de títulos mais rápida, confiável e simplificada;
- Elaborar plano de trabalho para a integração do serviço de diploma aos serviços da plataforma;
- Desenvolver solução de acordo com o plano de trabalho;
- Realizar validação da solução e execução de piloto em uma das instituições parceiras.

***DESENVOLVER 2FA* e *Chain Moodle***

- Realizar entrevistas e análise essencial com os gestores da UFBA para identificar os requisitos para integração, quais as aplicações serão integradas e qual o protocolo será usado a partir dos serviços da plataforma base do **ChainID**;
- Desenvolver plano de trabalho para o projeto de integração das bases de dados das organizações à plataforma;
- Elaboar plano de trabalho para a integração do serviço de diploma aos serviços da plataforma;
- Desenvolver solução de acordo com o plano de trabalho;
- Realizar validação da solução e execução de piloto em uma das instituições parceiras.

**IDENTIFICAR novos Serviços junto à RNP e AMPLIAR parcerias.**

- Realizar entrevistas e análise essencial com os gestores da RNP para identificar novos serviços a serem disponibilizados a partir dos serviços da plataforma base do **ChainID**;
- Realizar entrevistas e análise essencial com os gestores da EBSERH;
- Estabelecer parceria com o CT-Blockchain para a implantação da rede de identidade nacional, incluindo um nó validador em parceria com a instituição parceira UFBA;
- Realizar testes e análise da solução na rede Indy de teste orquestrada pelo CT-Blockchain e conta com parceiros do ecossistema RNP, além de governo e indústria.

## 8. Cronograma de marcos

| Entregas (E) e Atividades (A) | Mês | Prazo |
|---|---|---|
| | | |

| | | 2021 | | | | 2022 | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | SET-OUT | OUT | NOV | DEZ | JAN | FEV | MAR | ABR | MAI | JUN | JUL | AGO | SET | OUT | NOV | DEZ | |
| E4 | Plano de Desenvolvimento da Modelagem do Produto/Serviço | | | | X | | | | | | | | | | | | | 12/15/2021 |
| E4.1 | Realizar experimentações e laboratórios | | X | X | X | | | | | | | | | | | | | |
| E4.2 | Realizar testes de usabilidade com os usuários finais da instituição UFBA | | X | X | X | | | | | | | | | | | | | |
| E4.3 | Realizar testes de usabilidade do console com os clientes institucionais | | X | X | X | | | | | | | | | | | | | |
| E4.4 | Realizar testes no ambiente de homologação do CAFe | | X | X | X | | | | | | | | | | | | | |
| E4.5 | Elaborar plano de trabalho a partir dos dados coletados | | | | X | | | | | | | | | | | | | |
| E5 | Primeira Versão do Catálogo de Serviços do GT | | | | | X | | | | | | | | | | | | 1/31/2022 |
| E5.1 | Realizar entrevistas e análise essencial com os gestores da RNP | | X | X | X | X | | | | | | | | | | | | |
| E5.2 | Realizar entrevistas e análise essencial com os gestores da EBSERH | | X | X | X | X | | | | | | | | | | | | |
| E5.3 | Estabelecer parceria com o CT-Blockchain para a implantação da rede de identidade nacional | | X | X | X | X | | | | | | | | | | | | |
| E5.4.1 | Chain Diploma - Realizar aproximação com o MEC, LedgerTech e RNP | | | X | X | X | | | | | | | | | | | | |
| E5.4.2 | Chain Diploma - Elaborar plano de trabalho | | | | | X | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| E5.5.1 | 2FA e Chain Moodle - Realizar entrevistas e análise essencial com os gestores da UFBA | | | X | X | X | | | | | | | | | | | | |
| E5.5.2 | 2FA e Chain Moodle - Elaborar plano de trabalho | | | | | X | | | | | | | | | | | | |
| A7 | Ciclos mensais de acompanhamento do desenvolvimento do MVP e validação | | | X | X | X | X | X | X | X | X | X | X | X | X | X | X | 01/11/2021 a 31/12/2022 |
| A7.1 | Adicionar resolução universal de redes | | | | | | | | | X | X | X | | | | | | |
| A7.2 | Chain Diploma - Desenvolver atividades definidas no plano de trabalho | | | | | | X | X | X | X | | | | | | | | |
| A7.3 | Chain Diploma - Realizar validação da solução e execução de piloto | | | | | | | | X | X | | | | | | | | |
| A7.4 | 2FA e Chain Moodle - Desenvolver atividades definidas no plano de trabalho | | | | | X | X | | | | | | | | | | | |
| A7.5 | 2FA e Chain Moodle - Realizar validação da solução e execução de piloto | | | | | X | X | X | | | | | | | | | | |
| A7.6 | Adicionar suporte a HUB de atributos | | | | | | | | | | | | X | X | X | | | |
| A7.7 | Adicionar suporte a outros protocolos de autenticação ao IDP, como o Outh2 e CAS | | | | | | | | | | | | | | X | X | X | |
| A7.8 | Melhorar a arquitetura atual | | | | | | | | | | | | X | X | X | X | X | |
| A7.9 | Construir clientes para a plataforma em diversas linguagens | | | X | X | X | X | X | | | | | | | | | | |
| A7.10 | Reformular a *landing page*, site principal e formulário de coleta de dados | | X | X | X | X | X | | | | | | | | | | | |
| A7.11 | Implementar método de onboard | | | X | X | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A7.12** | **Construção do wallet próprio do projeto** | | | | | **X** | **X** | **X** | **X** | **X** | **X** | **X** | | | | | | |
| **A7.13** | **Criar mecanismo de tarifação e bilhetagem** | | | | | **X** | **X** | **X** | **X** | | | | | | | | | |
| **A7.14** | **Realizar integração com a plataforma NasNuvens** | | | | **X** | **X** | **X** | **X** | **X** | | | | | | | | | |

