



**UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA**

Autorizada pelo Decreto Federal nº 77.496 de 27/04/76  
Recredenciamento pelo Decreto nº 17.228 de 25/11/2016



**PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO**  
**COORDENAÇÃO DE INICIAÇÃO CIENTÍFICA**

## **XXVII SEMINÁRIO DE INICIAÇÃO CIENTÍFICA DA UEFS SEMANA NACIONAL DE CIÊNCIA E TECNOLOGIA - 2023**

### **Implementação de Identidades Descentralizadas com Blockchain em Ambientes de Névoa das Coisas**

**Allan Capistrano de Santana Santos<sup>1</sup>; Antonio Augusto Teixeira Ribeiro  
Coutinho**<sup>2</sup>;

1. Bolsista PROBIC, Graduando em Engenharia de Computação, Universidade Estadual de Feira de Santana,  
e-mail: [asantos@ecomp.uefs.br](mailto:asantos@ecomp.uefs.br)
2. Orientador, Departamento de Tecnologia, Universidade Estadual de Feira de Santana,  
e-mail: [augusto@ecomp.uefs.br](mailto:augusto@ecomp.uefs.br)

**PALAVRAS-CHAVE:** Névoa das Coisas; Blockchain; Identidade Descentralizada.

### **INTRODUÇÃO**

A inovação tecnológica tem provocado mudanças no que se refere a comunicação entre diferentes dispositivos inteligentes que produzem juntos um grande volume de dados e que precisam ser processados rapidamente. A Névoa das Coisas (*Fog of Things*, FoT) (Prazeres & Serrano, 2016) (Coutinho et al., 2016) surge como uma resposta à necessidade de uma interação mais ágil e eficiente entre dispositivos conectados em cenários diversos. Ela não apenas reduz a latência das comunicações, mas também pode otimizar a utilização de recursos locais, permitindo que a autenticação e autorização das identidades ocorram de forma rápida e confiável.

A segurança e a confiança em transações digitais representam um desafio constante, especialmente quando intermediários centralizados são substituídos por transações entre pares (*peer-to-peer*) (Androutsellis-Theotokis, 2004). Com isso, as tecnologias de livro razão distribuído (*Distributed Ledger Technologies*, DLTs) como *blockchain* (Greve et al., 2018) podem garantir a consistência e a imutabilidade dos registros de identidade, fortalecendo a segurança dos dados e reduzindo a possibilidade de ataques maliciosos.

A crescente preocupação com a privacidade dos dados e o controle sobre as informações pessoais fomentou o desenvolvimento da Identidade Descentralizada (López, 2020), conceito no qual os indivíduos têm controle total sobre suas informações pessoais e de identificação, em contraste com os sistemas centralizados tradicionais, onde terceiros controlam e armazenam as informações.

Diante desses desafios e oportunidades, este trabalho se propôs a implementar os conceitos de Identidades Descentralizadas em Ambientes de FoT, utilizando a tecnologia DLT/*Blockchain*. O objetivo principal foi aprimorar a eficiência na autenticação e autorização dos nós FoT, almejando facilitar desafios cruciais como a segurança das informações pessoais dos usuários. Como resultado, foram realizados experimentos que evidenciaram a eficiência da abordagem proposta ao garantir que cada dispositivo possua uma identidade digital auto-soberana e uma credencial verificável válida. Além disso, constatou-se a melhora no tempo de resposta de aplicações FoT analisadas.

## METODOLOGIA

Para alcançar os objetivos propostos neste estudo, foi adotada uma abordagem metodológica que se baseou em revisões bibliográficas criteriosas. Inicialmente, foram conduzidas revisões abrangentes sobre os conceitos de Névoa das Coisas e *Blockchain*, com foco na sua utilização conjunta com Identidades Descentralizadas. A pesquisa concentrou-se no uso da DLT *Indy* (Soltani et al., 2018), uma tecnologia permissionada onde apenas os nós autorizados da rede podem participar da validação e da escrita de registros na *blockchain*, oferecendo maior controle e privacidade em comparação com soluções públicas.

Posteriormente, a pesquisa concentrou-se em identificar recursos, tecnologias e ferramentas que pudessem ser aplicados na implementação prática da convergência entre Identidades Descentralizadas e a Névoa das Coisas, utilizando a tecnologia DLT/*Blockchain* como facilitadora.

