Plataforma para Gestão de Identidades Descentralizadas Baseada em Blockchain

Silvio Queiroz[1], Fabíola Greve[1], Leobino N. Sampaio[1], Eduardo Marques[2]

[1]Programa de Pós-Graduação em Ciência da Computação (PGCOMP)
Departamento de Ciência da Computação – Universidade Federal da Bahia (UFBA)
Salvador – BA – Brasil

[2]Departamento de Tecnologia – Universidade Estadual de Feira de Santana (UEFS)
Feira de Santana - BA - Brasil

{silvio.queiroz, fabiola, leobino}@ufba.br, esantos@ecomp.uefs.br

Abstract. *Identity is fundamental for recognizing entities (i.e., individuals, things, and organizations) and their diverse relationships in the context they are located. The Identity Management (GId) establishes procedures for authentication, authorization, accountability, and auditing to preserve the security of access to organizations' resources. Once centralized or federated, GId systems can evolve into a decentralized and self-sovereign model (IDD), through which the user himself becomes the administrator of information about his identity and indeed becomes unique and shareable in the entire ecosystem. This paper presents the ChainID platform for managing decentralized identities through the blockchain. It contemplates the decentralized management of identities, their attributes, and credentials, being sufficiently generic to abstract the complexity of the communication standards and protocols involved in the solution, thus providing the IDD infrastructure in different usage flows safely and transparently. As a proof of concept, an authentication component has been developed, benefiting federated networks, like as Cafe by RNP.*

Resumo. *A identidade é fundamental para o reconhecimento das entidades (indivíduos, coisas e organizações) e das suas diversas relações no contexto em que estão inseridas. A gestão de identidades (GId) estabelece procedimentos de autenticação, autorização, responsabilização e auditoria, de forma a preservar a segurança do acesso aos recursos das organizações. Até então centralizados ou federados, os sistemas de GId podem evoluir para um modelo descentralizado e autossoberano (IDD), no qual o próprio usuário passa a ser o administrador das informações sobre sua identidade, e esta, inclusive, passa a ser única e compartilhável em todo o ecossistema. Esse trabalho apresenta a ChainID, uma plataforma para gestão de identidades descentralizadas através da blockchain, que contempla a GId, seus atributos e credenciais, e é suficientemente genérica para abstrair a complexidade dos padrões e protocolos de comunicação envolvidos, proporcionando assim o uso da infraestrutura de IDD em diversos fluxos de oferta de serviços, de forma segura e transparente. Como prova de conceito da plataforma, foi desenvolvido o componente de autenticação da ChainID, que beneficia redes federadas, como a CAFe da RNP.*

1. Introdução

A gestão de identidades (GId) é um conjunto de políticas, processos e tecnologias usados para garantir que apenas entidades (pessoas, instituições, ou coisas) autorizadas tenham acesso a recursos numa organização. A identidade em si é fundamental para o reconhecimento da entidade e das suas diversas relações no contexto em que está inserida, sendo formada por identificadores, credencias e atributos [ITU 2009].

A maioria dos modelos de GId é *centralizado*, no qual uma única organização controla todo o sistema e oferece as identidades e os serviços agregados. No entanto, as próprias identidades geradas podem ser federadas. Ambientes federados destacam-se como um modelo de GId no qual as instituições parceiras são associadas como federações utilizando um conjunto comum de atributos, práticas e políticas para troca de informações e serviços [Liu et al. 2020]. Em tais ambientes, os usuários podem usar informações de identidades estabelecidas em um domínio para autenticar e autorizar o acesso a outro domínio federado, separando-se desta maneira o provimento de identidade da oferta de serviços. Desta forma, as federações criam provedores de identidade (IdP) a partir das identidades de cada domínio, aproveitando, assim, das autenticações locais já implementadas. A rede acadêmica federada da RNP, a CAFe, é um exemplo bem sucedido.

O recente modelo de GId com *identidade digital descentralizada (IDD) e autossoberana* resgata o controle da identidade para o próprio usuário, de tal forma que ele passa a ser o administrador da sua identidade [Kubach et al. 2020]. 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.

A implementação de IDD só é possível com o estabelecimento de uma infraestrutura descentralizada, em que as relações de confiança entre as partes acontece de forma ubíqua em todo o ecossistema. Tais requisitos são possíveis através da tecnologia *blockchain*, uma rede de confiança digital que oferece um arcabouço seguro para realização de transações diretas entre pares que não necessariamente têm confiança entre si [Bano et al. 2017]. Ela tem potencial para promover a interação segura entre diversos atores da GId estabelecendo serviços de compartilhamento, verificação de credenciais e autorização aos diversos ativos na rede, de forma a preservar a integridade e privacidade dos dados, para além de promover transparência, auditabilidade e disponibilidade [Narayanan et al. 2016].

