Proposta para Grupo de Trabalho 2020

GT-ChainID – Plataforma Universal para Gestão de Identidades através da Blockchain

Fabíola Gonçalves Pereira Greve

03 de maio de 2020

1. Título

GT-ChainID – Plataforma Universal para Gestão de Identidades através da Blockchain

2. Coordenador Acadêmico

Fabíola Gonçalves Pereira Greve
Profa. Titular do Departamento de Ciência da Computação
Universidade Federal da Bahia (UFBA), fabiola@ufba.br; Cel.: (71) 99302-7775

CV Lattes: http://lattes.cnpq.br/0120615995402345

LinkedIn: https://www.linkedin.com/in/fabiolagreve/

3. Assistente de Inovação

Leobino Sampaio
Prof. Associado do Departamento de Ciência da Computação
Universidade Federal da Bahia (UFBA), leobino@gmail.com

CV Lattes: http://lattes.cnpq.br/1952937182023132

LinkedIn: https://www.linkedin.com/in/leobino-sampaio-878a0922/

4. Tema(s)

Gestão de Identidade:

- Novas técnicas e tecnologias de identificação, autenticação e autorização, com controle de acesso dinâmico e melhoria da usabilidade e segurança; ● Solução de agregação de atributos.

5. Resumo

Este projeto propõe o desenvolvimento de uma plataforma/framework com capacidade de interoperar com diversos fornecedores e soluções de gestão de identidades federadas ou não, provendo serviços de autenticação e autorização com suporte a multi-domínios, possibilitando o compartilhamento e auditoria de recursos, como dados de usuários e informações sobre a autorização dos diversos ativos da rede com o uso de uma identidade digital única por usuário. Para tanto, será utilizada a tecnologia Blockchain que oferece uma rede de confiança digital, com capacidade de implementação de processos seguros e universais de identificação das pessoas, numa escala nacional e global.

6. Abstract

This project offers the development of a platform/framework with the ability to interoperate with different vendors and identity management solutions, either federated ot not, providing authentication and permission services with support for multiple domains, allowing the sharing and auditing of resources, such as user data and information about the permission of various network assets using the user's unique digital identity. To this end, Blockchain technology will be used, which offers a digital trust network, with the capacity to implement safe and universal processes for the identification of people, on a national and global scale.

7. 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, com assistência do Prof. Leobino Sampaio. A equipe proponente desta proposta irá modelar, projetar, implementar e acompanhar o desenvolvimento da plataforma em todas suas etapas.

Profa. Fabíola é 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.

Prof. Leobino Sampaio é especialista em redes de computadores, com foco em medição e avaliação de desempenho, tendo participado de vários projetos de desenvolvimento tecnológico nessa área. Tem formação eclética, com graduação em Administração de Empresas e ensino superior em disciplinas dessa área.

(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) Universidade Estadual de Feira de Santana (UEFS) - a equipe do Prof. Antônio Augusto Teixeira Ribeiro Coutinho, membro do Gaudi, irá auxiliar na construção do ambiente de testes e nos testes da ferramenta.

(4) Universidade Estadual de Santa Cruz (UESC) - a equipe do Prof. Jaubert Abijaude, membro do Gaudi, irá auxiliar na construção do ambiente de testes e execução do mesmo.

8. Descrição do problema e da solução proposta com destaque para as inovações

8.1 Contextualização

Universidades, centros de pesquisa e empresas, públicas e privadas, vem participando de redes colaborativas com o objetivo de realizar pesquisas em escala global, nas quais compartilham grande quantidade de dados, recursos computacionais e infraestrutura extrapolando os domínios de uma única organização e sendo conectados através da internet. Estes ambientes são denominados *e-science* .

Como resultado das conexões entre diversas instituições geograficamente distribuídas como o objetivo de desenvolver pesquisas colaborativas são gerados grupos sem fronteiras comumente chamados de Organizações Virtuais (OV).

O estabelecimento das OVs possui como desafio a criação e o gerenciamento de um ambiente controlado entre diferentes domínios administrativos que possibilite a interação entre os pesquisadores autorizados [Capuano et al. 2010]. Desta forma, torna-se necessário determinar um conjunto de usuários e suas respectivas autorizações, estabelecendo permissões de acesso a recursos computacionais e dados [Foster et al. 2001]. Criar, manter e gerir estas identidades digitais são tarefas desafiadoras que requisitam garantia de eficiência, segurança, integridade e sincronia entre bases e infraestrutura de autorização.