Para avaliar a implementação do sistema proposto, foram explorados os recursos oferecidos pela plataforma SOFT-IoT (Prazeres & Serrano, 2016), reconhecida pela sua estrutura modular e padronizada. A plataforma apresenta uma arquitetura que se baseia na organização de serviços em módulos independentes chamados de *bundles* (Prazeres et al., 2017). Dentro deste projeto, um *bundle* específico foi desenvolvido para gerenciar todas as funcionalidades relacionadas ao uso de Identidade Descentralizada entre os *gateways* e dispositivos emulados como containers *Docker* (Boettiger, 2015).

A próxima fase envolveu a criação e execução de experimentos configurados com diferentes combinações de *gateways* e dispositivos virtuais, simulando cenários variados de Névoa das Coisas. O foco principal dos experimentos foi avaliar a confiabilidade e a eficiência da abordagem proposta, que visa garantir que cada dispositivo possua sua própria identidade digital e credenciais verificáveis. É importante notar que, devido à natureza descentralizada da identidade, a alocação e verificação das identidades podem resultar em atrasos na comunicação.

## RESULTADOS E DISCUSSÃO

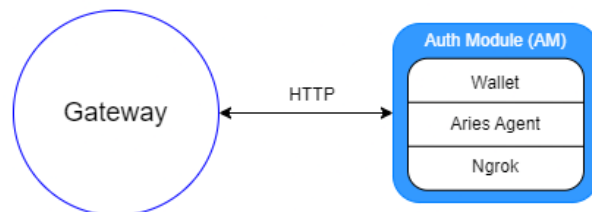
O desenvolvimento dessa pesquisa contou com a utilização de ferramentas que tornaram possível a implementação do projeto de acordo com os objetivos propostos. Optou-se por utilizar o Aca-py (*Aries Cloud Agent - Python*) (Labs, 2023), que é uma implementação específica do *Hyperledger Aries*, ou seja, é um agente de comunicação descentralizado que permite a interação entre diferentes sistemas de identidade descentralizada, seguindo os protocolos e padrões definidos pelo *Hyperledger Aries*. Para gerenciar as credenciais verificáveis, foi implementado um componente de carteira (*Wallet*) como um banco de dados relacional. A carteira é um repositório seguro para armazenar as credenciais verificáveis e outras informações relacionadas à identidade de cada agente. Ela permite que os agentes controlem suas credenciais e decidam quais informações desejam compartilhar com outras entidades na rede.

A integração do sistema de gerenciamento de identidades com a arquitetura SOFT-IoT se deu através do desenvolvimento do *bundle soft-iot-dlt-client-hyperledger-aries*, responsável por tratar das requisições trocadas entre os *gateways* que participam do ambiente de Névoa das Coisas e por fazer requisições HTTP para o agente *Aries* diretamente conectado ao *gateway*. Com isso, é possível verificar as novas conexões de

dispositivos ou *gateways*, bem como acompanhar o fluxo de comunicação entre o *bundle* e o agente *Aries*, garantindo assim a confiança de que todos os nós conectados possuem a autorização devida para participar de um ambiente seguro.

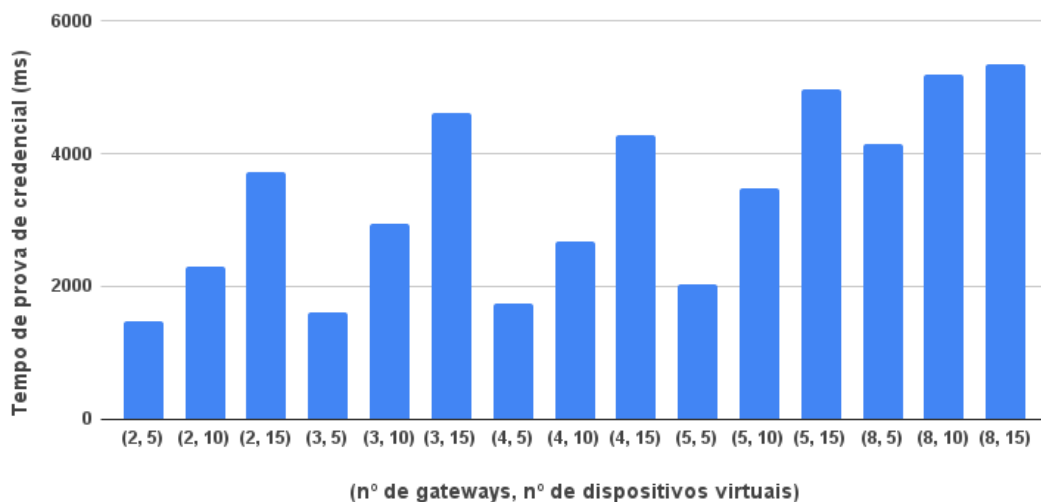
Como forma de facilitar a execução do projeto, foi desenvolvido um módulo de autenticação (*Auth Module*, AM) como uma composição *Docker*, formada pelos containers: *Wallet*, *Aca-py* e o *Ngrok*. O *Ngrok* desempenha um papel relevante ao criar túneis de conexão para os serviços do *Aca-py*, disponibilizando o agente *Aries* na rede e garantindo uma comunicação segura entre os dispositivos e os *gateways* (*Ngrok*, 2023). A Figura 1 ilustra essa abordagem integrada, onde cada *gateway* possui um AM associado para gerenciar as operações necessárias.