Atualmente, alguns poucos sistemas começam a despontar no sentido de propor uma implementação desse novo paradigma de identidade descentralizada [Liu et al. 2020]. Os principais exemplos são o da rede SOVRIN [Tobin and Reed 2017] para blockchains permissionadas, e utiliza o arcabouço Hyperledger Indy[1], 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. Nessa linha, algumas iniciativas tem surgido,

[1] hyperledger.org

como a SeLF[2] e a Evernym[3], além de outras envolvendo alianças, a exemplo da Lacchain [López 2020].

Este artigo apresenta a plataforma ChainID[4] para gestão de identidades descentralizadas, com base na tecnologia blockchain. Ela permite serviços de autenticação e autorização com suporte a multi-domínios, e utiliza protocolos de comunicação e frameworks para a construção de uma infraestrutura arquitetural que oferece interoperabilidade com diversos fornecedores e soluções de gestão de identidades e segurança no compartilhamento de informações entre pares.

Com o intuito de validar a plataforma ChainID, um serviço de autenticação foi desenvolvido, fazendo uso dos serviços de emissão e revogação de credenciais e solicitação de prova. Em complemento, foi desenvolvido um provedor de identidades (IDP) para uma rede federada, a exemplo da CAFe da RNP.

Desta forma, as principais contribuições deste trabalho são: (i) a proposta da plataforma ChainID que oferece um *framework* genérico e interoperável para tratar a complexidade de aplicações descentralizadas com identidade autossoberana (ii) um componente de autenticação para gestão de identidades descentralizadas, (iii) um repositório confiável de identidades para a construção de organizações virtuais de forma facilitada e interoperável com outras soluções.

O restante deste artigo está assim organizado: a Seção 2 apresenta principais conceitos. A Seção 3 aborda trabalhos relacionados. A Seção 4 descreve a arquitetura, seus principais componentes e interações. A Seção 5 apresenta a implementação da plataforma, com serviço de autenticação. Por fim, a Seção 6 apresenta a conclusão.

2. Fundamentos

A identidade de uma entidade (pessoa, coisa, ou instituição) refere-se a tudo que possa caracterizá-la no contexto que está inserida. Uma pessoa é identificada de diversas maneiras (e.g., RG, email, logins/senhas), possui diferentes *atributos* (e.g., físicos, biométricos, genêro), e *credencias* que o habilitam por ex. a exercer alguma profissão.

2.1. Identidade Digital Descentralizada e Autossoberana

A IDD é construída a partir de dois novos padrões em desenvolvimento no W3C, são eles: (i) identificadores descentralizados ou *Decentralized Identifiers* (DIDs) [W3C 2019a] e (ii) credenciais verificáveis ou *Verifiable Credentials* (VCs) [W3C 2019b]. A DID propõe uma maneira de associar a qualquer entidade (pessoa, organização, coisa) uma identidade única e própria, que permita a essa entidade uma interação no mundo digital. Já as VCs são as credenciais digitais, pertencentes à entidade, e carregam seus atributos e informações necessárias ao seu reconhecimento, como nome, gênero, data de nascimento, diplomas profissionais, etc. Tais credenciais são outorgadas por terceiros ou pelo próprio usuário da identidade.

Em contraste com os identificadores federados típicos, os DIDs foram projetados de forma que possam ser separados dos registros centralizados, provedores de identidade

[2]self-ssi.com

[3]evernym.com

[4]ChainID é um nome fictício devido à anonimização.

e autoridades de certificação. As especificações para a construção de um DID são apresentadas em [W3C 2019a], conforme a Tabela 1.

Tabela 1. Requisitos para o DID segundo o W3C

REQUISITO	DESCRIÇÃO
Descentralização	Os DIDs não devem necessitar de autoridades centralizadas.
Controle	As entidades representadas pelo identificador devem possuir poder de controlar diretamente seus identificadores digitais sem a necessidade de depender de autoridades externas.
Privacidade	Permitir que as entidades controlem a privacidade de suas informações, incluindo a divulgação mínima, seletiva e progressiva de atributos ou outros dados.
Segurança	Habilite segurança suficiente para que as partes solicitantes dependam dos documentos DID para seu nível de garantia exigido.
Baseado em Provas	Permita que os controladores DID para fornecer prova criptográfica ao interagir com outras entidades.
Detectabilidade	Permita que entidades descubram DIDs para outras entidades, para aprender mais sobre ou interagir com essas entidades.
Interoperabilidade	Use padrões interoperáveis para que a infraestrutura DID possa fazer uso de ferramentas e bibliotecas de software existentes projetadas para interoperabilidade.
Portabilidade	Seja independente do sistema e da rede e permita que as entidades usem seus identificadores digitais com qualquer sistema que suporte DIDs e métodos DID.
Simplicidade	Preferência a um conjunto reduzido de recursos simples para tornar a tecnologia mais fácil de entender, implementar e implantar.
Extensibilidade	É importante, sempre que possível, habilitar a extensibilidade, desde que não atrapalhe muito a interoperabilidade, portabilidade ou simplicidade.