Prover Gestão de Identidade, 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 OVs [ITU-T 2009].

Os ambientes federados destacam-se como um 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 precisem colaborar em um ambiente de *e-science* envolvendo mais de uma federação. Muitos sistemas de gestão de identidade federadas não possuem políticas ou mecanismos que possibilitem o estabelecimento dinâmico de relações de confiança entre domínios administrativos de diferentes federações [Cabarcos et al. 2009].

Conforme estudos realizados em [Ates et al. 2007], 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 processo de interoperabilidade seja realizada por uma terceira parte confiável que atue em ambas as federações e que implemente os padrões a serem interoperáveis.

8.2 Objetivo

Diante do problema supracitado, propomos o desenvolvimento de uma plataforma/framework com capacidade de interoperar com diversos fornecedores e soluções de gestão de identidades federadas ou não, provendo serviços de autenticação e autorização com suporte a multi-domínios, possibilitando o compartilhamento e auditoria de recursos, como dados de usuários e informações sobre a autorização dos diversos ativos da rede com *o uso de uma identidade digital única por usuário.* Tal inovação será propiciada através da Blockchain.

A Blockchain ou DLTs (*Distributed Ledger Technologies*) oferece uma rede de confiança digital, com potencial para o desenvolvimento de aplicações distribuídas descentralizadas disruptivas. 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. O registro das transações é 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) de maneira universal, através de criptografia assimétrica, utilizando uma par de chaves públicas/privadas [Greve et al. 2018].

As redes blockchain podem ser categorizadas em dois grupos: blockchain pública ou *permissionless* (sem permissão, de acesso aberto), e blockchain federada/privada ou *permissioned* (com permissão e acesso controlado). Na blockchain pública, o conjunto de nós da rede é desconhecido e sua composição (*membership*) é dinâmica, permitindo entradas e saídas aleatórias de nós. Como os nós não precisam de identificação, costumam ser anônimos. A blockchain pode atuar em escala planetária, sem controle dos seus participantes. Nesta categoria, encontra-se a rede do Bitcoin, do Ethereum e de diversas outras criptomoedas. A blockchain federada ou privada tem uma composição conhecida, formada por n processos, cujas entradas e saídas estão sujeitas a permissões. Os nós são identificados, autenticados e autorizados. A blockchain irá atender melhor a interesses corporativos ou privados, onde os participantes têm papéis

bem definidos e podem inclusive se organizarem grupos. Nesta categoria, encontram-se o Hyperledger Fabric, Hyperledger Indy e o Corda [Greve et al. 2018].

8.3 Descrição

A plataforma ChainID utilizará dados de cada domínio administrativo ou federado que compõem as OVs, compartilhados através dos serviços de integração, para criar identidades digitais únicas compartilhadas e oferecer mecanismos confiáveis de gerenciamento desta identidade, através da DLT e consenso da blockchain, ao mesmo tempo que permita a cada domínio administrativo ou federado especificar suas próprias regras de autorização a objetos, em conformidade ao negócio e as necessidades dos mesmos.

Conforme apresentado na Figura 1, a plataforma terá uma arquitetura modular, composta por cinco módulos integrados:

1. Gerenciamento de Identidade
2. Controle de Autenticação
3. Controle de Autorização
4. Módulo de Integração
5. Módulo de Serviços

Nesta abordagem, as instituições utilizarão a camada de integração para registrar os dados sobre seus usuários e recursos, fornecendo informações como nome, cpf, data de nascimento, perfil, permissões, entre outros, que serão insumos para a geração das identidades digitais únicas compartilhadas.