A arquitetura geral do ambiente conta com *gateways* posicionados nas três camadas essenciais: *Cloud*, *Fog* e *Edge*. Os dispositivos conectados aos *gateways* são autenticados de forma segura, permitindo que enviem dados com integridade e confidencialidade em todo o ambiente. Dessa forma, todos os nós na rede possuem uma identidade descentralizada e uma credencial verificável que pode ser usada como prova de permissão para participar da rede.



**Figura 1:** Comunicação do *gateway* com o módulo de autenticação.

Os experimentos foram conduzidos com a execução de *gateways* nas camadas da *Fog* e *Edge*, a fim de verificar o tempo necessário para os dispositivos virtuais provarem a posse de credenciais verificáveis válidas. A Figura 2 apresenta os resultados desses experimentos, que foram conduzidos com diferentes números de *gateways* e dispositivos virtuais. Constatou-se que o tempo médio de espera para que um nó receba uma prova de credencial de outro nó é de 3365 milissegundos (ms).



**Figura 2:** Relação entre o tempo de prova de credencial e a quantidade de nós na rede.

## CONSIDERAÇÕES FINAIS

Os resultados obtidos com a implementação de identidades descentralizadas através do *Aca-py* nos *gateways* demonstraram ser promissores para a segurança e autenticação no ecossistema FoT. Embora a atribuição de identidade descentralizada possa resultar em atrasos na comunicação, a vantagem significativa em termos de segurança justifica essa pequena sobrecarga. Os experimentos realizados com diferentes números de *gateways* e dispositivos virtuais proporcionaram uma visão clara sobre o tempo médio de espera para prova de credencial verificável, evidenciando a eficiência da abordagem proposta. Ao garantir que cada dispositivo possua uma identidade digital e uma credencial verificável, o sistema obteve maior proteção contra ataques maliciosos, estabelecendo uma base sólida para a comunicação segura e confiável em ambientes descentralizados.

## REFERÊNCIAS

- ANDROUTSELLIS-THEOTOKIS, Stephanos; SPINELLIS, Diomidis. A survey of peer-to-peer content distribution technologies. **ACM computing surveys (CSUR)**, v. 36, n. 4, p. 335-371, 2004.
- BOETTIGER, C., An introduction to Docker for reproducible research. **ACM SIGOPS Operating Systems Review**, 49(1), 71-79, 2015.
- COUTINHO, A. A. T. R.; CARNEIRO, Elisângela Oliveira; GREVE, Fabíola Gonçalves Pereira. Computação em névoa: Conceitos, aplicações e desafios. **Minicursos do XXXIV SBRC**, p. 266-315, 2016.
- GREVE, Fabíola Greve et al. Blockchain e a Revolução do Consenso sob Demanda. **Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)-Minicursos**, 2018.
- LABS, H. Aries Cloud Agent Python Java Client Library. Disponível em: <<https://github.com/hyperledger-labs/acapy-java-client>>. Acesso em: 26 ago. 2023.
- LÓPEZ, M. Allende. Self-sovereign identity: The future of identity: Self-sovereignty, digital wallets, and blockchain. Inter-American Development Bank, v. 10, p. 0002635, 2020.
- NGROK. Serve Web Apps with one command. Disponível em: <<https://ngrok.com/>>. Acesso em: 27 ago. 2023.
- PRAZERES, Cássio et al. Design and implementation of a message-service oriented middleware for fog of things platforms. In: **Proceedings of the Symposium on Applied Computing**. 2017. p. 1814-1819.
- PRAZERES, Cássio; SERRANO, Martin. Soft-iot: Self-organizing fog of things. In: **2016 30th international conference on advanced information networking and applications workshops (WAINA)**. IEEE, 2016. p. 803-808.
- SOLTANI, Reza; NGUYEN, Uyen Trang; AN, Aijun. A new approach to client onboarding using self-sovereign identity and distributed ledger. In: **2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)**. IEEE, 2018. p. 1129-1136.