2.2. Tecnologia Blockchain

A Blockchain ou Tecnologia de Registro Distribuído, do inglês, *Distributed Ledger Technology* (DLT) oferece uma rede de confiança digital, com potencial para o desenvolvimento de aplicações distribuídas descentralizadas disruptivas [Bano et al. 2017][Narayanan et al. 2016]. Ela alicerça suas bases em elementos da segurança computacional – em especial as funções *hash* e criptografia de chave assimétrica – e da computação distribuída tolerante a falhas – em especial o consenso distribuído – oferecendo um arcabouço seguro, escalável e confiável para a realização de transações entre pares que não se conhecem, sem a necessidade de entidades centralizadoras para validação. Nas blockchains privadas ou permissionadas, a exemplo do Hyperledger Fabric [Androulaki et al. 2018], o conjunto de nós validadores da rede são conhecidos e autenticados através de algum mecanismo de infraestrutura de chave pública (PKI), já nas blockchains públicas, a exemplo da Ethereum [Buterin et al. 2014], os nós são desconhecidos e não são autenticados na rede.

O registro das transações é validado através do protocolo de consenso e mantido num livro-razão distribuído (*distributed ledger*), que é replicado, mas único, oferecendo uma base comum e transparente, passível de verificação e auditoria. Nesse bojo, é possível representar as identidades (IDs) dos participantes de maneira universal, através de criptografia assimétrica, utilizando uma par de chaves públicas/privadas [Narayanan et al. 2016]. A adoção da blockchain viabiliza assim a criação das identidades digitais descentralizadas atendendo aos requisitos apresentados pela W3C na Tabela 1 e justificados através das suas propriedades de confiança.

Prover uma plataforma para o gerenciamento de identidades descentralizadas, segura, capaz de oferecer serviços de autenticação de forma genérica e abstraindo a complexidade técnica de padrões e protocolos de comunicação é um desafio. A plataforma precisar garantir um repositório de identidades descentralizadas confiável, permitir a manipulação de credenciais (emissão e revogação), prover autenticação com uso das informações obtidas dessas credenciais e manter-se aderente aos padrões dos identificadores descentralizados [W3C 2019a] e credenciais verificáveis [W3C 2019b]. O uso de credenciais verificáveis e a utilização de provas criptográficas como método de interação e identificação entre entidades (por ex., Universidade e Aluno) requer a escolha de um arcabouço descentralizado, sem a necessidade de autoridades centralizadoras. Neste ponto, a blockchain é uma escolha válida, interessante e natural [Sovrin 2018].

Desta forma, a adoção da blockchain proporciona benefícios, tais como: (i) o uso de endereços na blockchain como IDDs, (ii) uso de contratos inteligentes [Buterin et al. 2014] para registros de IDD, (iii) carteiras digitais como repositórios privados de dados permitindo que indivíduos armazenem e gerenciem suas chaves [Narayanan et al. 2016].

2.3. Arcabouços Blockchain para IDD

A ChainID foi desenvolvida a partir dos arcabouços Hyperledger Indy (HLI), em conjunto com o Hyperledger Aries (HLA) e Hyperledger Ursa (HLU). Todos eles são oferecidos pelo Hyperledger Greenhouse[5], um consórcio de código aberto para o desenvolvimento de tecnologias em blockchain, hospedado pela Linux Foundation. A sua escolha para o desenvolvimento do ChainID levou em consideração a finalidade, a comunidade, a maturidade e a adesão a padrões interoperáveis desses arcabouços. O Hyperledger Indy (HLI)[6] [Bhattacharya et al. 2020] fornece ferramentas, bibliotecas e componentes reutilizáveis para criar e usar identidades descentralizadas que sejam interoperáveis entre domínios administrativos, aplicativos e redes organizacionais distintas. A iniciativa da Indy ainda carece de implementações que promovam a interoperabilidade entre diferentes sistemas descentralizados. Desta forma, foi necessário adicionar mais um componente ao conjunto de conceitos e padrões utilizados na plataforma incluindo, assim, o Hyperledger Aries (HLA)[7] como mais um componente estrutural. O HLA é uma infraestrutura para interações entre pares confiáveis e troca de mensagens servindo como um cliente da blockchain, provendo interoperabilidade através de um protocolo de troca de mensagens robusto com uso do suporte criptográfico fornecido pelo Hyperledger Ursa[8].

[5]hyperledger.org
[6]hyperledger.org/use/hyperledger-indy
[7]hyperledger.org/use/aries
[8]hyperledger.org/use/ursa

3. Trabalhos Relacionados

A gestão de identidades tradicional contempla um conjunto de sistemas e padrões já estabelecidos e amplamente adotados. A literatura já apresenta diversas soluções para prover a interoperabilidade entre padrões distintos de GId. Contudo, em sua maioria consistem em soluções que se baseiam no uso de *proxies*, responsáveis por intermediar a comunicação entre dois elementos da GId, sob as mesmas regras de federação e soluções implementadas através da tecnologia blockchain.