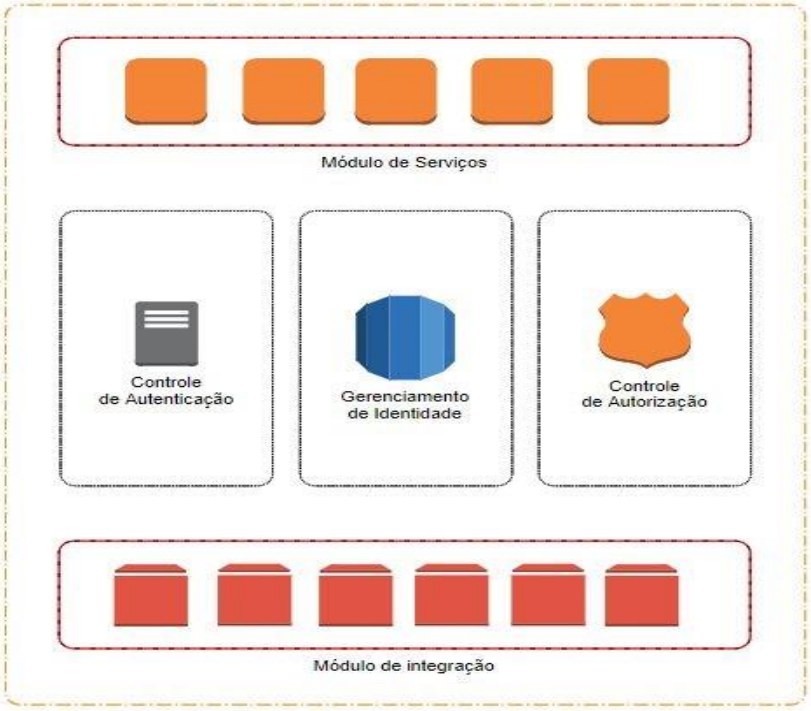

Figura 1: Arquitetura da Plataforma ChainID

(1) Módulo de Gerenciamento da Identidade compartilhada: A plataforma definirá sua própria noção de identidade, atributos, contextos e regras pelas quais essas identidades são geridas (criação, modificação e validação) e autenticadas (geração e verificação de assinaturas). A identidade digital compartilhada será suportada através da tecnologia blockchain, em sua implementação federada, como infraestrutura base para armazenamento e compartilhamento da identidade digital entre os participantes da rede, provendo confiança, segurança, compartilhamento e escalabilidade.

Através da integração com o serviço ICPEdu, como autoridade certificadora, dados de usuário podem ser verificados, certificados digitais podem ser gerados e serviços como pseudo-anonimato, criptografia e autorizações serão disponibilizados dentro da plataforma.

(2) Módulo Controle de autenticação: contempla os mecanismos de autenticação e fornecerá mecanismos de acesso baseados em Single Sign On (SSO) e integrações a diversas tecnologias e protocolos de mercado, como por exemplo CAS e OAuth. A autenticação utilizará a identidade criada na plataforma para prover a identificação do usuário.

(3) Módulo Controle de Autorização: utilizará os padrões RBAC+ABAC, em conjunto com o controle de autenticação, e definirá níveis de acesso aos usuários suportando multi-domínio e oferecendo controle de acesso a objetos com nível de granularidade por papel ou atributo. Novos atributos podem ser implementados.

(4) Módulo de Integração: será responsável pelo compartilhamento do estado global dos objetos da rede, auditoria, pseudo-anonimato e utiliza a capacidade da tecnologia blockchain em prover uma rede confiável, escalável, compartilhada e permanente de informações através do mecanismo de consenso.

(5) Módulo de Serviços: disponibilizará uma camada de integração com diversas aplicações através do protocolo RESTFULL e permite o gerenciamento de dados dos objetos, alteração do estado, autenticação e autorização além de serviços às comunidades de usuários participantes das OVs. Será através da camada de serviço que os domínios poderão atualizar os dados dos registros e interagir com a plataforma e suas funcionalidades.

8.4 Aspectos Inovacionais

O projeto traz a inovação da tecnologia Blockchain fornecendo uma cadeia distribuída de informação segura, escalável, passível de auditoria e controle de permissão de acesso, além de prover interoperabilidade entre diversos fornecedores e tecnologias de gerenciamento de identidade, resolvendo requisitos de confiança em diferentes cenários de colaboração, e proporcionando a integração com tecnologias que vão surgir.

A RNP se beneficiará com a inovação e segurança da blockchain para o compartilhamento de informações de usuários de maneira alinhada ao contexto atual de cada instituição, no momento que possibilitará a cooperação entre diversos domínios administrativos e federados, de maneira facilitada, criptografia de dados, controle de acesso, compartilhamento de estados globais e ainda aproveitando tecnologias já existente em cada domínio ou federação ao integrá-las à plataforma proposta, reduzindo o custo de implantação de um novo sistema e com aderência a novas tecnologias que estão por vir.