## 9. Recursos financeiros

### 9.2. Infraestrutura

### 9.2.1. Recursos de Nuvem

| Categoria | Descrição da Configuração | Mês Inicial | Mês Final | Unid. | Qtd. | Custo Médio Unitário (R$) | Subtotal em R$ estimado |
|---|---|---|---|---|---|---|---|
| 2. ARMAZENAMENTO DE DADOS | SERVIÇO DE ARMAZENAMENTO DE OBJETOS. com os recursos de inclusão, leitura, exclusão e consultas, acessíveis por meio de interface web e API RESTful | 15/10/2021 | 31/12/2022 | 1 | 14 | 13,15 | 184,10 |
| 2. ARMAZENAMENTO DE DADOS | SERVIÇO DE BACKUP E RESTORE. Deve garantir serviço gerenciado de armazenamento persistente de dados de forma escalável e com disponibilidade de, no mínimo, 99,95% | 15/10/2021 | 31/12/2022 | 1 | 14 | 3,75 | 52,50 |
| 3. COMUNICAÇÃO DE DADOS | IP PÚBLICO IPV4 | 15/10/2021 | 31/12/2022 | 2 | 14 | 30,46 | 852,88 |
| 3. COMUNICAÇÃO DE DADOS | TRÁFEGO DE SAÍDA DE REDE | 15/10/2021 | 31/12/2021 | 1 | 14 | 10,12 | 141,68 |
| 1. SERVIDORES VIRTUAIS | SERVIDOR VIRTUAL TIPO 1.2 vCPUs (2 vCPUs e, no mínimo, 7 GB de RAM, HD 50GB, 150 IOPs) | 15/10/2021 | 31/12/2022 | 2 | 14 | 616,00 | 17248,00 |
| 1. SERVIDORES VIRTUAIS | SERVIDOR VIRTUAL TIPO 2.2 vCPUs (2 vCPUs, 3,75 GB de RAM, HD 50GB, 150 IOPs) | 15/10/2021 | 31/12/2022 | 1 | 14 | 369,60 | 5178,60 |
| | | | | | | **Total** | 23.657,76 |

## 10. Referências

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al. (2018). Hyperledger Fabric:a

distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, page 30. ACM.

Aries, H. (2021a). In Hyperledger Aries. Hyperledger Aries. https://github.com/hyperledger/aries-rfcs/tree/master/features/0036-issue-credential.

Aries, H. (2021b). In Hyperledger Aries. Hyperledger Aries.https://github.com/hyperledger/aries-rfcs/blob/master/features/0037-present-proof/README.md.

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., and Danezis, G. (2017). SoK: Consensus in the age of blockchains. Technical report, University College London, United Kingdom. https://arxiv.org/pdf/1711.03936.pdf.

Bhattacharya, M. P., Zavarsky, P., and Butakov, S. (2020). Enhancing the security and privacy of self-sovereign identities on hyperledger indy blockchain. In 2020 Int. Symp. on Networks, Computers and Communications (ISNCC), pages 1–7.

Buterin, V. et al. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37).

García, A. L., Fernandez-del Castillo, E., and Puel, M. (2013). Identity federation with voms in cloud infrastructures. In 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, volume 1, pages 42–48.

Gemmill, J., Robinson, J., Scavo, T., and Bangalore, P. (2009). Cross-domain authorization for federated virtual organizations using the myvocs collaboration environment. Concurrency and Computation: Practice and Experience, 21:509–532.

ITU (2009). In NGN Identity Management Framework - Recommendation Y.2720. [S.l.]. ITU. http://www.itu.int/rec/T-REC-Y.2720-200901-I/en.

Kubach, M., Schunck, C., Sellung, R., and Rossnagel, H. (2020). Self-sovereign and decentralized identity as the future of identity management? In Open Identity Summit.

Liu, Y., He, D., Obaidat, M., Kumar, N., Khan, M. K., and Choo, K.-K. R. (2020). Blockchain-based identity management systems: A review. J. Netw. Comput. Appl., 166:102731.

López, M. A. (2020). SELF-SOVEREIGN IDENTITY: The Future of Identity: Self Sovereignty, Digital Wallets, and Blockchain. Inter-American Development Bank.

Naik, N. and Jenkins, P. (2020). uport open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain. In 2020 IEEE Int. Symp. on Systems Engineering (ISSE), pages 1–7.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies. Princeton University Press.

Sovrin (2018). In A Protocol and Token for SelfSovereign Identity and Decentralized Trust. The Sovrin Foundation.

Tobin, A. and Reed, D. (2017). In The Inevitable Rise of Self-Sovereign Identity, volume 29. The Sovrin Foundation. Vullings, E., Dalziel, J., and Buchhorn, M. (2007). Secure federated authentication and authorisation to grid portal applications using saml and xacml. J. Res. Pract. Inf. Technol., 39:101–114.

W3C (2019a). In Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations.

W3C. https://w3c-ccg.github.io/did-spec/.W3C (2019b). In Verifiable Credentials Data Model 1.0: Expressing verifiable information on the Web. W3C. https://www.w3.org/TR/vc-data-model/.