Entre os exemplos de GId baseadas em *proxy*, é possível citar o myVocs (*my Virtual Organization Collaboration System*), que utiliza autenticação federada através de ferramenta Shibboleth (SAML) [Gemmill et al. 2009][García et al. 2013]. A solução é implementada em conjunto com atributos auto-gerenciados de uma organização virtual (OV) e possui foco em ambientes de grid. O IAA (*Identity Access Management Suite*) também pode ser citado; trata-se de uma solução baseada nas especificações SAML e XACML para o acesso a um ambiente de pesquisas virtuais (VRE). O IAA combina atributos recebidos pelo IdP do usuário com os atributos específicos da VRE fornecendo autenticação e acesso a serviços que estão em diferentes federações [Vullings et al. 2007].

A plataforma ChainID aqui apresentada vai além de um *proxy*, pois contempla um repositório confiável de identidades e atributos para a construção de uma OV de forma facilitada e interoperável com várias soluções de gerenciamento de identidade existentes e serviços das federações. A confiança e segurança da blockchain, em conjunto com os mecanismos de autenticação e autorização, proporciona as relações de confiança entre federações e domínios administrativos necessárias para a criação e manutenção das OVs.

Ainda no escopo dos trabalhos relacionados, é preciso destacar aqui as implementações de gestão descentralizada de identidades através de redes blockchain. Entre as iniciativas, destaca-se a rede Sovrin, o sistema uPort, e adoção de arcabouços de base, a exemplo do Hyperledger Indy, para o desenvolvimento de outros componentes, sistemas e aplicações com IDD [Liu et al. 2020].

A Sovrin[9] [Tobin and Reed 2017] é uma rede de IDD de código aberto, baseada numa blockchain permissionada, e mantida pelos nós administradores localizados em instituições como empresas, universidades e governo. Atualmente, a rede possui em torno de 50 nós espalhados em vários pontos do globo. Os mesmos são responsáveis por executar o protocolo de consenso na geração dos blocos, pela governança da rede e sua manutenção. A Sovrin oferece como arcabouço de base o Hyperledger Indy (HLI).

O framework uPort [Naik and Jenkins 2020] é uma solução de IDD de código aberto baseada na Ethereum, uma blockchain aberta. O uPort foca na oferta de IDD para todos os participantes da rede, oferecendo recursos de IDD para o desenvolvimento de aplicações descentralizadas (DApps). Sua identidade é a conta do usuário na Ethereum e esta é permanente. A aliança Lacchain [López 2020] tem investido no desenvolvimento do uPort para a sua integração com o Hyperledger Besus[10], uma plataforma que agrega clientes Ethereum a redes blockchains públicas ou privadas/permissionadas.

[9] sovrin.org

[10] hyperledger.org/use/besu

4. Arquitetura da Plataforma ChainID

A plataforma ChainID fornece uma arquitetura baseada em serviços concebida com o objetivo de facilitar a criação de aplicações e serviços utilizando IDDs com agilidade, rapidez e transparência. Estas características estão associadas a abstração do complexo conjunto de infraestrutura, protocolos de comunicação, padrões e demais componentes necessários a soluções com IDD; através da implementação de um controlador de negócio baseado na arquitetura recomendada pelo HLA para aplicações de identidade autosoberana (do inglês, *Self-Sovereign Identity* – SSI) [ACA-Py 2021]. A arquitetura ChainID é composta com base no padrão HLA, que consiste em quatro chaves, a saber: (i) um controlador de negócios, (ii) API REST, (iii) Indy Node; e (iv) a DLT (ver Figura 1). As subseções seguintes descrevem tais elementos e suas interações na plataforma desenvolvida.

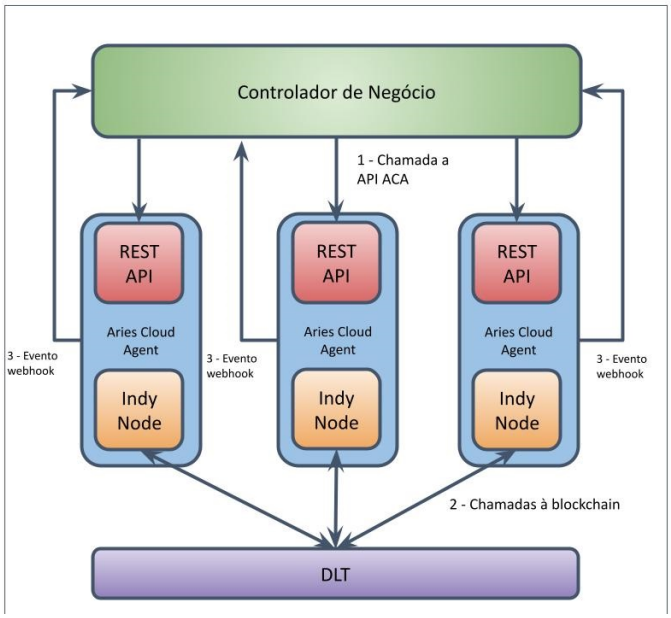

Figura 1. Arquitetura adaptada a partir arquitetura recomendada pela HLA [ACA-Py 2021].