Diversas soluções para prover a interoperabilidade entre padrões distintos de gestão de identidade já foram pensadas e desenvolvidas. Em sua maioria são *proxy* , que tem o papel de realizar o intermédio entre dois elementos da GID, mas que estão sob as mesmas regras de federação, tais como:

- *my Virtual Organization Collaboration System* (myVocs), utiliza autenticação federada através de *Shibboleth* (SAML), combinada a atributos auto-gerenciados de uma OV possui foco em ambientes de *grid* [GARCIA et al.

  2013]*;*

- *Identity Access Management Suite* (IAA), baseada nas especificações SAML e XACML para o acesso a um ambiente de pesquisas virtuais (VRE) combina atributos recebidos pelo IDP do usuário com os atributos específicos da VRE fornecendo autenticação e acesso a serviços que estão em diferentes federações [Vullingse e Buchhorn 2014].

A solução aqui proposta vai além de um proxy. É um repositório confiável de identidades e atributos para a construção de uma VO de forma facilitada e interoperável com várias soluções de gerenciamento de identidade disponíveis no mercado e serviços das federações. A confiança e segurança da blockchain em conjunto com os mecanismos de autenticação e autorização proporcionarão as relações de confiança entre federações e domínios administrativos necessárias para a criação e manutenção das OVs.

Como está baseada em Blockchain, a evolução da plataforma ChainID, uma vez desenvolvida, será a incorporação dos elementos necessários para suporte à *identidade digital autossoberana* de forma plena, de tal maneira a considerar aspectos de privacidade de dados. Neste caso, o próprio usuário passa a deter o controle e gestão dos seus dados, sejam estes pessoais, ou interpessoais, nas suas diversas relações, com pessoas, empresas e até coisas (Objetos Inteligentes).

9. Ambiente de validação da solução proposta e documentação dos aprendizados

A fim de avaliar a plataforma proposta, serão realizados testes em três ambientes distintos: ambiente local, ambiente simulado utilizando o *GidLab da RNP* e ambiente real de integração envolvendo as instituições parceiras do projeto. Todos os ambientes serão compostos de várias federações e uma blockchain federada, tal como a Hyperledger Indy, que incorpora facilidades para identidades digitais*.* A plataforma de blockchain a ser utilizada será definida no Marco 1 do projeto.

No *primeiro momento*, serão realizados testes de validação da implementação conforme cada fase de desenvolvimento da plataforma. Nesta fase, utilizaremos o ambiente local, com uso de dois provedores de identidade e serviços do GidLab, simulando instituições distintas com as tecnologias SAML e OpenId.

No *segundo momento*, utilizaremos o ambiente simulado do GidLab para realizar as validações dos módulos.

No *terceiro momento*, utilizaremos o ambiente real de integração envolvendo as instituições parceiras.

Os testes consistem basicamente em:

- Validação dos serviços do Módulo de Gerenciamento de Identidade: Serão registrados dados de identidade contidos em apenas uma instituição e em ambas as instituições em momentos distintos. As identidades serão modificadas e as alterações devem ser refletidas na identidade única da plataforma.
- Validação dos serviços do Módulo de autenticação: Serão realizados testes de autenticação na plataforma nas duas instituições;
- Validação dos serviços do Módulo de Autorização: Serão realizados testes de autorização na plataforma envolvendo as duas instituições;
- Validação dos serviços do Módulo de Integração: Serão integrados serviços utilizando os protocolos SAML e OpenID de forma a atestar a interoperabilidade das duas tecnologias de gestão de identidade;
- Validação do Módulo de Serviços para a OV: Testes com o objetivo de realizar o ciclo de vida completo de uma OV. Criação, operação, evolução e dissolução.

Todas as implementações serão documentadas e entregues junto à ferramenta ao final do projeto, assim como serão criados manuais de uso da ferramenta.

10. Cronograma de marcos

Os seguintes marcos são propostos para o desenvolvimento da plataforma/framework:

- **Marco 1:** Estudo de tecnologias e padrões de federação e autorização bem como a escolha de quais serão inicialmente suportados pela plataforma; estudo e escolha da blockchain federada a ser adotada e documento do projeto com arquitetura e tecnologias envolvidas;
- **Marco 2:** Modelagem dos contratos inteligentes e estrutura da identidade digital compartilhada e desenvolvimento do módulo de Gerenciamento de Identidades;
- **Marco 3:** Integração do ICPEdu na blockchain;
- **Marco 4:** Desenvolvimento do serviços do módulo de autenticação, autorização e integração;
- **Marco 5:** Piloto experimental com análise dos resultados;
- **Marco 6:** Refinamentos do sistema proposto.