A ChainID foi concebida a partir da arquitetura recomendada pela HLA [ACA-Py 2021], conforme Figura 1. Nela, estão definidas as aplicações, denominadas controladores de negócio, que consistem em clientes da API fornecida pelos agentes de borda e processam eventos *webhook* para definir comportamentos personalizados.

Nesta abordagem, o evento *webhook* é uma solução empregada para o tratamento de chamadas assíncronas à API. Em (1), o controlador de negócio realiza chamadas ao componente Aries Cloud Agent (ACA); em seguida (passo 2), o ACA realiza chamadas à DLT para armazenar ou recuperar informações necessárias as operações e, e por fim, em (3) o agente retorna eventos *webhook* para o controlador com informações sobre a operação realizada.

4.1. Controlador de Negócios

O controlador de negócios foi implementado conforme descrito na Figura 2 e permite que a plataforma gerencie identidades descentralizadas abstraindo a complexidade inerente de

um ecossistema descentralizado, sendo resultado do maior esforço empregado durante o desenvolvimento.

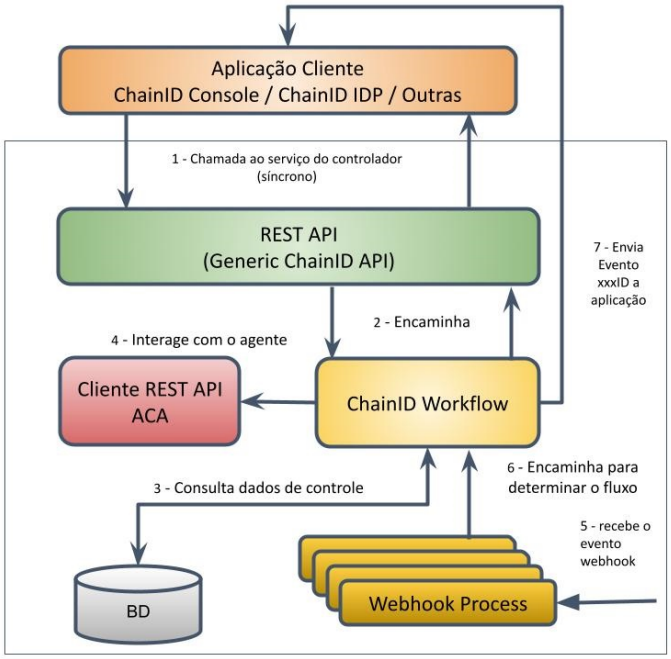

Figura 2. Arquitetura da plataforma ChainID.

O funcionamento do controlador acontece através de uma sequencia de ações, conforme a seguir: No **passo 1**, o serviço é iniciado a partir de uma chamada da aplicação cliente, que pode acontecer de diferentes formas, tais como uma console (e.g., ChainID console) e até mesmo uma IDP de uma rede federado (e.g., ChainID IDP). Assim, na interação, a aplicação realiza chamada ao *Generic ChainID API*, através da qual é informada a chave de acesso da organização no cabeçalho da requisição na propriedade "*X-API-Key*"[11]. Esta é utilizada para (i) identificar a organização que solicita o processamento da requisição e (ii) efetuar a autorização da operação, validando os parâmetros informados. No **passo 2**, os parâmetros são validados e encaminhados ao ChainID workflow, que por sua vez, obtém as informações sobre o fluxo da solicitação, consulta na base de metadados o endereço da instância do *ACA* da organização (**passo 3**) e interage com o agente no **passo 4**. De forma assíncrona, no **passo 5**, o *Webhook Process* processa os eventos e valida aqueles que estão de acordo com o padrão. Após a validação, os dados destes são encaminhados ao *ChainID Workflow* (**passo 6**) que, por sua vez, identifica a organização, resgata o registro na base de metadados e, caso a solicitação esteja concluída, **no passo 7** o *ChainID Workflow* emite o evento para a aplicação cliente informando a situação da mesma.

As subseções seguintes detalham como a plataforma ChainID trata a complexidade de aplicações SSI fornecendo um *framework* genérico e interoperável.

4.2. Serviços da Arquitetura

Os principais serviços da ChainID consistem na emissão e revogação de credenciais e solicitação de prova. Estes podem beneficiar o desenvolvimento de um amplo conjunto

[11]Padrão de autenticação utilizada ...

de aplicações, tais como o IDP Blockchain que será descrito na seção 5.2.

Emitir credenciais é um processo pelo qual uma credencial verificável é atribuída ao titular. Segundo o protocolo do HLA, existem quatro métodos para emitir credenciais: (i) o titular propõe a credencial a um potencial emissor, (ii) o emissor oferece a credencial a um potencial titular, (iii) o potencial titular requisita a credencial ao emissor e (iv) o emissor emite a credencial ao titular com os dados do atributo [Aries 2021a]. A plataforma ChainID oferece o serviço de emissão de credencial usando o método (iv). Desta forma, o emissor 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.

Solicitar prova é o processo pelo qual uma credencial verificável pode ser apresentada e validada. Neste processo existem dois atores: o provador e o verificador. O provador é o ator que realizada a prova apresentando sua credencial. O verificador é o ator que valida a credencial apresentada. O protocolo atual consiste em três métodos: (i) o provedor propõe a prova ao verificador, (ii) o verificador requisita a prova ao provedor e (iii) o provedor apresenta a prova ao verificador. A plataforma ChainID oferece o fluxo (iii) no qual o provedor apresenta a prova ao verificador [Aries 2021b].

Revogar credencias 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.

4.3. Orquestração de Serviços

Orquestração é a configuração, o gerenciamento e a coordenação automatizada de serviços, aplicações e sistemas de computador. A orquestração 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 da HLA. Desta forma, as operações com IDD foram mapeadas em fluxos contendo chamadas orquestradas a serviços de forma a automatizar o processo no componente *ChainID Workflow*.

Desta forma, a operação emitir credenciais é mapeada como um fluxo que possui o pré-requisito outro fluxo, estabelecer relação de confiança. Nesta situação o *ChainID Workflow* busca pelo registro da relação de confiança estabelecida antes de emitir a credencial. Caso não encontre, o fluxo para estabelecer a relação de confiança é invocado criando o convite de conexão e encaminhado ao e-mail do titular. O convite é criado realizando a chamada ao serviço */connections/create-invitation* para o agente de borda do emissor. O agente retorna o *invitation_url* que é encaminhado ao titular e aguarda a resposta do titular. Este em posse do *invitation_url* aceita a solicitação de conexão emitindo ao agente do emissor o evento *connection* informando o aceite da emissão através do *webhook*. O *webhook process* processa e encaminha ao *ChainID Workflow* os metadados da conexão.

Com a conexão estabelecida, o *ChainID Workflo*w realiza a próxima etapa do fluxo, emitir a credencial: Envia a credencial para o connectionId gerado na criação da conexão através da chamada ao serviço */issue-credential/send* do agente do emissor. O

titular receberá em seu agente a oferta de credencial emitida e ao aceitá-la o *Webhook process* receberá o evento de confirmação finalizando o processo de emissão de credencial.

4.4. Tratamento de Eventos

Como apresentado na seção anterior, algumas fluxos da plataforma ChainID necessitam de interação assíncrona e aguardam serem sensibilizadas para atualizar seu estado. As notificações destas interações são realizadas por meio de eventos *webhook* encaminhados para a plataforma através de chamadas ao serviço POST */topic/{evento}* pelo agente do emissor. Estes eventos são processados pelo *Webhook process*. O *Webhook process* valida o evento e o *payload* possui um conjunto de estratégias para o processamento de eventos. Cada estratégia implementa a interface *EventStrategy* que possui três métodos: *eventKey*, *convertTO* e *process*. O método *eventKey* retorna o evento tratado pela estratégia, *convertTo* converte o *payload* da mensagem para a classe referente ao evento e process processa o dados recebidos pelo evento. Novos eventos podem ser processados com a implementação desta interface e permitem a extensão do comportamento atual.

O *Webhook process* trata o retorno das chamadas e delega ao *Workflow* a decisão da próxima ação necessária ao fluxo da operação que fará ou não uma nova operação, como por exemplo: aceitar a requisição de conexão realizando uma nova chamada ao agente cloud ou simplesmente ignorar o evento recebido.

5. Implementação

A fim de validar a plataforma ChainID foi feita a implementação de um serviço de autenticação que faz uso dos serviços de emissão e revogação de credenciais e solicitação de prova. A implementação envolveu o desenvolvimento de uma console e um IDP de autenticação de rede federada. As próximas subseções apresentam os detalhes envolvidos em tais desenvolvimentos.

5.1. Console Administrativo

A aplicação cliente *ChainID console* funciona como um configurador e uma interface com fluxos simplificados para a criação de credenciais, requisições de prova e revogações de credenciais. A aplicação foi construída utilizando a tecnologia *Vue.js* e funciona como um cliente das funcionalidades do *ChainID API*. Para um serviço de autenticação, a console é um facilitador de administrador das credenciais uma vez que este necessita criar e manter os atributos dos usuários de serviços.

A Figura 3 apresenta um conjunto de capturas de telas da console desenvolvida. Como é possível perceber, em (a) é apresentada a funcionalidade de cadastro de credenciais, que permite criar credenciais com suporte a revogação. Em (b) é apresentada a tela de cadastro de atributo de uma credencial. A criação de atributos permite estabelecer o tipo do dado a ser informado no atributo, possibilitando que o serviço de emissão de credencial do *Generic ChainID API* realize validações sobre os valores informados. Em (c) são apresentadas as operações básicas sobre a credencial, como editar, excluir e publicar credenciais além de editar atributos destas credenciais.