Marco	1	2	3	4	5	6	7	8	9	10	11	12
Marco 1												
Marco 2												
Marco 3												

Marco 4												
Marco 5												
Marco 6												

11. Recursos financeiros

11.1 Infraestrutura

11.1.1. Créditos no serviço compute@RNP

Descrição do Recurso	S.O./Distr	Qtde. do recurso	Mês Inicial	Mês Final	Qtd. Meses	Valor em R$ por mês	Valor em R$ total
Máquina Virtual 8 vCPUs e 12 GB de RAM	Linux / Ubuntu	3	01/06/2020	31/05/2021	12	R$ 680,79	R$ 8.169,48
Máquina Virtual 4 vCPUs e 6 GB de RAM	Windows	1	01/06/2020	31/05/2020	12	R$ 340,40	R$ 4.080,00
Armazenamento 1TB	-	1	01/06/2020	31/05/2020	12	R$ 291,32	R$ 3.495,84
						Subtotal	R$ 15.745,32

11.1.2. Equipamentos

Descrição	Instituição de Destino	Qtd.	Valor em R$ estimado
Notebook 14” Modelo i5 (Core i5 - 8GB - SSD 256GB)	UFBA	2	8.880,00
		Subtotal	R$ 8.880,00

12. Referências

[Ates et al. 2007] Ates, M., Gravier, C., Lardon, J., Fayolle, J., e Sauviac, B. (2007). Interoperability between heterogeneous federation architectures: Illustration with saml and wsfederation. In Proceedings of the 2007 Third International IEEE Conference on Signal-Image Technologies and Internet-Based System, SITIS ’07, pages 1063–1070, Washington, DC, USA. IEEE Computer Society.

[Cabarcos et al. 2009] Cabarcos, P. A., Mendoza, F. A., Marín-López, A., e Díaz-Sánchez, D. (2009). Enabling saml for dynamic identity federation management. In Wozniak, J., Konorski, J., Katulski, R., e Pach, A., editors, Wireless and Mobile Networking, volume 308 of IFIP Advances in Information and Communication Technology, pages 173–184. Springer Berlin Heidelberg.

[Capuano et al. 2010] Capuano, N., Gaeta, A., Gaeta, M., Orciuoli, F., Brossard, D., e Gusmini, A. (2010). Management of virtual organizations. In Dimitrakos, T., Martrat, J., e

Wesner, S., editors, Service Oriented Infrastructures and Cloud Service Platforms for the Enterprise, pages 49–73. Springer Berlin Heidelberg.

[Chard et al. 2014] Chard,K.,Lidman, M.,Bryan, J.,Howe,T., McCollam,B., Ananthakrishnan,R., Tuecke, S.,e Foster,I. (2014). Globusnexus: Research identity,pro□le,and group management as a service. In e-Science (e-Science), 2014 IEEE 10th International Conference on, volume 1, pages 31–38.

[GARCIA et al. 2013] Garcia, A. L.; Castillo, E. Fernandez-del; PUEL, M. Identity federation with voms in cloud infrastructures. In: Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on. [s.n.], 2013. v. 1, p. 42–48. Disponível em: http://dx.doi.org/10.1109/CloudCom.2013.13.

[GEMMILL, J. et al. 2009] Cross-domain authorization for federated virtual organizations using the myvocs collaboration environment. Concurr. Comput. : Pract. Exper., John Wiley and Sons Ltd., Chichester, UK, v. 21, n. 4, p. 509–532, mar. 2009. ISSN 1532-0626. Disponível em: http://dx.doi.org/10.1002/cpe.v21:4.

[Greve et al. 2018] Blockchain e a Revolução do Consenso sob Demanda. Fabíola Greve, Leobino Sampaio, Jauberth Weyll Abijaude, Antonio Augusto Ribeiro Coutinho, Ítalo Valcy, Sílvio Queiroz. Livro Texto Minicursos SBRC 2018, ISSN: 2595-2676, Vol.36, Maio 2018, Capítulo 5, SBC - Sociedade Brasileira de Computação, 2018.

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

[Vullingse e Buchhorn 2014] VULLINGS, E.; DALZIEL, J.; BUCHHORN, M. Secure federated authentication and authorisation to grid portal applications using saml and xacml. Journal of Research and Practice in Information Technology, v. 39, n. 2, p. 101–113, 2007. Cited By 5. Disponível em: http://dx.doi.org/10.1016/j.future.2015.09.006.