As credenciais no *ChainID* são relacionadas à organização do usuário logado, e apresentam três estados sequenciais: cadastrado, publicado e revogado. Uma credencial cadastrada é uma credencial em edição; apenas credencias no estado cadastrado podem

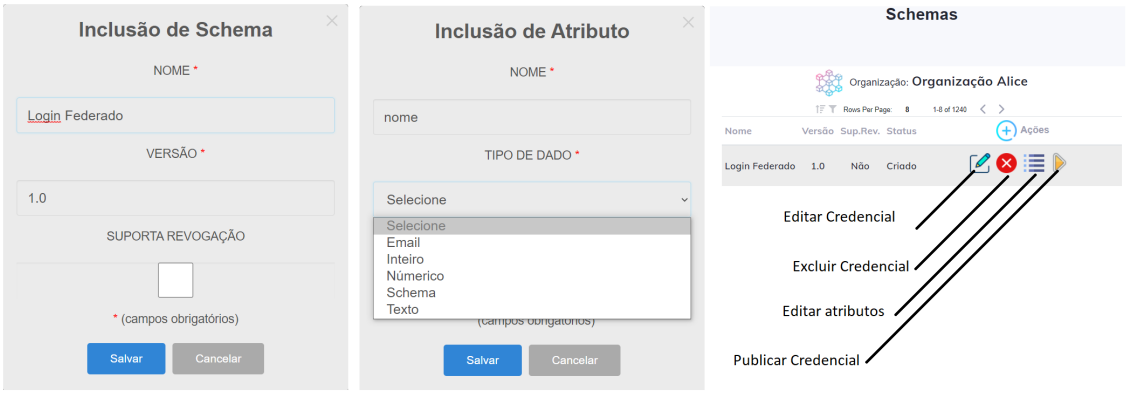

Figura a - Cadastro de Credencial

Figura b - Cadastro de Atributo

Figura c - Operações sobre as Credenciais

Figura 3. Telas da aplicação console

ser editadas. O estado publicado é definido a credenciais publicadas na blockchain. A exclusão da credencial revoga a credencial, tornando-a inativa e, consequentemente, revoga todas as emissões desta credencial.

5.2. IDP para Rede Federada

Além da console, o serviço de autenticação utilizado na validação da plataforma envolveu o desenvolvimento de um IDP (denominado aqui por IDP Blockchain) para uma rede federada, tal como a rede CAFe[12] (Comunidade Acadêmica Federada) da Rede Nacional de Ensino e Pesquisa[13] (RNP).

O serviço de autenticação *SingleSingle Sign-On* (SSO) provido pelo IDP Blockchain foi implementado através da customização do *middleware* CAS da Apereo[14]. Este *middleware* fornece serviços de autenticação com suporte a vários protocolos abertos, várias fontes de autenticação, integração nativa a diversos softwares de mercado, clientes em diversas linguagens de programação e uma arquitetura extensível através de *plugin* e *overlays*.

O *plugin* construído é nomeado *ChainIDAuthenticationHandler* e implementa a interface *org.apereo.cas.authentication.AuthenticationHandler* da arquitetura do CAS. Além do *plugin* foram necessárias as implementações do serviço POST */topic/{event}* e uma nova página de login para apresentação da solicitação de requisição de prova com um *QRCode*.

A autenticação federada utilizando a nova fonte de autenticação (denominada *ChainIDAuthenticationHandler*) é apresentada na Figura 4.

Conforme a Figura 4, **No passo 1**, o usuário solicita acesso a um recurso do provedor de serviço. O provedor de serviço necessita da identificação do usuário e solicita **no passo 2** ao componente *WAYF*, do inglês *Where Are You From?*, que determine o IDP que possui a identidade a ser autenticada. Após o usuário informar sua instituição, o WAYF **no passo 3** direciona o usuário ao endereço do IDP para autenticação. **No passo 4**, o IDP identifica que não existe um sessão SSO para o browser e solicita ao *Generic ChainID API*

[12]https://www.rnp.br/servicos/alunos-e-professores/identidade-e-seguranca/cafe
[13]https://www.rnp.br/
[14]apereo.github.io/cas/

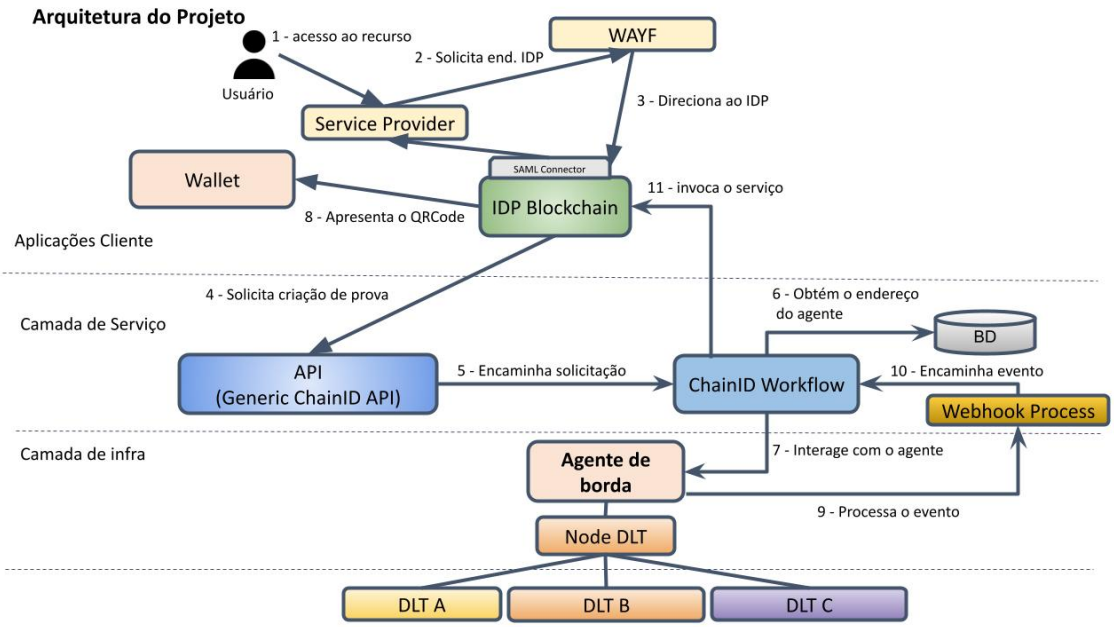

Figura 4. Arquitetura da plataforma ChainID autenticando numa rede federada

a criação de uma solicitação de prova informando o schemaID da credencial verificável e os atributos a serem apresentados durante a prova. **No passo 5**, a *Generica ChainID API* valida os parâmetros e encaminha ao *ChainID Workflow*, que por sua vez, obtém as informações sobre o fluxo da solicitação, consulta na base de metadados, obtém o endereço da instância do ACA da organização (**passo 6**) e interage com o agente no passo **passo 7**. O resultado da interação com agente é encaminhado, **no passo 8**, para o IDP que apresenta a solicitação de prova com um *QRCode*. De forma assíncrona, **no passo 9**, o *Webhook process* processa o evento *present_proof* e encaminha ao *ChainID Workflow* (**passo 10**) que, por sua vez, identifica a organização, resgata o registro na base de metadados e invoca o serviço POST */topic/{event}* do IDP passando o evento prova realizada juntamente com os atributos informados. **No passo 11**, o IDP criar a sessão SSO e encaminha todos os atributos recebidos ao provedor de serviço via mensagem *SAML*, encerrando o ciclo de autenticação.

A solução apresentada pela Figura 4 possui alguns pré-requisitos para o pleno funcionamento: (i) apenas credenciais revogáveis podem ser utilizadas para em uma requisição de prova, (ii) as credenciais indicadas na requisição de prova devem obrigatoriamente possuir os atributos obrigatório ao padrão EDUPerson, (iii) o usuário a ser identificado deve possui a credencial para o schemaID requisitado pela prova e (iv) o usuário deve aceitar a prova para que os atributos sejam informados ao IDP.

6. Conclusão e Trabalhos Futuros

Este artigo apresentou a plataforma ChainID, que oferece um arcabouço genérico e interoperável para tratar a complexidade de aplicações descentralizadas com identidade autossoberana. Através da ChainID, o trabalho apresenta alternativas ao modelo de GId providos atualmente por federações, através do qual uma única organização controla todo o processo de fornecimento de identidades e os serviços agregados. Por meio da identi-

dade digital descentralizada (IDD) e autossoberana, implementados através da tecnologia blockchain, a ChainID resgata o controle da identidade para o próprio usuário. Desta forma, o mesmo passa a ser o administrador da sua identidade, consolidando frutos dos modelos anteriores e avançando no estabelecimento de uma auto soberania do usuário no controle da sua identidade, de forma segura e universal. O projeto e a implementação do componente de autenticação da plataforma demonstraram os benefícios da gestão descentralizada das identidades, seus atributos e credenciais. A plataforma proposta mostrou-se ainda suficientemente genérica para abstrair a complexidade dos padrões e protocolos de comunicação envolvidos na solução. Como trabalhos futuros, pretende-se dar continuidade à implementação da ChainID, com o consequente desenvolvimento de uma aplicação descentralizada de IDD utilizando a plataforma.

Referências

ACA-Py (2021). In *Hyperledger Aries Cloud Agent - Python*. Hyperledger Aries. `https://github.com/hyperledger/aries-cloudagent-python/blob/main/README.md`.

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 International Symposium 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-Sovereignity, 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 International Symposium 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. `https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf`.

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/`.